Patrones

Recomendaciones de AWS

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Recomendaciones de AWS: Patrones

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

AWS Patrones de orientación prescriptiva 1
Fundamentos de la nube 3
Automatización de la creación de cuentas mediante el Acelerador de zonas de aterrizaje 4
Resumen 4
Requisitos previos y limitaciones 4
Arquitectura 5
Tools (Herramientas) 6
Prácticas recomendadas 9
Epics 9
Recursos relacionados 36
Información adicional 36
Realice un inventario automático de AWS los recursos 38
Resumen 38
Requisitos previos y limitaciones 39
Arquitectura 40
Tools (Herramientas) 40
Prácticas recomendadas 42
Epics 42
Resolución de problemas 49
Recursos relacionados 50
Construye una AWS landing zone con MongoDB Atlas 51
Resumen 51
Requisitos previos y limitaciones 52
Arquitectura 52
Tools (Herramientas) 54
Epics 54
Recursos relacionados 66
Configure los registros de VPC Flow en todas las cuentas 67
Resumen 67
Requisitos previos y limitaciones 67
Arquitectura 68
Tools (Herramientas) 68
Prácticas recomendadas 69
Epics 71

Recursos relacionados 72
Información adicional 73
Administre los conjuntos de AWS permisos con Terraform 75
Resumen 75
Requisitos previos y limitaciones 76
Arquitectura 76
Tools (Herramientas) 78
Prácticas recomendadas 80
Epics 80
Resolución de problemas 92
Recursos relacionados 93
Información adicional 93
Etiquete automáticamente la conexión de puerta de enlace de tránsito 96
Resumen 96
Requisitos previos y limitaciones 96
Arquitectura 97
Tools (Herramientas) 98
Epics 100
Recursos relacionados 106
Más patrones 108
Aprendizaje & automático con IA 109
Asociar un AWS CodeCommit repositorio a Amazon SageMaker AI Studio Classic en todas las cuentas 111
Resumen 111
Requisitos previos y limitaciones 111
Arquitectura 111
Tools (Herramientas) 112
Epics 113
Información adicional 119
Extraer contenido de archivos PDF automáticamente 122
Resumen 122
Requisitos previos y limitaciones 122
Arquitectura 123
Tools (Herramientas) 124
Epics 125
Recursos relacionados 129

Conexiones 130
Cree un modelo de previsión de arranque en frío con SageMaker AI DeepAR 131
Resumen 131
Requisitos previos y limitaciones 131
Arquitectura 132
Tools (Herramientas) 133
Prácticas recomendadas 134
Epics 134
Recursos relacionados 136
Cree un MLOps flujo de trabajo con SageMaker IA y Azure DevOps 137
Resumen 137
Requisitos previos y limitaciones 137
Arquitectura 138
Tools (Herramientas) 140
Prácticas recomendadas 142
Epics 142
Resolución de problemas 152
Recursos relacionados 153
Configure el inicio de sesión en Amazon Bedrock mediante CloudFormation 155
Resumen 155
Requisitos previos y limitaciones 155
Arquitectura 156
Tools (Herramientas) 157
Epics 158
Recursos relacionados 161
Cree contenedores Docker SageMaker para el entrenamiento de modelos en Step Functions . 162
Resumen 162
Requisitos previos y limitaciones 162
Arquitectura 163
Tools (Herramientas) 163
Epics 164
Recursos relacionados 178
Creación de controles de acceso en Amazon EKS con los agentes de Amazon Bedrock 179
Resumen 179
Requisitos previos y limitaciones 179
Arquitectura 180

Tools (Herramientas) 181
Prácticas recomendadas 182
Epics 182
Resolución de problemas 201
Recursos relacionados 202
Implemente un caso de uso de RAG en AWS 203
Resumen 203
Requisitos previos y limitaciones 203
Arquitectura 205
Tools (Herramientas) 206
Prácticas recomendadas 207
Epics 208
Recursos relacionados 211
Información adicional 212
Implemente varios objetos del modelo de canalización en un único punto final SageMaker 214
Resumen 214
Requisitos previos y limitaciones 214
Arquitectura 215
Tools (Herramientas) 215
Epics 216
Recursos relacionados 226
Implemente la validación de la seguridad de la codificación en tiempo real con Kiro 227
Resumen 227
Requisitos previos y limitaciones 228
Arquitectura 229
Tools (Herramientas) 231
Prácticas recomendadas 232
Epics 233
Resolución de problemas 242
Recursos relacionados 243
Información adicional 243
Desarrolle asistentes de chat de IA mediante RAG y mensajes ReAct 247
Resumen 247
Requisitos previos y limitaciones 248
Arquitectura 249
Tools (Herramientas) 250

Prácticas recomendadas 252
Epics 252
Resolución de problemas 260
Recursos relacionados 260
Información adicional 261
Desarrollo de un asistente basado en el chat con Amazon Bedrock 262
Resumen 262
Requisitos previos y limitaciones 263
Arquitectura 263
Tools (Herramientas) 264
Prácticas recomendadas 266
Epics 267
Recursos relacionados 271
Información adicional 272
Documentación del conocimiento institucional a partir de las entradas de voz 274
Resumen 274
Requisitos previos y limitaciones 274
Arquitectura 275
Tools (Herramientas) 276
Prácticas recomendadas 278
Epics 278
Recursos relacionados 284
Genere recomendaciones personalizadas con Amazon Personalize 286
Resumen 286
Requisitos previos y limitaciones 286
Arquitectura 286
Tools (Herramientas) 288
Epics 289
Recursos relacionados 291
Información adicional 292
Optimice los flujos de trabajo de aprendizaje automático con SageMaker IA e Hydra 296
Resumen 296
Requisitos previos y limitaciones 296
Arquitectura 297
Tools (Herramientas) 298
Prácticas recomendadas 299

Epics 300
Resolución de problemas 307
Recursos relacionados 307
Información adicional 307
..... 309
Resumen 309
Requisitos previos y limitaciones 310
Arquitectura 313
Tools (Herramientas) 315
Prácticas recomendadas 316
Epics 316
Recursos relacionados 324
Información adicional 324
Uso de Amazon Q Developer como asistente de codificación 330
Resumen 330
Requisitos previos y limitaciones 330
Tools (Herramientas) 331
Prácticas recomendadas 331
Epics 332
Resolución de problemas 341
Recursos relacionados 341
Utilice el SageMaker procesamiento para la ingeniería de características distribuidas de conjuntos de datos de aprendizaje automático a escala de terabytes 342
Resumen 342
Requisitos previos y limitaciones 342
Arquitectura 343
Tools (Herramientas) 346
Epics 347
Recursos relacionados 358
Conexiones 359
Visualice AI/ML los resultados con Flask y Elastic Beanstalk 360
Resumen 360
Requisitos previos y limitaciones 360
Arquitectura 361
Tools (Herramientas) 363
Epics 363

Resolución de problemas 374
Recursos relacionados 376
Información adicional 376
Más patrones 379
Análisis 380
Analizar los datos de Amazon Redshift en Microsoft SQL Server Analysis Services 382
Resumen 382
Requisitos previos y limitaciones 382
Arquitectura 382
Tools (Herramientas) 383
Epics 383
Recursos relacionados 385
..... 386
Resumen 386
Requisitos previos y limitaciones 386
Arquitectura 387
Tools (Herramientas) 387
Epics 388
Recursos relacionados 393
Automatice la ingesta de datos desde AWS Data Exchange Amazon S3 394
Resumen 394
Requisitos previos y limitaciones 394
Arquitectura 394
Tools (Herramientas) 395
Epics 396
Recursos relacionados 398
Conexiones 398
Automatice la aplicación del cifrado en AWS Glue 399
Resumen 399
Requisitos previos y limitaciones 399
Arquitectura 399
Tools (Herramientas) 400
Prácticas recomendadas 401
Epics 401
Recursos relacionados 404

Crea una canalización de datos para procesar los datos de Google Analytics con el kit de AWS DataOps desarrollo 405
Resumen 405
Requisitos previos y limitaciones 405
Arquitectura 406
Tools (Herramientas) 406
Epics 408
Resolución de problemas 410
Recursos relacionados 410
Información adicional 410
Cree una canalización de procesamiento de video 413
Resumen 413
Requisitos previos y limitaciones 413
Arquitectura 414
Tools (Herramientas) 414
Epics 415
Recursos relacionados 422
Información adicional 423
Conexiones 423
Diseño de una canalización de ETL desde Amazon S3 a Amazon Redshift 424
Resumen 424
Requisitos previos y limitaciones 424
Arquitectura 425
Tools (Herramientas) 425
Epics 426
Recursos relacionados 434
Información adicional 434
Cree una malla de datos empresarial con Amazon DataZone 436
Resumen 436
Requisitos previos y limitaciones 436
Arquitectura 437
Tools (Herramientas) 438
Epics 439
Recursos relacionados 453
Información adicional 454
Calcule el valor en riesgo (VaR) mediante los servicios de AWS 456

Resumen 456
Requisitos previos y limitaciones 456
Arquitectura 457
Tools (Herramientas) 458
Prácticas recomendadas 459
Epics 460
Recursos relacionados 463
Configuración del acceso entre cuentas a un catálogo de datos de AWS Glue compartido 464
Resumen 464
Requisitos previos y limitaciones 464
Arquitectura 464
Tools (Herramientas) 466
Epics 466
Recursos relacionados 479
Información adicional 479
Convierta NORMALIZE en Amazon Redshift SQL 480
Resumen 480
Requisitos previos y limitaciones 480
Arquitectura 480
Tools (Herramientas) 481
Epics 486
Recursos relacionados 486
Convierta RESET WHEN en Amazon Redshift SQL 488
Resumen 488
Requisitos previos y limitaciones 488
Arquitectura 488
Tools (Herramientas) 489
Epics 493
Recursos relacionados 493
Implementar y gestionar un lago de datos sin servidor en AWS 495
Resumen 495
Requisitos previos y limitaciones 495
Arquitectura 496
Tools (Herramientas) 497
Epics 498
Recursos relacionados 500

.... 502
Resumen 502
Requisitos previos y limitaciones 502
Arquitectura 503
Tools (Herramientas) 503
Epics 504
Recursos relacionados 507
Conexiones 508
Asegúrese de que el registro de Amazon EMR en Amazon S3 esté habilitado 509
Resumen 509
Requisitos previos y limitaciones 510
Arquitectura 510
Tools (Herramientas) 511
Epics 511
Recursos relacionados 514
Conexiones 514
Genere datos de pruebas con AWS Glue 515
Resumen 515
Requisitos previos y limitaciones 515
Arquitectura 516
Tools (Herramientas) 516
Prácticas recomendadas 516
Epics 517
Recursos relacionados 529
Información adicional 530
Capturar datos de IoT directamente en Amazon S3 535
Resumen 535
Requisitos previos y limitaciones 535
Arquitectura 536
Tools (Herramientas) 537
Prácticas recomendadas 537
Epics 538
Resolución de problemas 546
Recursos relacionados 546
Información adicional 547
Lanzar un trabajo de Spark en Amazon EMR mediante una función de Lambda 551

Resumen 551
Requisitos previos y limitaciones 551
Arquitectura 552
Tools (Herramientas) 552
Epics 553
Recursos relacionados 556
Información adicional 557
Conexiones 559
Migración de cargas de trabajo de Apache Cassandra a Amazon Keyspaces 560
Resumen 560
Requisitos previos y limitaciones 560
Arquitectura 560
Tools (Herramientas) 561
Prácticas recomendadas 562
Epics 562
Resolución de problemas 576
Recursos relacionados 576
Información adicional 576
Migración de Oracle Business Intelligence 12c a la nube de AWS 578
Resumen 578
Requisitos previos y limitaciones 578
Arquitectura 579
Tools (Herramientas) 580
Epics 581
Recursos relacionados 595
Información adicional 596
Migración de ELK Stack a la nube de AWS 601
Resumen 601
Requisitos previos y limitaciones 601
Arquitectura 603
Tools (Herramientas) 605
Epics 606
Recursos relacionados 614
Información adicional 616
Migre los datos para AWS usar Starburst 617
Resumen 617

Requisitos previos y limitaciones ... 617
Arquitectura ... 617
Tools (Herramientas) ... 619
Epics ... 620
Recursos relacionados ... 623
Optimice la incorporación ETL del tamaño del archivo de entrada ... 624
Resumen ... 624
Requisitos previos y limitaciones ... 624
Arquitectura ... 624
Tools (Herramientas) ... 625
Epics ... 625
Recursos relacionados ... 628
Información adicional ... 629
Orqueste una canalización de ETL con Step Functions ... 630
Resumen ... 630
Requisitos previos y limitaciones ... 630
Arquitectura ... 631
Tools (Herramientas) ... 632
Epics ... 633
Resolución de problemas ... 640
Recursos relacionados ... 641
Información adicional ... 641
Realizar análisis de ML avanzados mediante Amazon Redshift ML ... 642
Resumen ... 642
Requisitos previos y limitaciones ... 642
Arquitectura ... 643
Tools (Herramientas) ... 644
Epics ... 645
Recursos relacionados ... 649
Consulta de Amazon DynamoDB mediante Amazon Athena ... 651
Resumen ... 651
Requisitos previos y limitaciones ... 651
Arquitectura ... 652
Tools (Herramientas) ... 652
Epics ... 653
Resolución de problemas ... 656

Recursos relacionados 657
Consultar tablas de DynamoDB con Athena 658
Resumen 658
Requisitos previos y limitaciones 658
Arquitectura 659
Tools (Herramientas) 659
Epics 660
Recursos relacionados 669
Información adicional 670
Configure la clasificación por idioma para los resultados de las consultas de Amazon Redshift 671
Resumen 671
Requisitos previos y limitaciones 671
Tools (Herramientas) 672
Epics 672
Recursos relacionados 678
Información adicional 678
Suscriba una función de Lambda a las notificaciones de eventos de los buckets S3 entre regiones 682
Resumen 682
Requisitos previos y limitaciones 682
Arquitectura 683
Tools (Herramientas) 683
Epics 684
Recursos relacionados 689
Tres tipos de trabajos de AWS Glue para convertir datos 690
Resumen 690
Requisitos previos y limitaciones 690
Arquitectura 690
Tools (Herramientas) 691
Epics 692
Recursos relacionados 695
Información adicional 695
Conexiones 701
Visualice los registros de auditoría de Amazon Redshift con Athena y QuickSight 702
Resumen 702

Requisitos previos y limitaciones 702
Arquitectura 702
Tools (Herramientas) 703
Epics 703
Recursos relacionados 709
Conexiones 709
Visualice los informes de credenciales de IAM con Amazon Quick Sight 710
Resumen 710
Requisitos previos y limitaciones 710
Arquitectura 711
Tools (Herramientas) 712
Epics 712
Información adicional 718
Más patrones 720
Computación 722
Contenedores y microservicios 723
Acceso a Amazon Neptune desde Amazon EKS 725
Acceder a las aplicaciones de contenedores en Amazon ECS 737
Acceder a las aplicaciones en contenedores en Amazon ECS con un tipo de lanzamiento de AWS Fargate 755
Acceso a las aplicaciones de contenedores de forma privada en Amazon EKS 770
Automatizar las copias de seguridad de las instancias de base de datos de Amazon RDS para PostgreSQL 778
Automatice la implementación de Node Termination Handler 793
Crear e implementar de forma automática una aplicación Java en Amazon EKS 808
Copia de imágenes de contenedor de Amazon ECR en todas las cuentas y regines 834
Cree una definición de tarea de Amazon ECS en EC2 instancias mediante Amazon EFS ... 860
Implementar funciones de Lambda con imágenes de contenedor 867
Implementar microservicios de Java en Amazon ECS con AWS Fargate 876
Implementar paquetes de Kubernetes con Amazon EKS y Helm 883
Implemente un clúster de CockroachDB en Amazon EKS con Terraform 895
Implemente un microservicio Java en Amazon EKS y expóngalo mediante un Equilibrador de carga de aplicación 907
Implemente una aplicación basada en gRPC en Amazon EKS 921
Implemente aplicaciones en contenedores en AWS IoT Greengrass V2 935
Implementar contenedores mediante Elastic Beanstalk 960

.... 966
Genere una dirección IP saliente estática mediante Lambda y Amazon VPC 981
Identificación automática de las imágenes de contenedor duplicadas 998
Instalar el agente SSM en los nodos de trabajo de Amazon EKS 1028
Instale el agente SSM y el CloudWatch agente en los nodos de trabajo de Amazon EKS mediante preBootstrapCommands 1034
Migración de los controladores de entrada NGINX para el Modo automático de EKS 1041
Migración de cargas de trabajo de contenedores de ARO a ROSA 1061
Ejecute tareas de Amazon ECS en Amazon WorkSpaces 1077
Ejecute un contenedor de Docker de API web de ASP.NET en AWS 1087
Ejecute cargas de trabajo con almacenamiento de datos persistente 1100
Configuración del escalado automático mediante Amazon EKS Pod Identity y KEDA 1127
.... 1150
Utilice el TLS mutuo en Amazon ECS con ALB 1173
Más patrones 1204
Sin servidor 1206
Cree una aplicación React Native con AWS Amplify 1207
Administrar de forma centralizada a los inquilinos en varios productos SaaS 1227
Consolidación de la generación de URL prefirmadas y las descargas de objetos de Amazon S3 1241
Crea una conexión entre cuentas de Amazon EventBridge 1258
Entrega de registros de DynamoDB a Amazon S3 1273
Implementación del control de versiones de API basado en rutas mediante API Gateway . 1280
Importe la biblioteca psycopg2 a AWS Lambda 1292
Integración de API Gateway con Amazon SQS 1303
Procese de forma APIs asíncrona con AWS Lambda 1319
Procese de forma APIs asíncrona con Amazon DynamoDB Streams 1329
Procese de forma APIs asíncrona con Amazon SQS 1339
Puesta en marcha de las tareas de Automatización de Systems Manager de forma sincrónica desde Step Functions 1350
Ejecute lecturas paralelas de objetos S3 con AWS Lambda 1365
Enviar datos de telemetría de Lambda a OpenSearch 1378
Configuración de un enrutador de celdas sin servidor 1395
Configuración del acceso privado a un bucket de Amazon S3 1414
Solución de problemas de estado de Step Functions 1421
Más patrones 1431

Red 1434
Automatice la interconexión para AWS Transit Gateway 1435
Centralice la conectividad de red con AWS Transit Gateway 1448
Configure el cifrado HTTPS para Oracle JD Edwards EnterpriseOne mediante un Application Load Balancer 1455
Connect to MGN data and control planes over a private network 1467
Cree objetos de Infoblox con recursos personalizados de AWS CloudFormation 1482
Creación de una arquitectura de IPAM jerárquica y con varias regiones mediante Terraform 1496
Personalice CloudWatch las alertas para Network Firewall 1514
Implementación de recursos en una zona de Wavelength mediante Terraform 1533
Migre registros DNS de forma masiva a un Route 53 1542
Cómo modificar los encabezados HTTP al migrar de F5 a un equilibrador de carga de aplicación en AWS 1554
Informe los hallazgos de Network Access Analyzer en varios Cuentas de AWS 1560
Configure la resolución de DNS para redes híbridas en un entorno de cuentas múltiples AWS 1593
..... 1609
Visualización de los registros y las métricas de AWS Network Firewall con Splunk 1615
Más patrones 1627
Entrega de contenido 1628
Envía AWS WAF registros a Splunk mediante Firehose 1629
Sirva contenido estático en un bucket de S3 a través de una VPC mediante CloudFront ... 1639
Más patrones 1648
&Almacenamiento de bases de datos 1649
Bases de datos 1650
Acceso a los datos en las instalaciones de SQL Server mediante servidores vinculados ... 1653
Añada HA a Oracle PeopleSoft en AWS 1659
Análisis de los objetos para realizar migraciones parciales de Oracle a PostgreSQL 1684
Evalúe el rendimiento de las consultas para migrar SQL Server a MongoDB 1701
Automatice blue/green las implementaciones de las bases de datos globales de Aurora con iAC 1711
Automatización de la replicación de las instancias de Amazon RDS entre cuentas 1747
Automatice las tareas de la base de datos con un programador AWS Lambda de tareas .. 1764
Automatización de la conmutación por error y la conmutación por recuperación mediante DR Orchestrator Framework 1778

Cree copias de seguridad de las bases de datos de SAP HANA de forma automática 1806
Generación automática de modelos de PynamoDB y funciones CRUD para DynamoDB ... 1815
Bloquear el acceso público a Amazon RDS 1823
Configuración de la autenticación de Windows para Amazon RDS mediante Microsoft AD 1830
Configurar el acceso entre cuentas a Amazon DynamoDB 1848
Configure el enrutamiento de solo lectura en los grupos de disponibilidad de Always On ... 1862
Conectar mediante un túnel SSH en pgAdmin 1871
Convertir consultas JSON de Oracle en SQL de bases de datos PostgreSQL 1876
Copiar tablas de Amazon DynamoDB entre cuentas 1908
Copiar tablas de Amazon DynamoDB entre cuentas 1916
Crear informes de costos y uso para Amazon RDS y Amazon Aurora 1929
Implemente SQL Server FCIs en Amazon EC2 y Amazon FSx 1936
Emule las matrices PL/SQL asociativas de Oracle en Aurora y RDS 1953
Habilitar conexiones cifradas para instancias de base de datos PostgreSQL 1966
Cifrar una instancia de base de datos de Amazon RDS para PostgreSQL existente 1975
Imponga el etiquetado automático de las bases de datos de Amazon RDS en el lanzamiento 1984
Estime los costos de DynamoDB 1990
Costos de almacenamiento estimados para una tabla de Amazon DynamoDB 2003
Calcule el tamaño del motor de Amazon RDS para una base de datos de Oracle mediante informes de AWR 2007
Exporte tablas de Amazon RDS para SQL Server a un bucket de S3 2042
Gestionar bloques anónimos en sentencias SQL dinámicas 2055
Ayudar a reforzar el etiquetado en DynamoDB 2063
Implemente DR entre regiones 2069
Migración de funciones de Oracle con más de 100 argumentos a PostgreSQL 2088
Migre la base de datos de Oracle a Amazon RDS con Oracle Data Pump 2094
Migración de las cargas de trabajo de Redis a Redis Enterprise Cloud en AWS 2111
Migración de SAP HANA a AWS mediante HSR 2141
Migre el grupo de disponibilidad de SQL Server Always On mediante AWS MGN 2155
Migración de SQL Server a AWS mediante grupos de disponibilidad distribuidos 2168
Migrar una base de datos relacional a MongoDB Atlas en AWS 2180
Migre un entorno MongoDB autohospedado a MongoDB Atlas 2191
Migración de una base de datos de Oracle a Amazon DynamoDB 2203
Migre de Oracle 8i o 9i a Amazon RDS para Oracle con AWS DMS SharePlex 2209
Migración de datos MySQL en las instalaciones a Amazon EC2 2218

Supervise GoldenGate los registros mediante Amazon CloudWatch 2228
Cambie la plataforma de Oracle Database EE a Amazon RDS para Oracle SE2 2243
Replicar bases de datos de unidades centrales en AWS mediante Precisely Connect 2255
Programe trabajos para Amazon RDS y Aurora PostgreSQL 2276
Envío de notificaciones para RDS para SQL Server mediante un servidor SMTP 2282
Configure la DR para SAP en IBM Db2 en AWS 2297
Configure una CI/CD canalización para la migración de bases de datos mediante Terraform 2320
Configure una FCI de Microsoft SQL Server en Amazon EC2 mediante FSx 2330
Configurar una HA/DR arquitectura para Oracle E-Business Suite en Amazon RDS Custom 2349
Transmita datos de bases de datos a MongoDB Atlas en AWS 2358
Funciones de transición para una aplicación de Oracle PeopleSoft 2370
Descarga de datos de Amazon Redshift entre las cuentas 2406
Patrones de migración de bases de datos según carga de trabajo 2437
Más patrones 2448
Almacenamiento y copia de seguridad 2453
Permita que EC2 las instancias tengan acceso de escritura a los buckets de S3 en AMS .. 2454
Automatice la ingesta de flujos de datos en una base de datos de Snowflake 2460
Cifrar automáticamente los volúmenes de EBS 2471
Haga una copia de seguridad de los servidores Sun SPARC en el emulador Charon-SSP en AWS 2483
Copia de seguridad y archivo de datos en Amazon S3 con Veeam 2509
Copie los datos de Amazon S3 entre cuentas y regiones 2539
Habilite el archivado de DB2 registros en Amazon S3 2555
Migre los datos de Hadoop a Amazon S3 mediante DistCp AWS PrivateLink para Amazon S3 2574
Más patrones 2590
Herramientas para desarrolladores 2592
DevOps 2593
Acelere MLOps con las plantillas Backstage y de autoservicio de Amazon AI SageMaker . 2597
Automatice las operaciones AWS de infraestructura 2618
Automatice CloudFront las actualizaciones para los cambios en los puntos finales del equilibrador de carga 2628
Automatice CodeGuru las revisiones de las aplicaciones de AWS CDK Python 2637
Automatice la Supply Chain implementación de lagos de datos 2649

Automatice la evaluación de recursos de AWS 2685
Automatizar la instalación de los sistemas SAP 2700
Automatice la implementación de productos y la cartera de AWS Service Catalog mediante AWS CDK 2715
Automatización de una canalización de revisiones dinámica 2734
Automatice la eliminación de pilas CloudFormation 2763
Automatización de la ingesta de métricas personalizadas de Amazon MWAA 2775
Adjunte automáticamente una política gestionada para Systems Manager a los perfiles de EC2 instancia 2792
Cree CI/CD canalizaciones y clústeres de Amazon ECS para microservicios de forma automática 2808
Creación, ejecución y envío de imágenes de Docker a Amazon ECR 2822
Cree y pruebe aplicaciones iOS con los servicios de AWS 2829
Configure TLS mutua para aplicaciones en Amazon EKS 2835
Cree recursos de Amazon WorkSpaces Applications mediante CloudFormation 2847
Crear un analizador de registros personalizado para Amazon ECS con Firelens 2854
Creación de un marco de orquestación de recursos 2864
Cree solicitudes de extracción automatizadas para la infraestructura AWS 2878
Crear canalizaciones de CI dinámicas para proyectos de Java y Python 2890
Despliega CloudWatch Synthetics canaries 2907
Implemente una ChatOps solución para administrar los resultados del escaneo SAST 2915
Implementación de sistemas de agentes en Amazon Bedrock con CrewAI 2934
..... 2952
Implemente código en varias regiones de AWS 2956
Implemente cargas de trabajo desde DevOps canalizaciones de Azure a clústeres privados de Amazon EKS 2969
Ejecución de consultas SQL en Amazon Redshift 3003
Exportar etiquetas de instancias de Amazon EC2 a un archivo CSV 3016
Exportar los informes de AWS Backup como un archivo CSV 3023
Genere una CloudFormation plantilla de AWS que contenga las reglas administradas de AWS Config 3032
Otorgue a las instancias de SageMaker Notebook acceso multicuenta a un repositorio CodeCommit 3039
Implemente una estrategia de ramificación de GitHub Flow 3051
Implementación de una estrategia de ramificación de Gitflow 3062
Implementación de una estrategia de ramificación de Trunk 3074

Implementación de un análisis centralizado y personalizado de Checkov 3081
Implementación de diagnósticos con K8sGPT y Amazon Bedrock 3092
Inicie diferentes CI/CD canalizaciones después de detectar cambios en un monorepo 3107
Integrar un repositorio de Bitbucket con AWS Amplify 3125
Lance un CodeBuild proyecto en todas las cuentas de AWS con Lambda 3134
Administración de la conmutación por error de multi-AZ para clústeres de EMR mediante el Controlador de recuperación de aplicaciones 3148
Gestione blue/green las implementaciones de microservicios en varias cuentas y regiones 3165
Supervisar los repositorios de Amazon ECR en busca de permisos comodín 3199
Optimización de las implementaciones de varias cuentas sin servidor 3204
AWS Service Catalog Aprovisione productos mediante GitHub acciones 3224
Aprovisionamiento de roles de IAM con privilegio mínimo 3235
Publica CloudWatch las métricas de Amazon en un archivo CSV 3249
Eliminar EC2 entradas de Amazon de un lado a otro Cuentas de AWS 3255
Eliminar las EC2 entradas de Amazon en el mismo Cuenta de AWS 3273
Ejecute pruebas unitarias para trabajos ETL de Python en AWS Glue 3284
Configure una CI/CD canalización con CodePipeline 3295
Configuración del registro centralizado a escala con Terraform 3311
Configurar el end-to-end cifrado para aplicaciones en Amazon EKS 3336
Simplificación de la implementación de aplicaciones multiusuario de Amazon EKS 3350
Simplifique los flujos de trabajo de Amazon Lex 3369
Utilice la construcción de AWS Fargate WaitCondition gancho 3389
Utilice repositorios de Git de terceros en AWS CodePipeline 3402
Valide las configuraciones de Terraform mediante AWS CodePipeline 3412
Más patrones 3429
infraestructura 3433
Acceder a un host bastión mediante Session Manager e Instance Connect 3435
Centralice la resolución de DNS mediante AWS Managed Microsoft AD 3451
Centralice la supervisión mediante Observability Access Manager 3463
Comprueba EC2 las instancias para ver si hay etiquetas obligatorias en el momento del lanzamiento 3477
Eliminación segura de los recursos de AFT después de la pérdida de archivos de estado . 3483
..... 3497
Personalice los nombres de los roles predeterminados mediante AWS CDK aspectos y trampillas de escape 3505

Implemente un clúster de Cassandra en Amazon EC2 con estática privada IPs 3514
Amplíe VRFs sus servicios a AWS con Transit Gateway Connect 3522
Reciba notificaciones de Amazon SNS sobre cambios de estado en las claves de AWS KMS 3541
Preserve el espacio IP enrutable en los diseños de VPC de varias cuentas para subredes que no son de carga de trabajo 3549
Aprovisionamiento de un producto de Terraform en Service Catalog desde un repositorio . 3555
Registre varias Cuentas de AWS con una sola dirección de correo electrónico 3576
Configure la resolución de DNS para redes híbridas en un entorno de AWS de una sola cuenta 3594
Configura automáticamente los bots de UiPath RPA en Amazon EC2 3600
Configure una PeopleSoft arquitectura de alta disponibilidad en AWS 3617
Configure la recuperación ante desastres para Oracle JD Edwards EnterpriseOne 3647
Configuración de detección y generación de informes de desviaciones 3677
Importe correctamente un bucket de S3 como CloudFormation pila 3682
Sincronización de sistemas de archivos de Amazon EFS en regiones distintas 3695
Pruebe la AWS infraestructura con LocalStack Terraform Tests 3704
Actualice los clústeres de SAP Pacemaker de a ENSA1 ENSA2 3712
Utilice zonas de disponibilidad coherentes en VPCs las diferentes cuentas 3735
Utilice el usuario IDs en las políticas de IAM 3741
Validar Account Factory para el código Terraform localmente 3752
Más patrones 3772
Aplicaciones web y móviles 3776
Autentique a los usuarios de la aplicación web React 3777
Crear una aplicación React con AWS Amplify y Amazon Cognito 3787
Creación de un portal para micro-frontends 3804
Implemente un SPA basado en React en Amazon S3 y CloudFront 3836
Implemente una API de Amazon API Gateway mediante puntos de conexión privados 3844
Incorpore componentes visuales de Amazon Quick Sight en aplicaciones web 3852
Explore el desarrollo de aplicaciones web con Green Boost 3875
Estructurar un proyecto Python en arquitectura hexagonal 3904
Más patrones 3931
IoT 3933
Extraiga y consulte los atributos AWS IoT SiteWise de los metadatos 3934
Resumen 3934
Requisitos previos y limitaciones 3934

Arquitectura 3935
Tools (Herramientas) 3935
Epics 3936
Recursos relacionados 3939
Información adicional 3940
..... 3942
Resumen 3942
Requisitos previos y limitaciones 3943
Arquitectura 3943
Tools (Herramientas) 3944
Prácticas recomendadas 3944
Epics 3945
Resolución de problemas 3961
Recursos relacionados 3964
Información adicional 3964
Más patrones 3966
&Modernización de migración 3967
Migración 3968
..... 3969
Cree CloudFormation plantillas de AWS para AWS DMS 3978
Introducción a la detección automática de cartera 3982
Migración de cargas de trabajo Cloudera en las instalaciones a AWS 3991
Resolver los errores de conexión después de migrar SQL Server a AWS 4009
Rediseñar 4012
Volver a alojar 4411
Reubicar 4658
Redefinir la plataforma 4706
Patrones de migración por carga de trabajo 5147
Más patrones 5156
Modernización 5158
Archivar automáticamente datos de DynamoDB que han vencido en Amazon S3 5159
Cree una arquitectura sin servidor multiusuario en Amazon Service OpenSearch 5176
Implementar aplicaciones de varias pilas 5225
Implemente aplicaciones anidadas con SAM de AWS 5235
Implemente el aislamiento de inquilinos de SaaS para Amazon S3 mediante un TVM AWS Lambda 5244

Implementa el patrón saga sin servidor con Step Functions 5271
Gestión de las aplicaciones de contenedores en las instalaciones con Amazon ECS Anywhere 5286
Incorporación de inquilinos en la arquitectura SaaS 5296
Use CQRS y abastecimiento de eventos 5322
Más patrones 5349
Unidades centrales 5352
Acceda Servicios de AWS desde IBM z/OS instalando el AWS CLI 5354
Copia de seguridad y archivo de datos de mainframe en Amazon S3 5374
Cree programas COBOL Db2 utilizando y AWS Mainframe Modernization AWS CodeBuild 5401
Compile un Micro Focus Enterprise Server PAC 5427
Cree un visor de archivos de unidad central en la nube de AWS 5448
Almacene en contenedores las aplicaciones modernizadas de Blu Age 5464
Convierta datos EBCDIC a ASCII en AWS 5474
Convierta archivos EBCDIC de mainframe en archivos ASCII mediante AWS Lambda 5493
Convertir archivos de datos de mainframe con diseños de registros complejos 5517
Implementar un entorno para aplicaciones en contenedores 5537
Genere información sobre los datos de Db2 z/OS 5548
Genere información con AWS Mainframe Modernization Amazon Q 5600
Implemente la autenticación Microsoft Entra ID para AWS Blu Age 5619
Integrar el controlador universal Stonebranch con AWS 5639
Migración y réplica de archivos VSAM a la nube de AWS con Precisely 5675
Modernice una aplicación de mainframe de muestra mediante AWS Transform 5693
Modernice las aplicaciones de mainframe con Terraform AWS Transform 5713
Modernice la administración de la producción del mainframe en AWS 5751
Modernice las cargas de trabajo de impresión por lotes de su mainframe en AWS 5807
Modernización del entorno de mainframe con Rocket Software Enterprise Suite 5837
Modernizar sus cargas de trabajo de impresión en línea de mainframe en AWS 5855
Mover los archivos de mainframe a Amazon S3 mediante Transfer Family 5891
Optimice el rendimiento de su aplicación AWS modernizada Blu Age 5907
Proteja el acceso de los usuarios a una base de datos de federación Db2 5933
Transfiera z/OS datos de Db2 a AWS 5943
Transforma Easytrieve a idiomas modernos usando AWS Transform 5971
Más patrones 5991
Administración 5992

Administración de costos 5993
Crear informes detallados de costos y uso para los trabajos de AWS Glue 5994
Crear informes detallados de costos y uso para los clústeres de Amazon EMR 6000
Más patrones 6005
Informática para usuarios finales 6006
Implemente la autenticación SAML 2.0 para Amazon WorkSpaces 6007
Más patrones 6017
Computación de alto rendimiento 6018
Implementación de un sistema de archivos de Lustre mediante Terraform y DRA 6019
Configurar un panel de monitoreo de Grafana para AWS ParallelCluster 6028
Más patrones 6043
Nube híbrida 6044
Configure una canalización para la carga de trabajo híbrida en Amazon ECS Anywhere ... 6045
Más patrones 6066
Gestión y gobernanza 6067
Alertar cuando los recursos de Amazon Data Firehose no están cifrados 6069
Automatice las asignaciones de CIDR de IPv4 IPAM de Amazon VPC 6074
Automatice la adición o actualización de entradas de registro de Windows 6105
Crear automáticamente una RFC mediante Python 6110
Parada e inicio de una instancia de base de datos de Amazon RDS 6118
Centralización de la distribución de paquetes de software en AWS Organizations mediante Terraform 6133
Configure el registro para las aplicaciones .NET en CloudWatch Logs 6146
Copiar los productos de AWS Service Catalog en todas las cuentas y regiones de AWS ... 6156
Crear una matriz RACI para las operaciones en la nube 6166
Cree alarmas para métricas personalizadas mediante CloudWatch 6173
Crear un IDE de AWS Cloud9 que utilice volúmenes de EBS con cifrado predeterminado . 6181
Cree paneles de control basados en etiquetas automáticamente CloudWatch 6187
Documentación del diseño de su zona de aterrizaje 6196
Habilite Amazon DevOps Guru en toda la organización con la AWS CDK 6200
Control de los conjuntos de permisos para varias cuentas mediante AFT 6228
Implementación de AFT mediante una canalización de arranque 6240
Administre los productos de AWS Service Catalog en varias cuentas y regiones de AWS . 6265
Supervisión de los clústeres de SAP RHEL Pacemaker 6273
Supervise la actividad de las aplicaciones con CloudWatch Logs Insights 6294
Supervise el uso de una AMI en Cuentas de AWS 6308

Vea los detalles de la instantánea de EBS de su cuenta u organización de AWS 6325
Más patrones 6332
Mensajería y comunicaciones 6335
Automatizar la configuración de RabbitMQ en Amazon MQ 6336
Mejorar la calidad de las llamadas en las estaciones de trabajo de los agentes en Amazon Connect 6344
Más patrones 6362
Estrategia de varias cuentas 6363
Migre Cuenta de AWS y de AWS Organizations a AWS Control Tower 6364
Configure alertas para el cierre programático de cuentas en AWS Organizations 6375
Más patrones 6385
Seguridad, & cumplimiento de identidad 6386
Automatice la respuesta a incidentes y el análisis forense 6389
Resumen 6389
Requisitos previos y limitaciones 6389
Arquitectura 6390
Tools (Herramientas) 6393
Epics 6394
Recursos relacionados 6398
Información adicional 6398
Conexiones 6398
Acceso a la auditoría automática desde direcciones IP públicas 6399
Resumen 6399
Requisitos previos y limitaciones 6399
Arquitectura 6400
Tools (Herramientas) 6402
Prácticas recomendadas 6403
Epics 6403
Resolución de problemas 6408
Recursos relacionados 6408
Corrija automáticamente las instancias y los clústeres de bases de datos de Amazon RDS no cifrados 6409
Resumen 6409
Requisitos previos y limitaciones 6409
Arquitectura 6411
Tools (Herramientas) 6411

Prácticas recomendadas 6413
Epics 6413
Recursos relacionados 6420
Información adicional 6420
Validación e implementación automáticas de las políticas y los roles de IAM 6422
Resumen 6422
Requisitos previos y limitaciones 6423
Arquitectura 6424
Tools (Herramientas) 6424
Epics 6425
Recursos relacionados 6429
Integre de forma bidireccional Security Hub, CSPM y Jira 6430
Resumen 6430
Requisitos previos y limitaciones 6431
Arquitectura 6432
Tools (Herramientas) 6433
Epics 6434
Recursos relacionados 6444
Información adicional 6444
Cree un proceso para imágenes de contenedores reforzadas 6446
Resumen 6446
Requisitos previos y limitaciones 6446
Arquitectura 6447
Tools (Herramientas) 6450
Epics 6451
Resolución de problemas 6459
Recursos relacionados 6459
..... 6461
Resumen 6461
Requisitos previos y limitaciones 6462
Arquitectura 6462
Tools (Herramientas) 6464
Prácticas recomendadas 6465
Epics 6465
Resolución de problemas 6475
Recursos relacionados 6475

Comprueba la versión de registro de acceso, HTTPS y TLS en una CloudFront distribución de Amazon 6476
Resumen 6476
Requisitos previos y limitaciones 6477
Arquitectura 6477
Tools (Herramientas) 6478
Epics 6478
Recursos relacionados 6481
Conexiones 6481
Elección de un flujo de autenticación de Amazon Cognito 6482
Resumen 6482
Requisitos previos y limitaciones 6482
Arquitectura 6483
Tools (Herramientas) 6487
Epics 6488
Recursos relacionados 6491
Información adicional 6492
Cree reglas AWS Config personalizadas con Guard 6493
Resumen 6493
Requisitos previos y limitaciones 6494
Arquitectura 6494
Tools (Herramientas) 6499
Epics 6499
Resolución de problemas 6501
Recursos relacionados 6502
Cree un informe con los hallazgos de Prowler a partir de varios Cuentas de AWS 6504
Resumen 6504
Requisitos previos y limitaciones 6505
Arquitectura 6506
Tools (Herramientas) 6507
Epics 6508
Resolución de problemas 6533
Recursos relacionados 6533
Información adicional 6534
Implemente AWS Control Tower controles mediante AWS CDK 6536
Resumen 6536

Requisitos previos y limitaciones ... 6537
Arquitectura ... 6538
Tools (Herramientas) ... 6539
Prácticas recomendadas ... 6540
Epics ... 6540
Recursos relacionados ... 6548
Información adicional ... 6549
Implemente AWS Control Tower controles con Terraform ... 6552
Resumen ... 6552
Requisitos previos y limitaciones ... 6553
Arquitectura ... 6554
Tools (Herramientas) ... 6555
Prácticas recomendadas ... 6555
Epics ... 6556
Resolución de problemas ... 6561
Recursos relacionados ... 6563
Información adicional ... 6563
Implemente automatizaciones de seguridad para usar Terraform AWS WAF ... 6567
Resumen ... 6567
Requisitos previos y limitaciones ... 6567
Arquitectura ... 6568
Tools (Herramientas) ... 6568
Prácticas recomendadas ... 6569
Epics ... 6569
Resolución de problemas ... 6572
Recursos relacionados ... 6573
Implementación de una canalización que detecte problemas de seguridad en el código ... 6574
Resumen ... 6574
Requisitos previos y limitaciones ... 6574
Arquitectura ... 6574
Tools (Herramientas) ... 6575
Epics ... 6576
Resolución de problemas ... 6579
Recursos relacionados ... 6580
Información adicional ... 6580
Implementar controles de detección para subredes públicas ... 6582

Resumen 6582
Requisitos previos y limitaciones 6583
Arquitectura 6583
Tools (Herramientas) 6584
Prácticas recomendadas 6585
Epics 6585
Recursos relacionados 6593
Información adicional 6594
Implementación de controles de acceso preventivos para las subredes públicas 6596
Resumen 6596
Requisitos previos y limitaciones 6596
Arquitectura 6597
Tools (Herramientas) 6598
Epics 6599
Recursos relacionados 6605
Información adicional 6605
Detección de instancias de Amazon RDS con certificados CA que vencen 6608
Resumen 6608
Requisitos previos y limitaciones 6608
Arquitectura 6609
Tools (Herramientas) 6611
Prácticas recomendadas 6612
Epics 6612
Resolución de problemas 6616
Recursos relacionados 6617
Genere dinámicamente una política de IAM con IAM Access Analyzer 6618
Resumen 6618
Requisitos previos y limitaciones 6618
Arquitectura 6619
Tools (Herramientas) 6620
Epics 6622
Recursos relacionados 6629
Habilita el GuardDuty uso de plantillas CloudFormation 6630
Resumen 6630
Requisitos previos y limitaciones 6630
Arquitectura 6631

Tools (Herramientas) 6631
Epics 6632
Recursos relacionados 6636
Información adicional 6636
Habilitar el cifrado transparente de datos en Amazon RDS para SQL Server 6638
Resumen 6638
Requisitos previos y limitaciones 6638
Arquitectura 6638
Tools (Herramientas) 6639
Epics 6639
Recursos relacionados 6642
Ayudar a evitar la eliminación programada de claves de KMS 6643
Resumen 6643
Requisitos previos y limitaciones 6643
Arquitectura 6644
Tools (Herramientas) 6645
Epics 6646
Recursos relacionados 6649
Información adicional 6650
Conexiones 6650
Identifique los buckets públicos de Amazon S3 en AWS Organizations 6651
Resumen 6651
Requisitos previos y limitaciones 6651
Arquitectura 6652
Tools (Herramientas) 6653
Epics 6654
Resolución de problemas 6658
Recursos relacionados 6659
Información adicional 6659
Ingesta de registros de seguridad de AWS en Microsoft Sentinel 6661
Resumen 6661
Requisitos previos y limitaciones 6661
Arquitectura 6663
Tools (Herramientas) 6664
Prácticas recomendadas 6665
Epics 6665

Recursos relacionados 6677
Administre AWS Organizations las políticas como código 6678
Resumen 6678
Requisitos previos y limitaciones 6679
Arquitectura 6679
Tools (Herramientas) 6681
Prácticas recomendadas 6682
Epics 6682
Resolución de problemas 6701
Recursos relacionados 6703
Información adicional 6704
Gestione los conjuntos de permisos del Centro de Identidad de IAM mediante CodePipeline . 6706
Resumen 6706
Requisitos previos y limitaciones 6706
Arquitectura 6708
Tools (Herramientas) 6709
Prácticas recomendadas 6710
Epics 6710
Resolución de problemas 6721
Recursos relacionados 6722
Administrar credenciales con AWS Secrets Manager 6723
Resumen 6723
Requisitos previos y limitaciones 6723
Arquitectura 6723
Tools (Herramientas) 6724
Epics 6724
Recursos relacionados 6726
Información adicional 6726
Supervise ElastiCache los clústeres de Amazon para comprobar el cifrado en reposo 6729
Resumen 6729
Requisitos previos y limitaciones 6730
Arquitectura 6731
Tools (Herramientas) 6731
Prácticas recomendadas 6732
Epics 6733
Resolución de problemas 6736

Recursos relacionados 6738
Supervisar la actividad del usuario raíz de IAM 6739
Resumen 6739
Requisitos previos y limitaciones 6739
Arquitectura 6740
Tools (Herramientas) 6740
Epics 6742
Recursos relacionados 6747
Información adicional 6747
Notificar cuando se cree un usuario de IAM 6748
Resumen 6748
Requisitos previos y limitaciones 6748
Arquitectura 6748
Tools (Herramientas) 6749
Epics 6750
Recursos relacionados 6752
Conexiones 6753
Impedir el acceso a Internet mediante una SCP 6754
Resumen 6754
Requisitos previos y limitaciones 6754
Tools (Herramientas) 6755
Prácticas recomendadas 6755
Epics 6756
Recursos relacionados 6758
Informe de las identidades de IAM Identity Center y sus asignaciones 6759
Resumen 6759
Requisitos previos y limitaciones 6759
Arquitectura 6761
Tools (Herramientas) 6761
Epics 6762
Resolución de problemas 6763
Recursos relacionados 6765
Información adicional 6765
Restricción del acceso en función de la dirección IP o la geolocalización 6768
Resumen 6768
Requisitos previos y limitaciones 6768

Tools (Herramientas) 6769
Epics 6770
Recursos relacionados 6776
Escanea los repositorios de Git en busca de información confidencial 6777
Resumen 6777
Requisitos previos y limitaciones 6777
Arquitectura 6777
Tools (Herramientas) 6778
Prácticas recomendadas 6778
Epics 6778
Recursos relacionados 6782
Transferencias de archivos seguras con Transfer Family y GuardDuty 6783
Resumen 6783
Requisitos previos y limitaciones 6784
Arquitectura 6785
Tools (Herramientas) 6786
Prácticas recomendadas 6787
Epics 6788
Resolución de problemas 6792
Recursos relacionados 6796
Información adicional 6796
Proteja los datos confidenciales de los CloudWatch registros con Macie 6798
Resumen 6798
Requisitos previos y limitaciones 6798
Arquitectura 6799
Tools (Herramientas) 6800
Prácticas recomendadas 6801
Epics 6801
Resolución de problemas 6823
Recursos relacionados 6823
..... 6825
Resumen 6825
Requisitos previos y limitaciones 6825
Arquitectura 6826
Tools (Herramientas) 6828
Prácticas recomendadas 6828

Epics 6829
Resolución de problemas 6834
Recursos relacionados 6834
Información adicional 6835
Enviar alertas desde AWS Network Firewall a un canal de Slack 6836
Resumen 6836
Requisitos previos y limitaciones 6836
Arquitectura 6837
Tools (Herramientas) 6838
Epics 6839
Recursos relacionados 6845
Información adicional 6845
Envío de atributos personalizados a los tokens de Amazon Cognito 6850
Resumen 6850
Requisitos previos y limitaciones 6850
Arquitectura 6851
Tools (Herramientas) 6852
Prácticas recomendadas 6852
Epics 6854
Resolución de problemas 6863
Recursos relacionados 6863
Información adicional 6863
Simplifique la administración de certificados privados mediante AWS Private CA y AWS RAM 6867
Resumen 6867
Requisitos previos y limitaciones 6867
Arquitectura 6868
Tools (Herramientas) 6869
Epics 6870
Recursos relacionados 6879
Información adicional 6880
Optimice la gestión EC2 del cumplimiento de Amazon con los agentes de Amazon Bedrock y AWS Config 6881
Resumen 6881
Requisitos previos y limitaciones 6881
Arquitectura 6882

Tools (Herramientas) 6883
Prácticas recomendadas 6884
Epics 6885
Resolución de problemas 6887
Recursos relacionados 6887
Actualice las credenciales del Centro de Identidad de IAM mediante PowerShell 6889
Resumen 6889
Requisitos previos y limitaciones 6889
Arquitectura 6890
Tools (Herramientas) 6890
Prácticas recomendadas 6891
Epics 6891
Resolución de problemas 6894
Recursos relacionados 6894
Información adicional 6894
Uso de Network Firewall para capturar los nombres de DNS del tráfico saliente 6897
Resumen 6897
Requisitos previos y limitaciones 6897
Arquitectura 6898
Tools (Herramientas) 6898
Epics 6899
Utilice Terraform para activar automáticamente GuardDuty 6916
Resumen 6916
Requisitos previos y limitaciones 6917
Arquitectura 6919
Tools (Herramientas) 6920
Epics 6921
Recursos relacionados 6930
Información adicional 6931
Verificación de las prácticas recomendadas para PCI DSS 4.0 6932
Resumen 6932
Requisitos previos y limitaciones 6932
Tools (Herramientas) 6934
Epics 6934
Recursos relacionados 6937
Información adicional 6937

Conexiones 6938
Más patrones 6939
..... 6942

AWS Patrones de orientación prescriptiva

Los patrones de orientación prescriptiva de Amazon Web Services (AWS) proporcionan step-by-step instrucciones, arquitectura, herramientas y código para implementar escenarios específicos de migración, modernización e implementación a la nube. Estos patrones, que son examinados por expertos en la materia AWS, están pensados para desarrolladores y usuarios prácticos que planean migrar o están en proceso de migrar a ellos. AWS También ayudan a los usuarios que ya están conectados AWS y buscan formas de optimizar o modernizar sus operaciones en la nube.

Puede utilizar estos patrones para trasladar sus cargas de trabajo locales o en la nube de complejidad variable a la nube AWS y acelerar sus esfuerzos de adopción, optimización y modernización de la nube, independientemente de si se encuentra en la fase de prueba de concepto, planificación o implementación de su proyecto. Por ejemplo, para un proyecto de migración a la nube:

- En la fase de planificación, puede evaluar las diferentes opciones disponibles para migrar a AWS. Puede elegir el patrón adecuado que se adapte a sus necesidades, en función de si desea reubicar, realojar, redefinir la plataforma o rediseñar la arquitectura. También puede comprender las diferentes herramientas disponibles para la migración y empezar a planificar la adquisición de licencias o iniciar las primeras conversaciones con los proveedores.
- En las fases de prueba de concepto e implementación, puede seguir las step-by-step instrucciones que se proporcionan en el patrón para migrar su carga de trabajo a una. AWS Cada patrón incluye detalles como los requisitos previos, las arquitecturas de referencia objetivo, las herramientas, las step-by-step tareas, las mejores prácticas, la solución de problemas y el código.
- Si ya lo usa Nube de AWS, puede encontrar patrones que lo ayudarán a modernizar, optimizar, escalar y proteger el uso de los recursos de la nube.

Para ver las listas de patrones por dominio técnico, utilice los siguientes enlaces o las opciones de filtrado y búsqueda de la AWS página de inicio de la guía prescriptiva de.

- Cloud foundations
- AI & machine learning
- Análisis
- Computación
- Databases & storage

- Herramientas para desarrolladores
- IoT
- Migration & modernization
- Administración
- Security, identity & compliance

Para ver todas las publicaciones, incluidas las guías, las estrategias y los patrones, consulte la AWS página de inicio de la guía prescriptiva de.

Fundamentos de la nube

Temas

- Automatice la creación de cuentas mediante el acelerador de zonas de aterrizaje en AWS
- Inventario automático de AWS los recursos en varias cuentas y regiones
- Construye una AWS landing zone que incluya MongoDB Atlas
- Configure los registros de flujo de VPC para la centralización en Cuentas de AWS
- Administre los conjuntos de AWS permisos de forma dinámica mediante Terraform
- Etiquete automáticamente las conexiones de puerta de enlace de tránsito con AWS Organizations
- Más patrones

Automatice la creación de cuentas mediante el acelerador de zonas de aterrizaje en AWS

Justin Kuskowski, Joe Behrens y Nathan Scott, Amazon Web Services

Resumen

Este patrón explica cómo utilizar el acelerador de zonas de aterrizaje en una AWS solución para implementar automáticamente una nueva Cuenta de AWS cuando un usuario autorizado envía una solicitud. Se utiliza AWS Step Functions para organizar una serie de funciones. AWS Lambda Las funciones de Lambda añaden la información de la cuenta a un repositorio de Git, inician una AWS CodePipeline canalización y validan que se aprovisionen AWS los recursos necesarios. Cuando se completa el proceso, el usuario recibe una notificación de que se ha creado la cuenta.

Si lo desea, puede integrar grupos de ID de Microsoft Entra y asignar conjuntos de AWS IAM Identity Center permisos durante el proceso de creación de la cuenta. Si su organización utiliza Microsoft Entra ID como fuente de identidad, esta característica opcional lo ayudará a administrar y configurar automáticamente el acceso a la nueva cuenta.

Requisitos previos y limitaciones

Requisitos previos

- Acceso a la cuenta de administración en AWS Organizations
- AWS Cloud Development Kit (AWS CDK) versión 2.118.0 o posterior, instalada y configurada
- La versión 3.9 o posterior de Python instalada
- AWS Command Line Interface (AWS CLI) versión 2.13.19 o posterior, instalada
- La versión 24.0.6 o posterior de Docker instalada
- Landing Zone Accelerator es AWS una solución, implementada en la cuenta de administración
- (Opcional) Microsoft Entra ID e IAM Identity Center, integrados

Limitaciones

El flujo de trabajo de creación de cuentas admite ejecuciones secuenciales para implementar una sola Cuenta de AWS. Esta limitación garantiza que el flujo de trabajo de creación de cuentas se haya completado correctamente sin tener que competir por los recursos durante una ejecución paralela.

Arquitectura

Arquitectura de destino

La siguiente imagen muestra la arquitectura de alto nivel que automatiza la creación de una nueva Cuenta de AWS mediante el Landing Zone Accelerator activado. AWS AWS Step Functions organiza la automatización. Cada tarea del flujo de trabajo de Step Functions la realizan una o más AWS Lambda funciones.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El usuario solicita una cuenta mediante la ejecución de un script de Python o mediante Amazon API Gateway.
2. El flujo de trabajo del Orquestador de creación de cuentas comienza en AWS Step Functions.
3. El flujo de trabajo actualiza el archivo `account-config.yaml` en el repositorio de código fuente. También inicia el acelerador de zonas de aterrizaje en la AWS tubería y comprueba el estado de la tubería. Esta canalización crea y configura la nueva cuenta. Para más información sobre cómo funciona, consulte Descripción general de la arquitectura del Acelerador de zonas de aterrizaje en AWS.
4. (Opcional) Cuando se completa la canalización, el flujo de trabajo comprueba si el grupo existe en Microsoft Entra ID. Si el grupo no existe en Microsoft Entra ID, el flujo de trabajo lo agrega a Microsoft Entra ID.
5. El flujo de trabajo lleva a cabo pasos adicionales que la AWS solución Landing Zone Accelerator on no puede realizar. Los pasos predeterminados incluyen:
   - Crear un alias de cuenta en AWS Identity and Access Management (IAM)
   - Adjuntar etiquetas a la cuenta en AWS Organizations
   - Creación de parámetros en el almacén de parámetros de AWS Systems Manager en función de las etiquetas asignadas a la cuenta
6. (Opcional) El flujo de trabajo asigna uno o más conjuntos de permisos al grupo de Microsoft Entra ID que especificó anteriormente. Los conjuntos de permisos permiten a los usuarios del grupo acceder a la nueva cuenta y realizar las acciones que usted configure.
7. Una AWS Lambda función ejecuta pruebas de control de calidad y de validación. Valida la creación de recursos, comprueba que se hayan creado las etiquetas y confirma que se hayan implementado los recursos de seguridad.

8. El flujo de trabajo presenta la cuenta y utiliza Amazon Simple Email Service (Amazon SES) para notificar al usuario que el proceso se ha completado correctamente.

Para más información sobre el flujo de trabajo de Step Functions, consulte el diagrama de flujo de trabajo de Step Functions en la sección Información adicional de este patrón.

Aplicaciones de Microsoft Entra ID

Si decide realizar la integración con Microsoft Entra ID, tendrá que crear las dos aplicaciones siguientes al implementar este patrón:

- Una aplicación que esté vinculada a IAM Identity Center y que garantiza que los grupos de Microsoft Entra ID estén disponibles en IAM Identity Center. En este ejemplo, esta aplicación de Microsoft Entra ID se denomina `LZA2`.
- Aplicación que permite que una función Lambda se comunique con el Microsoft Entra ID y llame a Microsoft Graph. APIs En este patrón, esta aplicación se denomina `create_aws_account`.

Estas aplicaciones recopilan datos que se utilizan para sincronizar el grupo de Microsoft Entra ID y asignar conjuntos de permisos.

Tools (Herramientas)

Servicios de AWS

- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket APIs a cualquier escala. En este patrón, se utiliza API Gateway para comprobar la disponibilidad de Cuenta de AWS los nombres, iniciar el AWS Step Functions flujo de trabajo y comprobar el estado de la ejecución de Step Functions.
- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir y aprovisionar Nube de AWS la infraestructura en código.
- AWS Control Towerle ayuda a configurar y administrar un entorno de AWS múltiples cuentas, siguiendo las mejores prácticas prescriptivas.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, AWS Lambda funciones, puntos finales de invocación HTTP que utilizan destinos de API o buses de eventos en otros. Cuentas de AWS Esta solución utiliza una EventBridge regla que inicia una función Lambda si el estado del flujo de trabajo de Step Functions cambia a `FailedTimed-out`, o. `Aborted`

- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS IAM Identity Centerle ayuda a gestionar de forma centralizada el acceso mediante el inicio de sesión único (SSO) a todas sus aplicaciones y a las de la nube. Cuentas de AWS
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos. En este patrón, AWS KMS las claves se utilizan para cifrar datos, como los datos almacenados en Amazon Simple Storage Service (Amazon S3), las variables de entorno de Lambda y los datos en Step Functions.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar múltiples cuentas Cuentas de AWS en una organización que usted crea y administra de forma centralizada.
- Amazon Simple Email Service (Amazon SES) facilita poder enviar y recibir correos electrónicos a través de los dominios y direcciones de correo electrónico propios. Cuando haya creado correctamente una cuenta nueva, recibirá una notificación a través de Amazon SES.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico. Si se produce un error durante el proceso de creación de la cuenta, Amazon SNS envía una notificación a las direcciones de email que configure.
- AWS Step Functionses un servicio de organización sin servidor que le ayuda a combinar AWS Lambda funciones y otras Servicios de AWS para crear aplicaciones esenciales para la empresa.
- AWS Systems Manager Parameter Store proporciona un almacenamiento jerárquico y seguro para la gestión de los datos de configuración y la gestión de secretos.

Otras herramientas

- awscurl automatiza el proceso de firma de las solicitudes de AWS API y le ayuda a realizar solicitudes como un comando curl estándar.
- Microsoft Entra ID, anteriormente conocido como Azure Active Directory, es un servicio de administración de identidades y acceso basado en la nube.
- Microsoft Graph lo APIs ayuda a acceder a los datos y la inteligencia en los servicios en la nube de Microsoft, como Microsoft Entra y Microsoft 365.

Repositorio de código

El código de este patrón está disponible en el GitHub lza-account-creation-workflowrepositorio.

El directorio lambda_layer contiene las siguientes capas, a las que se hace referencia en más de una función de Lambda:

- account_creation_helper: esta capa incluye los módulos para asumir funciones y comprobar su progreso. AWS Service Catalog
- boto3: esta capa incluye el AWS SDK para Python (Boto3)módulo para garantizar que tenga la última versión. AWS Lambda
- identity_center_helper: esta capa admite llamadas a IAM Identity Center.

El directorio lambda_src contiene las siguientes funciones de Lambda:

- AccountTagToSsmParameter— Esta función utiliza las etiquetas adjuntas a la cuenta para crear parámetros AWS Organizations en el almacén de parámetros. Cada parámetro comienza con el prefijo `/account/tags/`..
- AttachPermissionSet— Esta función añade un conjunto de permisos a un grupo del IAM Identity Center.
- Azure ADGroup Sync: esta función sincroniza el grupo de ID de Microsoft Entra de destino con el Centro de identidades de IAM.
- CheckForRunningProcesses— Esta función comprueba si la `AWSAccelerator-Pipeline` canalización se está ejecutando actualmente. Si la canalización está en ejecución, la función retrasa el AWS Step Functions flujo de trabajo.
- CreateAccount— Esta función utiliza AWS Service Catalog y AWS Control Tower para crear lo nuevo Cuenta de AWS.
- CreateAdditionalResources— Esta función crea los AWS recursos que Landing Zone Accelerator no administra AWS CloudFormation, como el alias y las AWS Service Catalog etiquetas de la cuenta.
- GetAccountStatus— Esta función busca el producto aprovisionado AWS Service Catalog para determinar si el proceso de creación de la cuenta se ha completado.
- GetExecutionStatus— Esta función recupera el estado de una ejecución en ejecución o completada AWS Step Functions .
- NameAvailability— Esta función comprueba si ya existe un Cuenta de AWS nombre en AWS Organizations.

- ReturnResponse— Si la creación de la cuenta se realizó correctamente, esta función devuelve el ID de la nueva cuenta. Si la creación de la cuenta no se realizó correctamente, devuelve un mensaje de error.
- RunStepFunction— Esta función ejecuta el AWS Step Functions flujo de trabajo que crea la cuenta.
- SendEmailWithSES: esta función envía correos electrónicos a los usuarios que esperan que finalice la creación de la cuenta.
- Validar el ADGroup SyncTo inicio de sesión único: esta función comprueba si los grupos de ID de Microsoft Entra especificados están sincronizados con IAM Identity Center.
- ValidateResources— Esta función valida que todas las AWS Control Tower personalizaciones se hayan ejecutado correctamente.

Prácticas recomendadas

Se recomiendan las siguientes convenciones de nomenclatura para AWS CDK:

- Inicie todos los parámetros con un prefijo `p`.
- Inicie todas las condiciones con un prefijo `c`.
- Inicie todos los recursos con un prefijo `r`.
- Inicie todos los resultados con un prefijo `o`.

Epics

Implementación de los roles de IAM para la validación y el etiquetado

Tarea	Descripción	Habilidades requeridas
Prepara el acelerador de la zona de aterrizaje para personalizarlo. AWS	1. En el repositorio de AWS códigos del Landing Zone Accelerator, cree un archivo llamado. `customizations-config.yaml` Utilice este archivo para definir las personalizaciones de la	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	solución principal. Para más información, consulte Personalización de la solución. 2. En el archivo `customizations-config.yaml` , cree una sección llamada `cloudFormationStacks` .	

Tarea	Descripción	Habilidades requeridas
Prepárese para implement ar el rol `lza-account-creation-validation` .	Ahora puede personalizar la solución para implementar el rol de IAM `lza-account-creation-validation` en todas las cuentas, excepto en la cuenta de administr ación. Este rol proporcio na a la función de Lambda `ValidateResources` acceso de solo lectura a las nuevas cuentas. 1. Descargue el account-c reation-validation-rolearch ivo.yaml de. GitHub 2. Guarde el archivo en la ubicación que se indica en la sección de plantilla s del archivo `customiza tions-config.yaml` . 3. Abra el archivo `customiza tions-config.yaml` . 4. Añada el siguiente código a la sección `cloudForm ationStacks` : Actualiza el objetivo Región de AWS según sea necesario para tu landing zone: `- deploymen tTargets: organizat ionalUnits: - Root`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	<pre>excludedAccounts:
	- Management
	
	description: IAM Role to allow Account Validation
	name: lza-account-creation-validation
	regions:
	- us-east-1
	template: cloudformation/account-creation-validation-role.yaml
	runOrder: 1
	terminationProtection: true
	parameters:
	- name: pManagementAccountId
	value: "{{ account Management }}"</pre> 5. Guarde y cierre el archivo `customizations-config.yaml` .	

Tarea	Descripción	Habilidades requeridas
Prepárese para implementar el rol `account-tagging-to-ssm-parameter-role` .	Ahora puede personalizar la solución para implementar el rol de IAM `account-tagging-to-ssm-parameter-role` en todas las cuentas, excepto en la cuenta de administración. Esta función se utiliza para crear los parámetros en AWS Systems Manager Parameter Store. 1. Descargue el archivo account-tagging-to-ssm-parameter-role.yaml de. GitHub 2. Guarde el archivo en la ubicación que se indica en la sección de plantillas del archivo `customizations-config.yaml` . 3. Abra el archivo `customizations-config.yaml` . 4. Añada el siguiente código a la sección `cloudFormationStacks` : Actualiza el objetivo Región de AWS según sea necesario para tu landing zone: `- deploymentTargets: organizationalUnits: - Root`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	<pre>excludedA
	ccounts:
	-
	Management
	descripti
	on: IAM Role to
	create SSM Parameter
	s based on Account
	Tagging
	name: lza-
	account-tagging-to-
	ssm-parameter
	regions:
	- us-
	east-1
	template:
	cloudformation/acc
	ount-tagging-to-ss
	m-parameter-role.y
	aml
	runOrder: 1
	terminati
	onProtection: true
	
	parameters:
	- name:
	pManagementAccount
	Id
	value:
	"{{ account Managemen
	t }}"</pre> 5. Guarde y cierre el archivo `customizations-config.yaml` .	

Tarea	Descripción	Habilidades requeridas
Prepárese para implement ar el rol `config-log-validation-role` .	Ahora puede personalizar la solución para implement ar el rol de IAM `config-log-validation-role` en la cuenta de archivo de registros. Esta función permite a la función `ValidateResources` Lambda acceder al bucket de Amazon S3 para acceder a las reglas de registro y acceso AWS Config . 1. Descargue el config-log-validation-rolearchivo.yaml desde. GitHub 2. Guarde el archivo en la ubicación que se indica en la sección de plantillas del archivo `customizations-config.yaml` . 3. Abra el archivo `customizations-config.yaml` . 4. Añada el siguiente código a la sección `cloudFormationStacks` : Actualiza el objetivo Región de AWS según sea necesario para tu landing zone: `- deploymentTargets: accounts: - LogArchive`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	<pre>descripti
	on: IAM Role to
	 validate Config and
	 Logs
	name:
	 lza-config-log-val
	idation-role
	regions:
	- us-
	east-1
	template:
	 cloudformation/con
	fig-log-validation-
	role.yaml
	runOrder: 1
	terminati
	onProtection: true
	
	parameters:
	- name:
	 pManagementAccount
	Id
	value:
	 "{{ account Managemen
	t }}"</pre> 5. Guarde, cierre y confirme los cambios del archivo `customizations-con fig.yaml` .	

(Opcional) Obtenga datos de Microsoft Entra ID

Tarea	Descripción	Habilidades requeridas
Cree una aplicación que permita que una función de Lambda se comunique con Microsoft Entra ID.	1. En el centro de administr ación de Microsoft Entra ID, registre la aplicación `create_aws_account` .	ID de Microsoft Entra

Tarea	Descripción	Habilidades requeridas

	Para obtener instrucciones, consulte Registro de una aplicación en la documentación de Microsoft.
	2. Siga las instrucciones en Actualización de los permisos solicitados de una aplicación en la documentación de Microsoft para configurar los siguientes permisos de Microsoft Graph para la aplicación `create_aws_account` :
	• Application.Read.All
	  • Tipo: aplicación
	  • Se requiere el consentimiento del administrador: sí
	• AppRoleAssignment.ReadWrite.Todos
	  • Tipo: aplicación
	  • Se requiere el consentimiento del administrador: sí
	• Grupo. ReadWrite.Todos
	  • Tipo: aplicación
	  • Se requiere el consentimiento del administrador: sí
	• ServicePrincipalEndpoint.Leer todo
	  • Tipo: aplicación	

Tarea	Descripción	Habilidades requeridas

	• Se requiere el consentimiento del administrador: sí
	• Sincronización. ReadWrite.Todos
	  • Tipo: aplicación
	  • Se requiere el consentimiento del administrador: sí
	• Usuario.Read
	  • Tipo: delegada
	  • Se requiere el consentimiento del administrador: no	

Tarea	Descripción	Habilidades requeridas
Recupere los valores de la aplicación `create_aws_account` .	A continuación, recupere los valores que necesita para la aplicación `create_aws_account` . 1. En el centro de administración de Microsoft Entra ID, vaya a Registros de aplicaciones y, a continuación, elija `create_aws_account` . 2. En el panel izquierdo, elija Descripción general. 3. En la página de descripción general, anote los siguientes valores: • ID de aplicación (cliente) • ID de directorio (inquilino) 4. En el panel izquierdo, en Administrar, seleccione Certificados y secretos. 5. En la página Certificados y secretos, seleccione la pestaña Secretos del cliente y anote los siguientes valores: • Valor del secreto de cliente • ID del secreto de cliente	ID de Microsoft Entra

Tarea	Descripción	Habilidades requeridas
Cree la aplicación que integra Microsoft Entra ID con IAM Identity Center.	En el centro de administración de Microsoft Entra ID, registre la aplicación `LZA2`. Para obtener instrucciones, consulte Registro de una aplicación en la documentación de Microsoft.	ID de Microsoft Entra
Recupere los valores de la aplicación `LZA2`.	A continuación, recupere los valores que necesita para la aplicación `LZA2`. 1. En el centro de administración de Microsoft Entra ID, vaya a Aplicaciones de empresa y, a continuación, elija `LZA2`. 2. En el panel izquierdo, elija Descripción general. 3. En la página de descripción general, anote los siguientes valores: • Name • ID de objeto 4. En el panel izquierdo, en Administrar, elija Manifiesto. 5. En el archivo JSON, en la sección `appRoles`, busque el rol de aplicación denominado `User`. 6. Anote el valor `id` de este rol de aplicación.	ID de Microsoft Entra

Tarea	Descripción	Habilidades requeridas

Cree un secreto.	1. En AWS CLI, introduzca el siguiente comando para crear las variables. Utilice los valores que ha recuperado de las aplicaciones `create_aws_account` y LZA2:
	
	`# Variables for create_aws_account app`
	`TENANT_ID='<Directory ID>'`
	`CLIENT_ID='<Application ID>'`
	`SECRET_ID='<Client secret ID>'`
	`SECRET_VALUE='<Client secret value>'`
	
	`# Variables for LZA2 app`
	`OBJECT_ID='<Object ID>'`
	`APP_ROLE_ID='<App role ID>'`
	`ENTERPRISE_APP_NAME='<Name>'`
	
	2. Introduzca el siguiente comando para crear un secreto con el nombre `GraphApiSecret` AWS Secrets Manager siguiente:
	
	`aws secretsmanager create-secret \`
	`--name GraphApiSecret \`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	<pre> --secret-string "{\"client_id\": \"${CLIENT_ID}\", \"tenant_id\": \"${TENANT_ID}\", \"object_id\": \"${OBJECT_ID}\", \"app_role_id\": \"${APP_ROLE_ID}\" , \"secret_value\": \"${SECRET_VALUE}\ ", \"secret_id\": \"${SECRET_ID}\"}"</pre>	
	Si necesita actualizar el secreto en el futuro, puede actualizar las variables y ejecutar el siguiente comando:	

	<pre>aws secretsmanager
	 update-secret \
	  --secret-id
	 GraphApiSecret \
	  --secret-string
	 "{\"client_id\":
	 \"${CLIENT_ID}\",
	 \"tenant_id\":
	 \"${TENANT_ID}\",
	 \"object_id\":
	 \"${OBJECT_ID}\",
	 \"app_role_id\":
	 \"${APP_ROLE_ID}\"
	, \"secret_value\":
	 \"${SECRET_VALUE}\
	", \"secret_id\":
	 \"${SECRET_ID}\"}"</pre>	

Implementar la solución

Tarea	Descripción	Habilidades requeridas

Clone el código fuente.	1. Introduzca el siguiente comando para clonar el lza-account-creation-workflowrepositorio:
	`git clone https://github.com/aws-samples/lza-account-creation-workflow`
	2. Introduzca el siguiente comando para ir al directorio `config` del repositorio clonado.
	`cd lza-account-creation-workflow/config`
		DevOps ingeniero

Actualice el archivo `deploy-config.yaml` .	1. Abra el archivo `deploy-config.yaml` . 2. Revise la plantilla y actualice los valores según sea necesario para la implementación en su AWS entorno. Por ejemplo, actualice los valores de los siguientes elementos: • `accountCreationFailure` • `accountCompletionFromEmail` • `ssoLoginUrl` • `rootEmailPrefix`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• `rootEmailDomain` 3. Si va a realizar la integración con Microsoft Entra ID, haga lo siguiente: • Establece `enableAzureADIntegration` en `true`. • Para el valor `graphApiSecretName`, introduzca el secreto que creó anteriormente (`GraphApiSecret`). 4. Guarde y cierre el archivo `deploy-config.yaml`.	

Tarea	Descripción	Habilidades requeridas

Implemente la solución en su AWS entorno.	1. Introduzca el siguiente comando:
	`cdk bootstrap <account-number>/<Region>`
	Para obtener más información, consulte Bootstrapping en la documentación. AWS CDK
	2. Introduzca el siguiente comando para sintetizar la plantilla: CloudFormation
	`cdk synth`
	Para obtener más información, consulte Configurar y realizar la síntesis de AWS CDK pilas en la AWS CDK documentación.
	3. Introduzca el siguiente comando para implementar la solución.
	`cdk deploy`
	Para obtener más información, consulte Implementar AWS CDK aplicaciones en la AWS CDK documentación.
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Note Esta solución utiliza un bucket de Amazon S3 para almacenar el código fuente de esta solución. Puede usar el script upload_to_source_bucket.py para crear un archivo del código fuente y cargar una versión actualizada.	

Opción 1: Creación de una cuenta con Python

Tarea	Descripción	Habilidades requeridas
Identifique qué argumentos usar.	Elija los argumentos que desee utilizar al ejecutar el script de Python que inicia el flujo de trabajo de Step Functions. Para obtener una lista completa de argumentos, consulte la sección Información adicional de este patrón.	AWS DevOps, Python
Inicie el script de Python.	1. Introduzca el siguiente comando para ir al repositorio clonado: `cd lza-account-creation-workflow`	DevOps ingeniero, Python

Tarea	Descripción	Habilidades requeridas
	2. Ejecute el script de Python que inicia el flujo de trabajo de Step Functions. A continuación, tiene un comando de ejemplo que incluye muestas de argumentos y valores: `python ./run-stepfunction.py \ --account-name "lza-test-01" \ --support-dl "johnsmith@example.com" \ --managed-org-unit "Workloads/Workload-1" \ --purpose "Testing new micro service" \ --force-update true \ --ad-integration "{\"CustomerAccountAdmin\": \"platform-admin\", \"CustomerAccountDev\": \"workload1-app1\"}" \ --bypass-creation true \ --tags APPLICATION=TestingMicroService` 3. Espere hasta que reciba una notificación que indique que la cuenta se ha creado correctamente.	

Tarea	Descripción	Habilidades requeridas
	Note Si el proceso de creación de la cuenta no funciona, Amazon SNS envía una notificación a las direcciones de email que defina en `accountCreationFailure` en el archivo `deploy-config.yaml`. No se notifica al solicitante de la cuenta.	

Opción 2: Creación de una cuenta con API Gateway y awscurl

Tarea	Descripción	Habilidades requeridas
Configure las variables para awscurl.	1. Introduzca el siguiente comando para ir al directorio del código fuente: `cd lza-account-creation-workflow` 2. Introduzca el siguiente comando para configurar las variables de la clave de AWS acceso. Puede copiar las variables del	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	portal de acceso AWS y, a continuación, pegarlas en un intérprete de comandos. A continuación, se muestra un ejemplo:
	`export AWS_ACCES S_KEY_ID="<id>" export AWS_SECRE T_ACCESS_KEY="<key >" export AWS_SESSI ON_TOKEN="<token>"`
	3. Ingresa el siguiente comando para configura r las Región de AWS llamadas a la API:
	`export AWS_REGION= $(aws configure get region)`
	4. Introduzca el siguiente comando para recuperar el punto final de API Gateway de la `lza-account-creation-workflow-application` CloudForm ation salida:
	`export API_GATEW AY_ENDPOINT=$(aws cloudformation describe-stacks -- stack-name "lza-acco unt-creation-workf low-application"`	

Tarea	Descripción	Habilidades requeridas
	`--query 'Stacks[*].Outputs[?OutputKey==`oApiGatewayCreateAccountEndpoint`].OutputValue' --output text)`	
Compruebe la disponibilidad de del nombre.	Introduzca el siguiente comando para comprobar que el nombre esté disponible para la Cuenta de AWS. Sustituya <AWS_ACCOUNT_NAME> por el nombre de la cuenta de destino: `awscurl --service execute-api \ --region ${AWS_REGION} \ --access_key ${AWS_ACCESS_KEY_ID} \ --secret_key ${AWS_SECRET_ACCESS_KEY} \ --security_token ${AWS_SESSION_TOKEN} \ -X POST ${API_GATEWAY_ENDPOINT}check_name?account_name=<AWS_ACCOUNT_NAME>`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Ejecute el flujo de trabajo de creación de cuentas.	1. En la carpeta raíz del repositorio clonado, abra el archivo `api_example.json` . 2. Actualice los parámetros con los valores de la configuración. `{ "account_name": "lza-test-01", "account_email": "johnsmith+lzatest01@example.com", "support_dl": "johnsmith@example.com", "managed_org_unit": "Workloads/Workload-1", "ad_integration": [{ "PermissionSetName": "CustomerAccountAdmin", "ActiveDirectoryGroupName": "platform-admin" }, { "PermissionSetName": "CustomerAccountDev", "ActiveDirectoryGroupName": "workload1-app1" }`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	<pre>],
	    "force_update":
	 "true",
	    "bypass_c
	reation": "false",
	    "account_tags": [
	        {
	            "Key":
	 "Environment",
	            "Value":
	 "Dev"
	        }, {
	            "Key":
	 "DeploymentMethod",
	            "Value":
	 "ApiGateway"
	        }
	    ]
	}</pre> 3. Guarde y cierre el archivo `api_example.json` .
	4. Introduzca el siguiente comando para iniciar el flujo de trabajo de Step Functions:
	<pre>awscurl --service
	 execute-api \
	    --data @api-exam
	ple.json \
	    --region ${AWS_REG
	ION} \
	    --access_key
	 ${AWS_ACCESS_KEY_I
	D} \
	    --secret_key
	 ${AWS_SECRET_ACCES
	S_KEY} \</pre>	

Tarea	Descripción	Habilidades requeridas

	<pre>--security_token ${AWS_SESSION_TOKEN} \
	-X POST ${API_GATEWAY_ENDPOINT}execute</pre>
	5. En el resultado del comando anterior, anote la ejecución de Step Functions de Nombre de recurso de Amazon (ARN).
	6. Si desea comprobar el estado del flujo de trabajo de Step Functions, introduzca el siguiente comando. Sustituya `<STEP_FUNCTION_EXECUTION_NAME>` por el nombre o el ARN de ejecución de Step Functions:
	<pre>awscurl --service execute-api \
	--region ${AWS_REGION} \
	--access_key ${AWS_ACCESS_KEY_ID} \
	--secret_key ${AWS_SECRET_ACCESS_KEY} \
	--security_token ${AWS_SESSION_TOKEN} \
	-X GET ${API_GATEWAY_ENDPOINT}get_execution_status?e</pre>	

Tarea	Descripción	Habilidades requeridas
	`xecution=<STEP_FUN CTION_EXECUTION_NA ME>` 7. Espere hasta que reciba una notificación que indique que la cuenta se ha creado correctamente. **Note** Si el proceso de creación de la cuenta no funciona, Amazon SNS envía una notificación a las direcciones de email que defina en `accountCr eationFai lure` en el archivo `deploy-config.yaml`. No se notifica al solicitante de la cuenta.	

(Opcional) Eliminación de la solución

Tarea	Descripción	Habilidades requeridas
Elimine objetos de los buckets de Amazon S3.	Elimine cualquier objeto de los siguientes buckets de Amazon S3:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• `lza-account-creation-work-<CDK_UNIQUE_ID>` • `lza-account-creation-workflow-src-<AWS_REGION>-<AWS_ACCOUNT>` • `lza-account-creation-workflow-<AWS_REGION>-<AWS_ACCOUNT>`	

Elimine la CloudFormation pila.	Ingresa el siguiente comando para eliminar la CloudFormation pila:
	`aws cloudformation delete-stack \ --stack-name lza-account-creation-workflow-application`
	`aws cloudformation wait stack-delete-complete \ --stack-name lza-account-creation-workflow-application`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
Elimine la canalización.	Escriba el comando siguiente para eliminar la canalización `lza-account-creation-workflow-pipeline` : `cdk destroy lza-account-creation-workflow-pipeline --force`	AWS DevOps

Recursos relacionados

- Landing Zone Accelerator activado AWS (biblioteca de AWS soluciones)
- Solución de AWS CDK problemas comunes (AWS CDK documentación)

Información adicional

Diagrama del flujo de trabajo de Step Functions

En la siguiente imagen se muestran los estados del flujo de trabajo de Step Functions.

Argumentos

Puede usar los siguientes argumentos al ejecutar el script de Python que inicia el flujo de trabajo de Step Functions.

Se requieren los siguientes argumentos:

- `account-name (-a)`(cadena): el nombre del nuevo Cuenta de AWS.
- `support-dl (-s)` (cadena): dirección de correo electrónico que recibe la notificación cuando se completa el proceso de creación de la cuenta.
- `managed-org-unit (-m)` (cadena): unidad organizativa (UO) administrada que contendrá la nueva cuenta.

Los siguientes argumentos son opcionales:

- `ad-integration (-ad)` (diccionario de cadenas): grupo de Microsoft Entra ID y conjunto de permisos asignado. A continuación, se muestra un ejemplo de cómo utilizar este argumento:

```
--ad-integration "{\"<PermissionSetName>\": \"<EntraIdGroupName>\"}"
```

- `account-email (-e)`(cadena): la dirección de correo electrónico del usuario raíz del nuevo Cuenta de AWS.

> **Note**
>
> Si no se utiliza este argumento, se generará una dirección de correo electrónico mediante los valores `rootEmailPrefix` y `rootEmailDomain` a partir del archivo `configs/deploy-config.yaml`. Si no se proporciona una dirección de correo electrónico, se generará una dirección de correo electrónico con el siguiente formato: `rootEmailPrefix+accountName@rootEmailDomain`.

- `region (-r)`(string): el Región de AWS lugar donde se implementó el flujo de trabajo de Step Functions. El valor predeterminado es `us-east-1`.
- `force-update (-f)`(cadena booleana): introdúzcala `true` AWS Service Catalog para forzar la actualización del producto aprovisionado.
- `bypass-creation (-b)` (cadena booleana): introduzca `true` para evitar añadir la cuenta al archivo `accounts-config.yaml` y evitar que se ejecute la canalización `AWSAccelerator-Pipeline`. Este argumento se suele utilizar para probar el proceso del flujo de trabajo de creación de cuentas o para ejecutar el resto de los pasos de Step Functions si se produce un error en la canalización `Landing Zone Accelerator`.
- `tags (-t)`(cadena): etiquetas adicionales que desee añadir a. Cuenta de AWS De forma predeterminada, se añaden las siguientes etiquetas: `account-name`, `support-dl` y `purpose`. A continuación, se muestra un ejemplo de cómo utilizar este argumento:

```
--tags TEST1=VALUE1 TEST2=VALUE2
```

Inventario automático de AWS los recursos en varias cuentas y regiones

Matej Macek, Amazon Web Services

Resumen

Este patrón describe un enfoque automatizado para mantener un inventario integral de AWS recursos en varias cuentas y Regiones de AWS. Está diseñado para ayudar a los ingenieros de infraestructura y seguridad a mejorar sus prácticas de administración de recursos. Se utiliza AWS Config para realizar un seguimiento de los cambios en los recursos, Amazon Athena para realizar consultas y Amazon Quick Sight para paneles interactivos. Para implementar esta solución, debe implementar una pila. AWS CloudFormation

Esta solución es similar a la presentada en Visualización de AWS Config datos con Amazon Athena y Amazon Quick Sight AWS (entrada del blog). Este patrón amplía esa solución para abordar los siguientes requisitos comunes y ofrecer los siguientes beneficios clave:

- Fundamentado en la conformidad: este enfoque puede ayudarlo a cumplir requisitos normativos como PCI DSS, NIST SP 800-53, ISO/IEC 27001, HIPAA y GDPR, entre otros, que exigen inventarios precisos de recursos.
- Marco de personalización: proporciona una base para crear paneles de Quick Sight para varios AWS recursos, de modo que pueda personalizar la solución según sus requisitos específicos.
- Mejoras impulsadas por los usuarios: este enfoque incorpora comentarios de casos de uso reales y responde a las solicitudes de una solución más completa.

Los equipos de infraestructura, seguridad y finanzas suelen enfrentarse a desafíos de visibilidad y colaboración en entornos dinámicos que cuentan con varias cuentas o regiones. Esta solución está diseñada para abordar esos desafíos y reducir significativamente el tiempo y el esfuerzo necesarios para crear y mantener un inventario de recursos. El resultado es una visión centralizada de los recursos que lo ayuda a mejorar las decisiones de asignación de recursos, identificar y mitigar los riesgos, optimizar los costos y mejorar la visibilidad y la colaboración en general. Este enfoque cierra la brecha entre las soluciones conceptuales y las necesidades de implementación reales para fines operativos, de seguridad y de conformidad.

Requisitos previos y limitaciones

Requisitos previos

- La siguiente Cuentas de AWS activa:
  - Cuenta de administración: cuenta centralizada para facturar, crear cuentas y controlar el acceso en toda la organización
  - Cuenta de auditoría: centro unificado para la supervisión de la seguridad, controles de conformidad y notificaciones de desviaciones
  - Cuenta de archivo de registros: cuenta centralizada para almacenar y analizar los datos recopilados
- En la cuenta de auditoría, un AWS Config agregador que recopila y agrega datos de configuración de las cuentas y regiones de destino
- En la cuenta de archivo de registros, configure lo siguiente:
  - Un depósito de Amazon Simple Storage Service (Amazon S3) en el que se almacenan los datos del agregador AWS Config
  - Una suscripción a Amazon Quick
  - Una conexión autorizada entre Quick Sight y Amazon Athena
  - Permisos para acceder al bucket de Amazon S3 mediante una consulta de Athena
- AWS Command Line Interface (AWS CLI), instalado y configurado
- Permisos para implementar una CloudFormation pila que aprovisione los siguientes recursos:
  - Una AWS Lambda función
  - Una configuración de notificaciones de Amazon S3
  - Base de datos, tablas y vistas de Athena
  - Conjuntos de datos y fuentes de datos de Quick Sight
- Permisos para ejecutar automatizaciones en AWS Systems Manager
- Permisos para acceder a Quick

Limitaciones

- La solución se basa en AWS Config. AWS Config por lo general, registra los cambios de configuración de los recursos inmediatamente después de que se detecta un cambio o con la frecuencia que usted especifique. Aunque el sistema hace todo lo posible porque sea así, a veces puede tardar más tiempo.

- Esta solución solo rastrea los tipos de recursos AWS Config compatibles.
- La solución no realiza un seguimiento del inventario de recursos de otros proveedores de nube o en entornos en las instalaciones.
- Algunos Servicios de AWS no están disponibles en todos Regiones de AWS. Para conocer la disponibilidad regional, consulta la página de límites y cuotas del servicio en la AWS documentación y elige el enlace correspondiente al servicio.

Arquitectura

El siguiente diagrama muestra un proceso simplificado para recopilar, organizar, analizar y visualizar los datos de configuración y conformidad de varias cuentas de una organización. AWS

En el diagrama, se muestra el siguiente flujo de trabajo:

1. De forma periódica, el AWS Config agregador recopila datos de configuración y conformidad sobre los recursos de las cuentas y regiones de destino y, a continuación, entrega los datos al depósito de Amazon S3 de la cuenta de archivo de registros.
2. Al añadir nuevos AWS Config datos al bucket de Amazon S3, se invoca una AWS Lambda función.
3. La función de Lambda divide los datos configurando claves con valores que corresponden a la región y la fecha de cada archivo de la instantánea. Esto ayuda a consultar y procesar de AWS Glue manera eficiente los datos de configuración y conformidad.
4. Amazon Athena utiliza un AWS Glue esquema para ejecutar consultas SQL en los datos almacenados en el bucket de Amazon S3. Utiliza los metadatos del esquema AWS Glue para comprender la estructura de los datos.
5. Las vistas de Athena definen y extraen los conjuntos de datos de destino.
6. Los paneles de Quick Sight le ayudan a visualizar y analizar los conjuntos de datos.

Tools (Herramientas)

Servicios de AWS

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en Cuentas de AWS todo el mundo. Regiones de AWS
- AWS Configproporciona una vista detallada de los recursos que tiene Cuenta de AWS y de cómo están configurados. Le ayuda a identificar cómo se relacionan los recursos entre sí y cómo han cambiado sus configuraciones a lo largo del tiempo. Un AWS Config agregador recopila datos AWS Config de configuración y conformidad de varias Cuentas de AWS regiones.
- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos. Este patrón utiliza un catálogo de AWS Glue datos y un registro de esquemas.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar múltiples cuentas Cuentas de AWS en una organización que puede crear y administrar de forma centralizada.
- Amazon Quick Sight es un servicio de inteligencia empresarial (BI) que le ayuda a transformar los datos sin procesar en información significativa mediante visualizaciones, paneles e informes interactivos. Quick Sight es un componente fundamental de Amazon Quick.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Systems Manager lo ayuda a administrar las aplicaciones y la infraestructura que se ejecutan en la Nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo necesario para detectar y resolver problemas operativos y le ayuda a administrar sus AWS recursos de forma segura y a escala. AWS Systems Manager La automatización simplifica las tareas habituales de mantenimiento, implementación y corrección para muchas personas. Servicios de AWS

Repositorio de código

La AWS CloudFormation plantilla para este patrón está disponible en el repositorio de AWS Config visualización GitHub . Esta CloudFormation plantilla implementa un manual de AWS Systems Manager automatización que se configura AWS Config para su uso con Amazon Athena. Esta

automatización se prepara AWS Glue para conectarse con el bucket de Amazon S3 designado, crea vistas en Amazon Athena y configura Quick Sight para la visualización del panel.

Prácticas recomendadas

- Le recomendamos que siga las prácticas recomendadas que se indican en la sección AWS Control Tower sobre AWS cómo configurar y administrar un AWS entorno seguro y con múltiples cuentas, siguiendo la guía prescriptiva.
- Le recomendamos que cree un AWS Config agregador que recopile los datos de configuración y conformidad de toda la organización. AWS Para obtener más información, consulte Agregación de datos multirregional y multicuenta en la documentación. AWS Config
- Antes de implementar esta solución, le recomendamos que revise la información de precios actual de Amazon S3 AWS Config, Athena y Quick.

Epics

Implemente la pila CloudFormation

Tarea	Descripción	Habilidades requeridas
Descarga la CloudFormation plantilla.	Descarga la plantilla Config-QuickSight CloudFormation - Visualization-SSM-Automation.yaml.	Administrador de AWS, administrador de la nube, DevOps ingeniero
Modifique la CloudFormation plantilla.	Complete este paso solo si está utilizando AWS Control Towery AWS Config está gestionado por AWS Control Tower. Debe modificar la CloudFormation plantilla. 1. Inicie sesión en la cuenta de administración de . 2. Abra la consola de AWS Organizations.	DevOps ingeniero, administrador de AWS

Tarea	Descripción	Habilidades requeridas

	3. Vaya a la página Configuración. En esta página se muestran detalles sobre la organización, incluido el ID de la organización.
	4. Copie el ID de organización.
	5. En el editor de texto que prefieras, abre el archivo Config- QuickSight -Visualization-SSM-Automation.yaml.
	6. Busque la siguiente línea:
	`return re.match( '^AWSLogs/(\d+)/Config/([\w-]+)/(\d+)/(\d+)/(\d+)/ConfigSnapshot/[^\\\]+$', object_key)`
	7. Sustituya esta línea por la siguiente, donde `<ORGANIZATION_ID>` es el ID que copió anteriormente:
	`return re.match( '^<ORGANIZATION_ID>/AWSLogs/(\d+)/Config/([\w-]+)/(\d+)/(\d+)/(\d+)/ConfigSnapshot/[^\\\]+$', object_key)`	

Tarea	Descripción	Habilidades requeridas
	8. Guarda y cierra el archivo Config- QuickSight -Visualization-SSM-Automation.yaml.	
Crea una CloudFormation pila.	Sigue las instrucciones de Crear una pila desde la CloudFormation consola. Tenga en cuenta lo siguiente: 1. Elija Cargar un archivo de plantilla y seleccione el archivo YAML que ha descargado. 2. En Nombre de pila, escriba `Config-QuickSight-Visualization-SSM-Automation` . 3. Seleccione Enviar.	Administrador de AWS, administrador de la nube, DevOps ingeniero

Ejecución de la automatización en Systems Manager

Tarea	Descripción	Habilidades requeridas
Encuentre su nombre de usuario rápido.	1. Abre la consola rápida. 2. Abra el menú del perfil. 3. Anote el nombre de usuario. Necesitará este valor más tarde.	Administrador de AWS, administrador de la nube, DevOps ingeniero
Busque el nombre del canal de entrega y el nombre del bucket de Amazon S3.	1. En AWS CLI, introduzca el siguiente comando:	Administrador de AWS, administrador de la nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	``` aws configservice describe-delivery- channels ``` 2. Anote el nombre del bucket de Amazon S3 y el nombre de su canal de entrega de AWS Config. Necesitará estos valores más adelante.	

Tarea	Descripción	Habilidades requeridas
Ejecute la automatización en Systems Manager.	1. Abra la Consola de AWS Systems Manager. 2. En el panel de navegación, elija Documentos. 3. Seleccione Owned by me (De mi propiedad). 4. Elija Config- QuickSight - Visualization. 5. Elija Ejecutar automatiz ación. 6. En la sección Parámetros de entrada, proporcione los valores para los parámetros siguientes: • `ConfigDeliveryChan nelName` — Introduzc a el nombre de su canal de AWS Config entrega. Este parámetro es obligatorio. • `ConfigS3BucketLoca tion` — Introduzca el nombre del depósito de Amazon S3 en el que almacena los datos AWS Config de configura ción. Este parámetro es obligatorio. • `QuickSightUserName` — Introduzca un nombre de usuario que tenga acceso administr	Administrador de AWS, administrador de la nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	ativo a Quick. Este parámetro es obligatorio. • `AutomationAssumeRole` — El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Este parámetro es opcional. Deje en blanco este parámetro. • `DeleteConfigVisualization` — Elige. `false` 7. Elija Ejecutar.	

Visualice los datos en Quick Sight

Tarea	Descripción	Habilidades requeridas
Actualice los datos.	Para programar las actualizaciones de los conjuntos de datos de acuerdo con sus requisitos específicos, siga las instrucciones de la sección Actualización de datos de SPICE.	Administrador, DevOps ingeniero y administrador de la nube de AWS
Cree un análisis de .	Para crear un panel en Quick Sight que le ayude a visualizar	Administrador de Quick Suite

Tarea	Descripción	Habilidades requeridas
	los recursos, siga las instrucciones que se indican en Cómo iniciar un análisis en Quick Sight.	
Cree un panel de control.	1. Cuando termine de modificar el análisis de Quick Sight, siga las instrucciones de Publicación de paneles para crear un panel. Un panel es un análisis que puede compartir con otros usuarios de Quick. 2. Sigue las instrucciones que se indican en Otorgar acceso a un panel para compartirlo con los usuarios de Quick a los que te dirijas.	Administrador de Quick Suite

(Opcional) Limpieza

Tarea	Descripción	Habilidades requeridas
Elimine los recursos creados por la automatización de Systems Manager.	1. Abra la Consola de AWS Systems Manager. 2. En el panel de navegación, elija Documentos. 3. Seleccione Owned by me (De mi propiedad). 4. Elija Config- QuickSight - Visualization.	Administrador de AWS, administrador de la nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	5. Elija Ejecutar automatiz ación. 6. En la sección Parámetros de entrada, en el parámetro `DeleteConfigVisual ization` , especifique `true`. 7. Elija Ejecutar.	
Elimine la CloudFormation pila.	Para eliminar los recursos de la `Config-QuickSight-Visualization-SSM-Automation` pila, sigue las instrucciones de Eliminar una pila de la CloudFormation consola.	Administrador de AWS, administrador de la nube, DevOps ingeniero

Resolución de problemas

Problema	Solución
Amazon Quick está intentando conectarse a esa región `us-east-1` Región de AWS, pero no está permitida la creación de recursos en esa región.	Una política de control de servicios restringe tu suscripción a Amazon Quick en esta región. En la política de control de servicios, especifiq ue el objetivo manualmente Región de AWS. Sustituya `<REGION_ID>` por el identificador de región correspondiente: `https://<REGION_ID>.quicksight.aws.a mazon.com/sn/start/dashboards` A continuación, se muestra un ejemplo:

Problema	Solución
	`https://eu-central-1.quicksight.aws.amazon.com/sn/start/dashboards`
En Amazon Athena, aparece el siguiente mensaje: `Before you run your first query, you need to set up a query result location in Amazon S3.`	Asegúrese de haber preparado un bucket de Amazon S3 en el que almacenará los resultados de las consultas de Amazon Athena. A continuación, siga las instrucciones de Especificación de una ubicación de resultados de consulta mediante la consola de Athena.

Recursos relacionados

AWS documentación

- AWS Config documentación
- Documentación de Amazon Quick

AWS entrada de blog

- Automatice la visualización de AWS Config datos con AWS Systems Manager
- Cómo registrar periódicamente los cambios en la configuración de los recursos con AWS Config

Otros recursos

- Centro de aprendizaje comunitario Amazon Quick
- Galería de la comunidad Amazon Quick

Construye una AWS landing zone que incluya MongoDB Atlas

Igor Alekseev, Amazon Web Services

Anuj Panchal, MongoDB

Resumen

Este patrón describe cómo construir una zona de AWS landing que esté integrada con un clúster de MongoDB Atlas. La infraestructura se implementa automáticamente mediante un script de Terraform.

Un AWS entorno multicuenta bien estructurado, denominado landing zone, ofrece escalabilidad y seguridad, especialmente para las empresas. Sirve de base para la rápida implementación de cargas de trabajo y aplicaciones, y permite garantizar la confianza en la seguridad y la infraestructura. La creación de una zona de aterrizaje requiere una cuidadosa consideración de los factores técnicos y empresariales, incluida la estructura de la cuenta, las redes, la seguridad y la gestión del acceso. Estas consideraciones deben coincidir con los objetivos empresariales y de crecimiento futuro de su organización.

Los casos de uso de este patrón incluyen lo siguiente.

- Plataformas SaaS y PaaS empresariales: las aplicaciones de software como servicio (SaaS) multiusuario y las plataformas de plataforma como servicio (PaaS) que se ejecutan AWS pueden utilizar esta configuración para ayudar a proporcionar un acceso seguro y privado a MongoDB Atlas sin exponer los datos a través de la Internet pública.
- Sectores altamente regulados: las cargas de trabajo bancarias, de servicios financieros, sanitarias y gubernamentales que requieren el estricto cumplimiento de normas como la Ley de Portabilidad y Responsabilidad de los Seguros Médicos (HIPAA), el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS), los Controles de Sistemas y Organizaciones (2) y el Reglamento General de Protección de Datos (GDPRSOC2) se benefician de:
  - La conectividad privada y cifrada mediante AWS PrivateLink
  - Una alta disponibilidad de conjuntos de réplicas de MongoDB en multi-AZ
- AI/ML Cargas de trabajo seguras: las canalizaciones de entrenamiento o inferencia en Amazon Bedrock, SageMaker Amazon AI o modelos de IA personalizados pueden recuperar y almacenar datos de forma segura en MongoDB Atlas over. PrivateLink
- Recuperación ante desastres y continuidad empresarial: el diseño de multi-AZ garantiza que ningún error en las zonas de disponibilidad interrumpa las cargas de trabajo. Una réplica de Atlas

distribuida en todas las zonas de disponibilidad garantiza la conmutación por error automática. Esto es fundamental para servicios permanentes, como las aplicaciones de tecnología financiera (fintech), la banca digital o la supervisión del sector sanitario.

Requisitos previos y limitaciones

Requisitos previos

- El propietario de la organización tiene acceso a MongoDB Atlas para crear claves de API de Atlas. Para obtener información sobre este requisito, consulte Administración del acceso a la organización en la documentación de MongoDB.
- Una Cuenta de AWS activa.
- Terraform, instalado y configurado.
- Un clúster de MongoDB Atlas, creado con la versión 6.0 o posterior de MongoDB.
- Conocimientos de MongoDB y MongoDB Atlas. Para obtener más información, consulte la documentación de MongoDB Atlas.

Limitaciones

- Algunos no están disponibles en todos. Servicios de AWS Regiones de AWS Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

El siguiente diagrama de arquitectura de referencia ilustra la configuración de despliegue de una AWS landing zone que está integrada con un punto final privado de MongoDB Atlas. Esta arquitectura de referencia demuestra cómo establecer una zona de AWS aterrizaje segura, escalable y de alta disponibilidad integrada con MongoDB Atlas. Al combinar las AWS mejores prácticas, como el despliegue en zonas de disponibilidad múltiples, los controles de seguridad con privilegios mínimos y la conectividad privada, este diseño permite a las organizaciones proporcionar un entorno sólido para las aplicaciones modernas.

Esta arquitectura se compone de lo siguiente:

VPC

- Una nube privada virtual (VPC) que se extiende por las tres zonas de disponibilidad.
- La VPC se subdivide en subredes alineadas con cada zona de disponibilidad. Estas subredes distribuyen las cargas de trabajo para lograr una alta disponibilidad.

Acceso a Internet

- Una puerta de enlace de Internet proporciona conectividad saliente a Internet para los recursos que la necesitan, como los hosts de aplicaciones o de bastión.
- Las subredes públicas pueden albergar puertas de enlace NAT, que permiten que las cargas de trabajo de las subredes privadas descarguen actualizaciones, parches y otros paquetes necesarios sin exponerlos directamente a la red pública de Internet.

Subredes privadas y tablas de enrutamiento

- Los componentes de la aplicación, microservicios u otros recursos confidenciales suelen estar en subredes privadas.
- Las tablas de enrutamiento dedicadas controlan los flujos de tráfico. Los enrutamientos dirigen el tráfico saliente desde las subredes privadas a las puertas de enlace NAT para conseguir un acceso seguro a Internet solo desde la salida.
- Las solicitudes entrantes de Internet fluyen a través de equilibradores de carga elásticos o hosts bastión (si se utilizan) en subredes públicas; a continuación, se enrutan adecuadamente a los recursos de subredes privadas.

Conectividad con MongoDB Atlas a través de PrivateLink

- La arquitectura utiliza PrivateLink (a través de un punto final de VPC) conectarse de forma segura a MongoDB Atlas sin exponer sus datos a la Internet pública.
- Las solicitudes permanecen en la red troncal AWS . Los datos en tránsito se benefician del PrivateLink cifrado y nunca se enrutan a través de la Internet pública.
- La VPC dedicada de MongoDB Atlas aloja sus nodos principal y secundario y proporciona un entorno seguro y aislado para su clúster de base de datos administrado.

Multi-AZ deployment (Implementación Multi-AZ)

- Los componentes críticos de la infraestructura (como las puertas de enlace NAT y las subredes de aplicaciones) se distribuyen en, al menos, tres zonas de disponibilidad. Si una zona de disponibilidad sufre una interrupción, esta arquitectura garantiza que las cargas de trabajo de las zonas de disponibilidad restantes permanezcan operativas.
- De forma predeterminada, MongoDB Atlas ofrece una alta disponibilidad a través de conjuntos de réplicas y garantiza que la capa de base de datos siga teniendo tolerancia a errores. La infraestructura crítica se distribuye en al menos tres zonas de disponibilidad para garantizar su resiliencia.

Tools (Herramientas)

Servicios de AWS

- AWS Secrets Manager lo ayuda a reemplazar las credenciales codificadas en su código, incluidas contraseñas, con una llamada a la API para recuperar el secreto mediante programación.

Otros productos y herramientas

- MongoDB Atlas es una base de datos como servicio (DbaaS) completamente administrada para implementar y administrar bases de datos de MongoDB en la nube.
- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube. En este patrón, se utiliza Terraform para ejecutar un script que facilite el despliegue de los recursos necesarios en AWS MongoDB Atlas.

Repositorio de código

El código de este patrón está disponible en el repositorio Atlas AWS Landing Zone y en MongoDB. GitHub

Epics

Finalización de las tareas de descubrimiento y evaluación

Tarea	Descripción	Habilidades requeridas
Identifique a las partes interesadas principales.	Identifique a todas las partes interesadas clave y a los	Líder de migración

Tarea	Descripción	Habilidades requeridas
	miembros del equipo que participan en el proyecto de la zona de aterrizaje. Esto podría incluir roles como los siguientes: • Administradores de bases de datos () DBAs • DevOps ingenieros • Desarrolladores de aplicaciones • Arquitectos de aplicaciones	
Cree un esquema estructural.	Cree un plano que describa la estructura deseada de su landing zone AWS y de la que dispone de MongoDB Atlas.	Líder de migración
Cree un plan de arquitectura.	Trabaje con los arquitectos de las aplicaciones para analizar los requisitos y diseñar una arquitectura resiliente y tolerante a errores. Este patrón proporciona una plantilla de arquitectura inicial para su referencia. Puede personalizar esta plantilla para adaptarla a las necesidades de seguridad e infraestructura de su organización.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Planifique la configuración y la implementación.	Determine, con todas las partes interesadas, cómo se implementará la arquitectura, cómo se implementarán las medidas de seguridad y cualquier otro aspecto para garantizar que todo se alinea con los intereses de la organización y del equipo solicitante.	Líder de migración, ingeniero y administrador de bases de datos DevOps

Configuración del entorno de MongoDB Atlas

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Clona el código del GitHub repositorio ejecutando el comando: `git clone https://github.com/mongodb-partners/AWS-MongoDB-Atlas-Landing-Zone`	Desarrollador de aplicaciones, DevOps ingeniero
Obtenga el ID de su organización de Atlas.	1. Si no tiene una cuenta de MongoDB Atlas, regístrese para obtener una. 2. Siga los pasos de la documentación de MongoDB para crear una organización. 3. Copie el ID de organización.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Genere claves de API a nivel de organización de Atlas.	Para generar las claves de API a nivel de organización en Atlas, siga las instrucciones de la documentación de MongoDB.	Administrador de base de datos
Crea un secreto en AWS Secrets Manager.	Guarde las claves de la API de MongoDB Atlas generadas en el paso anterior como un secreto clave-valor en Secrets Manager. Para obtener instrucciones, consulte la documentación de Secretes Manager.	DevOps ingeniero
Seleccione la capa del clúster de Atlas.	Siga las instrucciones de la documentación de MongoDB para seleccionar la capa del clúster de Atlas correcta.	Administrador de base de datos

Configure los AWS entornos

Tarea	Descripción	Habilidades requeridas
Modifique el script de Terraform.	En tu copia local del GitHub repositorio, actualiza el nombre secreto en el modules/mongodb-atlas/mainarchivo.tf (línea 12) para que Terraform pueda recuperar las credenciales de Secrets Manager durante el despliegue.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Cree un identificador de clave de AWS acceso y una clave secreta.	Para crear tu identificador de clave de AWS acceso y tu clave secreta, sigue las instrucciones del artículo de AWS Re:post ¿Cómo se crea una clave de AWS acceso? Se recomienda asignar políticas con los privilegios mínimos necesarios, pero en este caso, seleccione la política de `AdministratorAccess` . Tras crear la clave de acceso, consulte las prácticas recomendadas de seguridad de IAM para obtener información sobre las prácticas recomendadas para gestionar las claves de acceso.	DevOps ingeniero
Asigne las direcciones IP elásticas-	Asigne al menos dos direcciones IP elásticas IDs. Para obtener instrucciones, consulte la documentación de Amazon Virtual Private Cloud (Amazon VPC).	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Cree un bucket de S3 para almacenar el estado de su implementación de Terraform siguiendo las instrucciones de la documentación de Amazon Simple Storage Service (Amazon S3).	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Actualice el bucket de S3 para su almacenamiento.	Actualice la información del bucket de S3 en su versión local de environments/development/main.tf para que coincida con el nombre y la región del bucket que creó en el paso anterior y especifique un key prefijo. Por ejemplo: `terraform { ... backend "s3" { bucket = "startup-name-product-terraform" key = "network/dev" region = "ap-southeast-1" } }` En este ejemplo, puede configurar Terraform para que use la clave de prefijo `network/dev` para organizar el archivo de estado de Terraform. Puede cambiar el valor a `prod` o `staging` para que coincida con el entorno que desea crear. Para obtener información acerca del uso de varios entornos, consulte el último paso de esta sección.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Para obtener más informaci ón sobre los prefijos de claves de Amazon S3, consulte Organizar objetos con prefijos en la documentación de Amazon S3.	
Establezca las variables de Terraform.	La zona de aterrizaje de muestra define los valores de las variables de entrada mediante los archivos de definición de variables de Terraform. El archivo de variables se encuentra en environments/ development/variables.tf. Puede establecer los valores de las variables en el archivo environments/development/te rraform.tfvars. Configure estas variables como se describe en el archivo Léame del repositor io. GitHub	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Configure las variables de entorno.	Si planea ejecutar el script de Terraform en su máquina local, configure las siguientes variables de entorno: • `AWS_ACCESS_KEY_ID` : identificador de clave de AWS acceso • `AWS_SECRET_ACCESS_KEY` : clave de acceso AWS secreta • `AWS_DEFAULT_REGION` : Región de AWS • `TF_LOG`: nivel de registro de Terraform (`DEBUG` o `INFO`) Para obtener más información sobre la configuración de variables de entorno, consulte la documentación de AWS Command Line Interface (AWS CLI).	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Compruebe las configuraciones de VPC.	Para seguir las prácticas recomendadas por AWS, configure los ajustes de la VPC y la subred CIDRs, las puertas de enlace NAT, las rutas y las tablas de rutas en el script Terraform para satisfacer las necesidades de su organización. Para obtener información específica, consulta el archivo Léame del repositorio. GitHub	DevOps ingeniero
Etiquetar recursos de .	Puede etiquetar sus AWS recursos para supervisarlos cuando se desplieguen mediante el script Terraform. Para ver ejemplos, consulta el archivo Léame del GitHub repositorio. Para obtener información sobre la supervisión de los recursos mediante etiquetas de coste, uso, etc., consulte Activar etiquetas de asignación de costes definidas por el usuario en la AWS Billing documentación.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Utilice varios entornos.	El GitHub repositorio proporciona una carpeta de `development` entorno. También puede añadir sus propios entornos en la carpeta de entornos. Para añadir un entorno, copie la carpeta `development` en una nueva carpeta (por ejemplo, `prod` o `staging`) situada en `environments`. A continuación, puede actualizar el archivo `terraform.tfvars` con el nuevo valor.	DevOps ingeniero

Implementación de la zona de aterrizaje

Tarea	Descripción	Habilidades requeridas
Inicialice el directorio de trabajo de Terraform.	Para iniciar el directorio de trabajo y descargar los paquetes necesarios, ejecute el comando: `terraform init`	DevOps ingeniero
Cree un plan de ejecución.	Para crear un plan de ejecución y visualizar los cambios que Terraform realizará en su infraestructura, ejecute el comando:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`terraform plan`	
Implemente los cambios.	Para implementar los cambios en su infraestructura tal como se describe en el código, ejecute el comando: `terraform apply`	DevOps ingeniero
Valide la implementación.	Valide los componentes que Terraform creó o modificó en su infraestructura. Para probar la configuración, aprovisione un recurso informático (por ejemplo, una EC2 instancia o AWS Lambda función de Amazon) en la VPC o adjunto a ella.	DevOps ingeniero, desarrollador de aplicaciones

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Elimine recursos.	Cuando haya terminado las pruebas, ejecute el siguiente comando para eliminar los recursos que Terraform haya implementado en su infraestructura: `terraform destroy`	DevOps ingeniero

Recursos relacionados

Detectar y evaluar

- Consejos administrativos para la configuración de la landing zone (AWS Control Tower documentación)
- Expectativas para la configuración de la zona de aterrizaje (AWS Control Tower documentación)
- Mejores prácticas para las actualizaciones de las zonas de landing zone (AWS Control Tower documentación)

Configuración del Atlas y los entornos de MongoDB AWS

- Obtener MongoDB Atlas (AWS Marketplace)
- Memoria (documentación de MongoDB Atlas)
- Ejemplo de dimensionamiento con conjuntos de datos de muestra de Atlas (documentación de MongoDB Atlas)
- Ejemplo de dimensionamiento para aplicaciones móviles (documentación de MongoDB Atlas)
- Tráfico de red (documentación de MongoDB Atlas)
- Escalado automático de clústeres (documentación de MongoDB Atlas)
- Plantilla de dimensionamiento de Atlas (documentación de MongoDB Atlas)
- Configurar un emparejamiento de red (documentación de MongoDB Atlas)
- Puntos de conexión privados en Atlas (documentación de MongoDB Atlas)
- Cifrado en el nivel de campo del cliente (documentación de la base de datos de MongoDB)
- Cifrado automático (documentación de la base de datos de MongoDB)
- Selección de un nivel de clúster (documentación de MongoDB Atlas)

Implementación de la zona de aterrizaje

- Terraform en AWS (documento técnico sobre CI/CD para redes 5G en AWS)
- MongoDB Atlas con Terraform (documentación de MongoDB)

Configure los registros de flujo de VPC para la centralización en Cuentas de AWS

Benjamin Morris y Aman Kaur Gandhi, Amazon Web Services

Resumen

En una nube privada AWS virtual (VPC), la función de registros de flujo de la VPC puede proporcionar datos útiles para la resolución de problemas operativos y de seguridad. Sin embargo, existen limitaciones en cuanto al uso de los registros de VPC Flow en entornos multicuenta. En concreto, no se admiten los registros de flujos entre cuentas de Amazon CloudWatch Logs. En su lugar, puede centralizar los registros configurando un bucket de Amazon Simple Storage Service (Amazon S3) con la política de bucket adecuada.

> **Note**
>
> En este patrón se detallan los requisitos para enviar los registros de flujo a una ubicación centralizada. Sin embargo, si también desea que los registros estén disponibles localmente en las cuentas de los miembros, puede crear varios registros de flujo para cada VPC. Los usuarios que no tengan acceso a la cuenta de archivo de registros pueden ver los registros de tráfico para solucionar los problemas que tengan. Como alternativa, puede configurar un registro de flujo único para cada VPC que envíe registros a CloudWatch Logs. A continuación, puede usar un filtro de suscripción a Amazon Data Firehose para reenviar los registros a un bucket de S3. Para obtener más información, consulte la sección Recursos relacionados.

Requisitos previos y limitaciones

Requisitos previos

- Una activa Cuenta de AWS
- Una AWS Organizations organización con una cuenta que se usa para centralizar los registros (por ejemplo, Log Archive)

Limitaciones

Si utilizas la clave administrada AWS Key Management Service (AWS KMS) `aws/s3` para cifrar tu depósito central, no recibirá los registros de otra cuenta. En su lugar, verá un código de error 400 `Unsuccessful` con un mensaje como `"LogDestination: <bucketName> is undeliverable"` para el `ResourceId` indicado. Esto se debe a que las claves AWS administradas de una cuenta no se pueden compartir entre cuentas. La solución consiste en utilizar el cifrado gestionado de Amazon S3 (SSE-S3) o una clave gestionada por el AWS KMS cliente que pueda compartir con las cuentas de los miembros.

Arquitectura

Arquitectura de destino

En el siguiente diagrama se implementan dos registros de flujo para cada VPC. Una de ellas envía los registros a un grupo de CloudWatch registros local. El otro envía los registros a un bucket de S3 en una cuenta de registro centralizada. La política de bucket permite al servicio de entrega de registros escribir registros en el bucket.

> **Note**
>
> A partir de noviembre de 2023, AWS ahora es compatible con la clave de condición aws: SourceOrg ID. Esta condición le permite denegar la escritura en el depósito centralizado a cuentas ajenas a su AWS Organizations organización.

Automatización y escala

Cada VPC está configurada para enviar registros al bucket de S3 en la cuenta de registro central. Use una de las siguientes soluciones de automatización para asegurarse de que los registros de flujo estén configurados correctamente:

- CloudFormation StackSets
- AWS Control Tower Generador de cuentas para Terraform (AFT)
- Una AWS Config regla con corrección

Tools (Herramientas)

Herramientas

- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas y aplicaciones Servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS. Este patrón utiliza la característica Registros de flujo de la VPC para capturar información acerca del tráfico IP entrante y saliente de las interfaces de red de en su VPC.

Prácticas recomendadas

El uso de la infraestructura como código (IaC) puede simplificar en gran medida el proceso de implementación de los registros de VPC Flow. Al resumir las definiciones de implementación de la VPC para incluir una construcción de recursos de registro de flujo, se implementará VPCs automáticamente con los registros de flujo. Esto se demuestra en la siguiente sección.

Registros de flujo centralizados

Ejemplo de sintaxis para agregar registros de flujo centralizados a un módulo de VPC en HashiCorp Terraform: este código crea un registro de flujo que envía registros desde una VPC a un bucket S3 centralizado. Tenga en cuenta que este patrón no incluye la creación del bucket de S3. Para ver las instrucciones de política de bucket recomendadas, consulte la sección de Información adicional.

```
variable "vpc_id" { type = string }
locals { custom_log_format_v5 = "$${version} $${account-id} $${interface-id} $
${srcaddr} $${dstaddr} $${srcport} $${dstport} $${protocol} $${packets} $${bytes}
 $${start} $${end} $${action} $${log-status} $${vpc-id} $${subnet-id} $${instance-
id} $${tcp-flags} $${type} $${pkt-srcaddr} $${pkt-dstaddr} $${region} $${az-id} $
${sublocation-type} $${sublocation-id} $${pkt-src-aws-service} $${pkt-dst-aws-service}
 $${flow-direction} $${traffic-path}" }
resource "aws_flow_log" "centralized_flow_log" {
  log_destination      = "arn:aws:s3:::centralized-vpc-flow-logs-
<log_archive_account_id>" # Optionally, a prefix can be added after the ARN.
  log_destination_type = "s3"
  traffic_type         = "ALL"
  vpc_id               = var.vpc_id
  log_format           = local.custom_log_format_v5 # If you want fields from VPC Flow
 Logs v3+, you will need to create a custom log format.
```

```
}
```

Para obtener más información sobre el formato de registro personalizado, consulte la documentación de Amazon VPC.

Registros de flujo locales

Ejemplo de sintaxis para agregar registros de flujo locales a un módulo de VPC en Terraform con los permisos necesarios: este código crea un registro de flujo que envía registros desde una VPC a un grupo de registros local. CloudWatch

```
data "aws_region" "current" {}
variable "vpc_id" { type = string }
resource "aws_iam_role" "local_flow_log_role" {
  name = "flow-logs-policy-${var.vpc_id}"
  assume_role_policy = <<EOF
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Principal": {"Service": "vpc-flow-logs.amazonaws.com"},
      "Action": "sts:AssumeRole"
  }]
}
EOF
}
resource "aws_iam_role_policy" "logs_permissions" {
  name = "flow-logs-policy-${var.vpc_id}"
  role = aws_iam_role.local_flow_log_role.id
  policy = <<EOF
{
  "Version": "2012-10-17",
  "Statement": [{
      "Action": ["logs:CreateLog*", "logs:PutLogEvents", "logs:DescribeLog*",
 "logs:DeleteLogDelivery"],
      "Effect": "Allow",
      "Resource": "arn:aws:logs:${data.aws_region.current.name}:*:log-group:vpc-flow-
logs*"
  }]
}
EOF
}
resource "aws_cloudwatch_log_group" "local_flow_logs" {
```

```
  name              = "vpc-flow-logs/${var.vpc_id}"
  retention_in_days = 30
}
resource "aws_flow_log" "local_flow_log" {
  iam_role_arn    = aws_iam_role.local_flow_log_role.arn
  log_destination = aws_cloudwatch_log_group.local_flow_logs.arn
  traffic_type    = "ALL"
  vpc_id          = var.vpc_id
}
```

Epics

Implemente la infraestructura de registros de VPC Flow

Tarea	Descripción	Habilidades requeridas
Determine la estrategia de cifrado y cree la política para el bucket de S3 central.	El depósito central no admite la AWS KMS `aws/s3` clave, por lo que debes usar SSE-S3 o una clave administrada por el cliente. AWS KMS Si usas una AWS KMS clave, la política de claves debe permitir que las cuentas de los miembros usen la clave.	Conformidad
Cree el bucket de registro de flujo central.	Cree el bucket central al que se enviarán los registros de flujo y aplique la estrategia de cifrado que eligió en el paso anterior. Debe estar en un archivo de registro o en una cuenta con un propósito similar. Consulte la política de bucket en la sección de Informaci ón adicional y aplíquela a su bucket central después de	AWS general

Tarea	Descripción	Habilidades requeridas
	actualizar los marcadores de posición con los valores específicos de su entorno.	
Configure los registros de VPC Flow para enviar los registros al bucket de registros de flujo central.	Agregue registros de flujo a cada VPC de la que desee recopilar datos. La forma más escalable de hacerlo es utilizar herramientas de IaC como AFT o AWS Cloud Development Kit (AWS CDK). Por ejemplo, puede crear un módulo Terraform que despliegue una VPC junto con un registro de flujo. Si es necesario, añada los registros de flujo manualmente.	Administrador de red
Configure los registros de flujo de VPC para enviarlos a los registros locales CloudWatch .	(Opcional) Si quieres que los registros de flujo estén visibles en las cuentas en las que se generan los registros, crea otro registro de flujo para enviar datos a los CloudWatch registros de la cuenta local. Como alternativa, puede enviar los datos a un bucket de S3 específico de la cuenta en la cuenta local.	AWS general

Recursos relacionados

- Cómo facilitar el análisis de datos y cumplir los requisitos de seguridad mediante el uso de datos de registro de flujo centralizados (entrada AWS del blog)

- Cómo habilitar automáticamente los registros de flujo de VPC mediante AWS Config reglas (AWS entrada del blog)

Información adicional

Política de bucket

Este ejemplo de política de bucket se puede aplicar a su bucket central de S3 para los registros de flujo después de añadir valores en los nombres de los marcadores de posición.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceOrgID": "<ORG_ID>"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>",
            "Condition": {
                "StringEquals": {
                    "aws:SourceOrgID": "<ORG_ID>"
                }
            }
        },
```

```
        {
            "Sid": "DenyUnencryptedTraffic",
            "Effect": "Deny",
            "Principal": {
                "AWS": "*"
            },
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::<BUCKET_NAME>/*",
                "arn:aws:s3:::<BUCKET_NAME>"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

Administre los conjuntos de AWS permisos de forma dinámica mediante Terraform

Vinicius Elias y Marcos Vinicius Pinto Jordao, Amazon Web Services

Resumen

AWS IAM Identity Center mejora AWS Identity and Access Management (IAM) al proporcionar un centro centralizado para administrar el acceso de inicio de sesión único a las aplicaciones en la nube Cuentas de AWS y las aplicaciones en la nube. Sin embargo, la administración manual de los conjuntos de permisos de IAM Identity Center puede resultar cada vez más compleja y propensa a errores a medida que su organización crece. Esta complejidad puede provocar posibles brechas de seguridad y sobrecarga administrativa.

Esta solución le permite administrar los conjuntos de permisos mediante la infraestructura como código (IaC) con una canalización de integración y entrega continuas (CI/CD) creada con Servicios de AWS nativos. Permite una integración perfecta del mecanismo de asignación de conjuntos de permisos con los eventos AWS Control Tower del ciclo de vida o con un entorno de Account Factory for Terraform (AFT). Este enfoque proporciona configuraciones de identidad dinámicas tanto para las nuevas como para las existentes Cuentas de AWS.

EventBridge Las reglas de Amazon supervisan Cuenta de AWS la creación y las actualizaciones, lo que ayuda a que las configuraciones de identidad permanezcan sincronizadas con la estructura de la organización. Tras crear o actualizar las cuentas en AWS Control Tower o en AFT, se activa la canalización. Evalúa un conjunto de archivos JSON con definiciones de conjuntos de permisos y reglas de asignación. Luego, la canalización aplica y sincroniza la configuración en todas las cuentas.

A continuación, se enumeran las ventajas de este enfoque:

- Coherencia: elimina las desviaciones de configuración manual en toda AWS la organización
- Auditabilidad: mantiene un historial completo de todos los cambios en la administración de identidades.
- Escalabilidad: aplica automáticamente las configuraciones a medida que su AWS entorno crece
- Seguridad: reduce los errores humanos en la asignación de permisos.
- Conformidad: facilita el cumplimiento de los requisitos reglamentarios mediante cambios documentados y reglas de asignación.

Requisitos previos y limitaciones

- Un entorno de múltiples cuentas con AWS Control Tower y AWS Organizations configuración. Opcionalmente, puede usar AFT con AWS Control Tower.
- Un administrador delegado del IAM Identity Center Cuenta de AWS para recibir la solución. Para obtener más información, consulte Delegated administration en la documentación de IAM Identity Center.
- Un repositorio del sistema de control de versiones (VCS) para gestionar el código principal. Para ver un ejemplo, consulte el repositorio de la GitHub solución.
- AWS Recursos necesarios para la administración del backend de Terraform, como un bucket de Amazon Simple Storage Service (Amazon S3) y una tabla de Amazon DynamoDB.

Limitaciones

- La canalización utiliza recursos AWS nativos y Terraform de código abierto. La canalización no está preparada para hacer llamadas a ecosistemas de terceros.
- Algunos Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

En el siguiente diagrama se muestran los componentes y el flujo de trabajo de este patrón.

AWS Control Tower los eventos fluyen

La solución comienza con la integración de los eventos que provienen de AFT AWS Control Tower o de AFT. La elección entre un servicio u otro se lleva a cabo en el momento de la implementación mediante la definición de variables. Independientemente del método utilizado, la canalización se activa cada vez que se crea o actualiza una cuenta. La canalización reconcilia las políticas almacenadas en el repositorio de administración de conjuntos de permisos.

Los siguientes son los eventos AWS Control Tower del ciclo de vida:

- `CreateManagedAccount`: cuando se crea una cuenta nueva.

- `UpdateManagedAccount`: cuando se actualiza una cuenta existente.

Enrutamiento de eventos

EventBridge sirve como servicio central de procesamiento de eventos, capturando los eventos generados en la AWS Control Tower cuenta. Cuando se producen eventos, los dirige de EventBridge forma inteligente a un bus de eventos centralizado en la cuenta de la solución. AWS Control Tower los eventos del ciclo de vida siguen patrones de enrutamiento distintos. Si se define AFT como la fuente del evento, la cuenta de administración de AFT gestiona los eventos en lugar de la AWS Control Tower cuenta. Esta arquitectura basada en eventos permite respuestas automatizadas a los cambios organizativos sin intervención manual.

Proceso de integración de AFT

Cuando los eventos AWS Control Tower del ciclo de vida llegan a la cuenta de administración de la AFT, activan automáticamente varios procesos posteriores que son intrínsecos a la AFT. Una vez que se completa el flujo de trabajo de personalización de la cuenta de AFT, publica un mensaje en el tema dedicado de Amazon Simple Notification Service (Amazon SNS) `aft-notifications`. Ese tema activa la `aft-new-account-forward-event` AWS Lambda función que implementa esta solución. La función de Lambda envía el evento al bus de eventos de la cuenta de la solución, donde se utiliza para iniciar la canalización.

Canalización de infraestructura como código

La canalización de soluciones funciona como un mecanismo de implementación totalmente automatizado. El AWS CodePipeline servicio monitorea continuamente el repositorio para detectar cambios. Al detectar nuevas confirmaciones, inicia automáticamente el flujo de trabajo de implementación e inicia un proceso secuencial que incluye las fases de validación y ejecución. El sistema ejecuta `plan` las operaciones de Terraform para identificar los cambios propuestos, seguidas de los `apply` comandos de Terraform para implementar esos cambios en el AWS entorno. En particular, la canalización se ejecuta sin ninguna puerta de aprobación manual. Este enfoque permite implementar rápidamente los cambios en la infraestructura y, al mismo tiempo, mantener la auditabilidad mediante los registros de la canalización y los archivos de estado de Terraform.

La canalización se aprovecha AWS CodeBuild para ejecutar las operaciones de Terraform en un entorno controlado con los permisos adecuados. Mediante este enfoque de IaC, la canalización puede efectuar operaciones integrales de administración de permisos, tales como las siguientes:

- Creación de conjuntos de permisos nuevos.

- Actualización de conjuntos de permisos existentes.
- Eliminación de conjuntos de permisos innecesarios.
- Gestione la asignación de estos permisos entre las cuentas y los grupos de las AWS organizaciones.

Para mantener la coherencia de la infraestructura y evitar cambios conflictivos, la solución implementa el sistema de administración de estados del backend de Terraform mediante un bucket de Amazon S3 y una tabla dedicada de Amazon DynamoDB. Este enfoque proporciona una ubicación de almacenamiento persistente para los archivos de estado de Terraform y mecanismos de bloqueo de estado para evitar modificaciones simultáneas en los mismos recursos.

El código principal de Terraform usa el módulo oficial de AWS `permission-sets` Terraform. Este módulo puede administrar dinámicamente los conjuntos de permisos en IAM Identity Center basándose en plantillas de conjuntos de permisos.

Administración de control de origen

Las plantillas del conjunto de permisos (archivos JSON) residen en un sistema de control de versiones externo, por ejemplo GitHub, que proporciona un repositorio centralizado para las configuraciones de administración de identidades. Este enfoque establece una fuente única de información fiable para las definiciones de conjuntos de permisos y, al mismo tiempo, permite el desarrollo colaborativo mediante prácticas estándar de revisión del código. Los usuarios autorizados pueden confirmar cambios en estas plantillas siguiendo los procesos de administración de cambios organizativos. Estas confirmaciones son el principal desencadenante de la canalización de implementación automatizada, que inicia el proceso de actualización de la infraestructura.

Para ver un ejemplo de cómo configurar los conjuntos de permisos mediante el archivo JSON en el repositorio, consulte Información adicional.

Tools (Herramientas)

Servicios de AWS

- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- AWS CodeConnectionspermite que AWS los recursos y servicios, por ejemplo CodePipeline, se conecten a repositorios de código externos, por ejemplo. GitHub

- AWS CodePipeline permite diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software y automatizar los pasos necesarios para lanzar los cambios en el software de manera continua.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar Servicios de AWS mediante comandos en el shell de la línea de comandos.
- AWS Control Towerle ayuda a configurar y administrar un entorno de AWS múltiples cuentas, siguiendo las mejores prácticas prescriptivas.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, AWS Lambda funciones, puntos de enlace de invocación HTTP que utilizan destinos de API o buses de eventos en otros. Cuentas de AWS
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS IAM Identity Centerle ayuda a gestionar de forma centralizada el acceso mediante el inicio de sesión único (SSO) a todas sus aplicaciones y a las de la nube. Cuentas de AWS
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar múltiples cuentas Cuentas de AWS en una organización que puede crear y administrar de forma centralizada.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico. Permite las notificaciones push para los eventos de administración de cuentas, lo que garantiza que las partes pertinentes estén informadas de los cambios o acciones importantes que se produzcan en el sistema.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.

Repositorio de código

El código de este patrón está disponible en la organización AWS Samples y en el repositorio GitHub - sets-pipeline. sample-terraform-aws-permission

Prácticas recomendadas

- Fije siempre las versiones de los módulos y proveedores de Terraform que se utilizan para ejecutar el código en producción.
- Utilice una herramienta de análisis de código estático, como Checkov, para analizar el código y, a continuación, resolver los problemas de seguridad.
- Siga el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Creación de los requisitos previos (opcional)

Tarea	Descripción	Habilidades requeridas
Crear los recursos del backend de Terraform.	Si aún no ha creado sus AWS recursos de backend de Terraform, siga estos pasos para crear un bucket de Amazon S3 (`s3-tf-backend-{ACCOUNT_ID}`) y una tabla de DynamoDB (). `ddb-tf-backend` 1. Inicie sesión en el Cuenta de AWS lugar donde implementará la solución y ábrala en la página de	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	inicio. AWS CloudShell AWS Control Tower Región de AWS
	2. Ejecute los siguientes comandos y sustituya el marcador {ACCOUNT_ID} de posición por su Cuenta de AWS ID:
	`aws s3api create-bucket --bucket s3-tf-backend-{ACCOUNT_ID}`
	`aws s3api put-bucket-versioning --bucket s3-tf-backend-{ACCOUNT_ID} --versioning-configuration Status=Enabled`
	`aws dynamodb create-table --table-name ddb-tf-backend --attribute-definitions AttributeName=LockID,AttributeType=S --key-schema AttributeName=LockID,KeyType=HASH --provisioned-throughput ReadCapacityUnits=1,WriteCapacityUnits=1`	

Tarea	Descripción	Habilidades requeridas
Cree un rol multicuenta.	Debe proporcionar una función de IAM multicuenta en la configuración del proveedor de `event-source-account` Terraform AWS . Si aún no ha creado este rol, siga estos pasos para crearlo: 1. Inicie sesión en la Cuenta de AWS que será su fuente de eventos (cuenta de AWS Control Tower administración o cuenta AFT) y ábrala. AWS CloudShell 2. Ejecuta el siguiente comando y reemplaza el marcador `{ACCOUNT_ID}` de posición por el Cuenta de AWS ID que estás usando para esta solución, no por tu Cuenta de AWS ID actual: `aws iam create-role \ --role-name CrossAccountRole \ --assume-role-policy-document '{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": {`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	<pre>"AWS": "arn:aws:iam::{ACCOUNT_ID}:root"
	},
	
	"Action": "sts:AssumeRole"
	}
	]
	}'</pre>
	1. Compruebe la salida del comando y copie el Nombre de recurso de Amazon (ARN) del rol (por ejemplo, `arn:aws:iam::111122223333:role/CrossAccountRole`).
	2. Para asociar una política de IAM al rol, ejecute el comando siguiente:
	
	<pre>aws iam attach-role-policy \
	--role-name CrossAccountRole \
	--policy-arn arn:aws:iam::aws:policy/AdministratorAccess</pre>
	En este ejemplo, se utiliza la política de IAM AWS gestionada. AdministratorAccess Si lo prefiere,	

Tarea	Descripción	Habilidades requeridas
	puede utilizar una política más específica.	

Preparación del repositorio de conjuntos de permisos

Tarea	Descripción	Habilidades requeridas
Crear un repositorio dedicado.	En esta tarea se presupone que está utilizando GitHub. Cree un repositorio dedicado para almacenar el código principal de Terraform y los archivos JSON de la plantilla del conjunto de permisos.	DevOps ingeniero
Preparar el código del conjunto de permisos.	Para obtener información sobre cómo estructurar los siguientes archivos, consulte el código de ejemplo en el repositorio de soluciones: ├── main.tf ├── outputs.tf ├── providers.jinja └── templates Copie el contenido, conserve los valores de `providers.jinja` y haga los ajustes necesarios en los demás archivos. Por ejemplo, agregue archivos de plantilla s de conjuntos de permisos a	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`templates` o fije la versión del módulo `aws-ia/permission-sets/aws` en el archivo `main.tf`.	
Confirmar los cambios.	Confirme e inserte los cambios en el repositorio que creó anteriormente. Guarde el nombre del repositorio y su GitHub organización, por ejemplo,`myorg/aws-ps-pipeline` .	DevOps ingeniero

Preparación del código de implementación

Tarea	Descripción	Habilidades requeridas
Descargar el contenido.	Descargue (clone) el contenido del repositorio de soluciones.	DevOps ingeniero
Completar las variables.	Cree un archivo `terraform.tfvars` y agregue las siguientes variables necesarias: • `repository_name` : nombre del repositorio de conjuntos de permisos que creó anteriormente. • `branch_name` : nombre de la rama del repositorio de conjuntos de permisos. • `vcs_provider` : su proveedor de VCS.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	• `account_lifecycle_events_source` — El origen de los eventos que activan el oleoducto (AWS Control Tower o AFT)
	
	`repository_name = "myorg/aws-ps-pipeline"`
	`branch_name = "main"`
	`vcs_provider = "github"`
	`account_lifecycle_events_source = "CT"`
	
	Para obtener información sobre opciones de variables adicionales, consulta el archivo variables.tf en el repositorio de este patrón. GitHub	

Tarea	Descripción	Habilidades requeridas
Ajustar la configuración del backend de Terraform.	En el archivo `backend.tf`, sustituya los marcadores de posición por sus propios valores. Use el AWS Control Tower inicio Región de AWS y proporcione los nombres del bucket de Amazon S3 y la tabla de DynamoDB creados anteriormente. `terraform { required_version = ">=1.6" backend "s3" { region = "{region}" bucket = "{bucket_name}" key = "terraform.tfstate" dynamodb_table = "{table_name}" encrypt = "true" } }` Si lo prefiere, puede usar su propia configuración de backend de Terraform.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Ajustar la configuración del proveedor de Terraform.	En el archivo `providers.tf` , sustituya los marcadores de posición por su propia información. Utilice la región de AWS Control Tower origen y proporcione el ARN del rol de IAM multicuenta creado anteriormente para el proveedor. `event-source-account`
	`provider "aws" {`
	`  region = "{region}"`
	`}`
	
	`provider "aws" {`
	`  alias  = "event-source-account"`
	`  region = "{region}"`
	`  assume_role {`
	`  role_arn = "{role_arn}"`
	`  }`
	`}`
		DevOps ingeniero

Implementación manual de la solución

Tarea	Descripción	Habilidades requeridas
Seleccione el Cuenta de AWS.	Le recomendamos implementar la solución en la cuenta de administrador delegado de IAM Identity Center. Sin embargo, también puede implementarlo en la cuenta	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	AWS Organizations de administración. Para iniciar sesión en la cuenta seleccionada en la misma región que la instancia de IAM Identity Center, utilice la AWS CLI. Asegúrese de que el rol de IAM que está utilizando tiene permiso para asumir el rol que se especificó para el proveedor `event-source-account` en los pasos anteriores. Además, este rol debe tener acceso a los AWS recursos que se utilizan en la configuración del backend de Terraform.	
Ejecutar Terraform manualmente.	Para inicializar, planificar y aplicar las configuraciones, ejecute los siguientes comandos de Terraform en el orden que aparecen: 1. `terraform init` 2. `terraform plan` 3. `terraform apply`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Compruebe los resultados de la implementación.	En la cuenta de administrador delegado de IAM Identity Center, compruebe que se haya creado la canalización de `aws-ps-pipeline` . Compruebe también que haya una AWS CodeConnections conexión con el estado Pendiente.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Finalice la CodeConnections configuración.	Para finalizar la CodeConnections configuración, siga los siguientes pasos: 1. Vaya a CodeConnections, seleccione la conexión que se creó y elija Actualizar la conexión pendiente. 2. Proporcione sus GitHub credenciales, instale una nueva GitHub aplicación o seleccione una existente que tenga acceso al repositorio del conjunto de permisos y elija Connect. La canalización ahora debería tener acceso al repositorio de conjuntos de permisos. Para obtener instrucciones detalladas, consulte Update a pending connection en la documentación de la consola de herramientas para desarrolladores.	AWS DevOps

Elección de un flujo de ejecución de canalizaciones para probar la solución

Tarea	Descripción	Habilidades requeridas
Ejecute la canalización mediante AWS Control Tower las actualizaciones de AFT.	Una vez creada o modificada una cuenta mediante AWS Control Tower AFT (según el	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	tipo de eventos del ciclo de vida que elijas), se inicia la canalización.	
Cambiar el código para ejecutar la canalización.	Tras cambiar el código y confirmarlo en la rama `main`, se inicia la canalización.	AWS DevOps
Ejecutar la canalización manualmente.	Para iniciar la canalizac ión manualmente, utilice la función de cambio de versión de AWS CodePipeline.	AWS DevOps

Resolución de problemas

Problema	Solución
Acceso denegado	Compruebe que cuente con los permisos necesarios para implementar la solución.
CodeConnections problemas	• Compruebe que el estado de la conexión sea Disponible y no Pendiente. • Compruebe que la CodeConnections configuración se haya completado correctam ente con GitHub las credenciales. Para obtener instrucciones, consulte Update a pending connection en la documentación de la consola de herramientas para desarroll adores. • Asegúrese de que la GitHub aplicación tenga los permisos de acceso adecuados al repositorio del conjunto de permisos.

Problema	Solución
Problemas de ejecución de las canalizaciones	• Comprueba CloudWatch los registros de Amazon para ver si hay errores en la ejecución de la canalización. • Asegúrese de que la delegación de IAM Identity Center esté configurada correctam ente. De lo contrario, puede provocar errores en la canalización al leer Cuenta de AWS los metadatos.
Problemas de implementación de los conjuntos de permisos	• Compruebe que la sintaxis JSON de los archivos de plantillas de conjuntos de permisos sea correcta. • Compruebe que existan las políticas administradas de IAM a las que se hace referencia en las plantillas. • Compruebe si los grupos y usuarios especific ados en las asignaciones existen en IAM Identity Center.

Recursos relacionados

Servicio de AWS documentación

- AWS IAM Identity Center Guía del usuario
- Administre Cuentas de AWS con conjuntos de permisos (documentación del IAM Identity Center)

Otros recursos

- AWS Módulo de conjuntos de permisos (Terraform)

Información adicional

Archivo JSON con un ejemplo de conjunto de permisos

En el siguiente ejemplo se muestra cómo configurar un conjunto de permisos mediante el archivo JSON del repositorio:

```
{
  "Name": "ps-billing", // Permission set identifier
  "Comment": "Sample permission set for billing access", // Comment to document the
 purpose of the permission set
  "Description": "Billing access in AWS", // Detailed description
  "SessionDuration": "PT4H", // Session duration = 4 hours (ISO 8601 format)
  "ManagedPolicies": [ // List of AWS IAM managed policies
    "arn:aws:iam::aws:policy/job-function/Billing",
    "arn:aws:iam::aws:policy/job-function/SupportUser",
    "arn:aws:iam::aws:policy/AWSSupportAccess",
    "arn:aws:iam::aws:policy/job-function/ViewOnlyAccess"
  ],
  "CustomerPolicies": [], // References to IAM policies previously created
  "CustomPolicy": {}, // Inline IAM policy defined directly in the permission set
  "PermissionBoundary": {  // AWS or customer managed IAM policy to be used as boundary
    "ManagedPolicy": "",
    "CustomerPolicy": ""
  },
  "Assignments": [ // Define the assignment rules
    {
      "all_accounts": true, // Apply to ALL active AWS accounts in organization
      "principal": "G_BILLING_USERS", // Group/user name in Identity Center
      "type": "GROUP", // Can be "GROUP" or "USER"
      "account_id": [], // List of AWS account ID (empty since all_accounts=true)
      "account_ou": [], // List of AWS Organizational Unit IDs with target AWS accounts
      "account_tag": [] // List of tags (key:value) to match AWS Organization accounts
 tags
    }
  ]
}
```

Para obtener más información, consulte el esquema JSON en la documentación del módulo AWS Permission Sets del sitio web de Terraform.

Consejos

- Puede usar los bloques de importación de Terraform para importar un conjunto de permisos existente a la solución.

- Puede usar AFT para implementar la canalización del conjunto de AWS permisos en una cuenta delegada. Para obtener más información, consulte AFT Blueprints.

Etiquete automáticamente las conexiones de puerta de enlace de tránsito con AWS Organizations

Richard Milner-Watts, Haris Bin Ayub y John Capps, Amazon Web Services

Resumen

En Amazon Web Services (AWS), se puede utilizar AWS Resource Access Managerpara compartir a AWS Transit Gatewaytravés de Cuenta de AWS fronteras. Sin embargo, cuando crea conexiones de puerta de enlace de tránsito más allá de los límites de la cuenta, los archivos adjuntos se crean sin una etiqueta de nombre. Esto puede hacer que la identificación de los archivos adjuntos lleve mucho tiempo.

Esta solución proporciona un mecanismo automatizado para recopilar información sobre cada conexión de puerta de enlace de tránsito para las cuentas de una organización administrada por AWS Organizations. El proceso incluye buscar el rango de enrutamiento entre dominios sin clase (CIDR) en la tabla de enrutamiento de puerta de enlace de tránsito. Luego, la solución aplica una etiqueta con el nombre en forma de `<CIDR-range>-<AccountName>` a la conexión de la cuenta que contiene la puerta de enlace de tránsito.

Esta solución se puede utilizar junto con una solución como el Serverless Transit Network Orchestrator de la biblioteca de AWS soluciones. El orquestador de redes de tránsito sin servidor permite la creación automatizada de conexiones de puerta de enlace de tránsito a escala.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Una AWS Organizations organización que contiene todas las cuentas relacionadas
- Acceda a la cuenta de administración de la organización, ubicada en la raíz de la organización, para crear el rol necesario AWS Identity and Access Management (IAM)
- Una cuenta de miembro de una red compartida que contiene una o más puertas de enlace de tránsito que se comparten con la organización y tienen archivos adjuntos

Arquitectura

La siguiente captura de pantalla Consola de administración de AWS muestra ejemplos de archivos adjuntos de Transit Gateway sin etiqueta de nombre asociada y dos archivos adjuntos de Transit Gateway con etiquetas de nombre generados por esta solución. La estructura de la etiqueta de nombre generada es `<CIDR-range>-<AccountName>`.

Esta solución se utiliza AWS CloudFormationpara implementar un AWS Step Functionsflujo de trabajo que gestiona la creación de etiquetas de nombre de Transit Gateway en todas las configuraciones Regiones de AWS. El flujo de trabajo invoca las funciones de AWS Lambda, que hacen las tareas subyacentes.

Una vez que la solución haya obtenido los nombres de las cuentas AWS Organizations, la máquina de estados Step Functions recibirá todos los archivos adjuntos de Transit Gateway IDs. La región las procesa en paralelo. Este procesamiento incluye la búsqueda del rango de CIDR para cada archivo adjunto. El rango CIDR se obtiene buscando en las tablas de enrutamiento de puerta de enlace de tránsito de la región un identificador de la conexión de puerta de enlace de tránsito coincidente. Si toda la información requerida está disponible, la solución aplica una etiqueta con el nombre al archivo adjunto. La solución no sobrescribirá ninguna etiqueta de nombre existente.

La solución se ejecuta según un cronograma controlado por un EventBridge evento de Amazon. El evento inicia la solución todos los días a las 6:00 UTC.

Pila de tecnología de destino

- Amazon EventBridge
- AWS Lambda
- AWS Organizations
- AWS Transit Gateway
- Amazon Virtual Private Cloud (Amazon VPC)
- AWS X-Ray

Arquitectura de destino

La arquitectura de la solución y el flujo de trabajo se muestran en el siguiente diagrama.

1. El evento programado inicia la regla.
2. La EventBridge regla inicia la máquina de estados Step Functions.
3. La máquina de estados invoca la función de Lambda `tgw-tagger-organizations-account-query`.
4. La función de Lambda `tgw-tagger-organizations-account-query` asume la función en la cuenta de administración de la organización.
5. La función `tgw-tagger-organizations-account-query` Lambda llama a la API de Organizations para devolver Cuenta de AWS los metadatos.
6. La máquina de estados invoca la función de Lambda `tgw-tagger-attachment-query`.
7. Para cada región, en paralelo, la máquina de estados invoca la función de Lambda `tgw-tagger-rtb-query` para leer el rango CIDR de cada adjunto.
8. Para cada región, en paralelo, la máquina de estados invoca la función de Lambda para `tgw-tagger-attachment-tagger`
9. Las etiquetas de nombre se crean para las conexiones de puerta de enlace de tránsito en la cuenta Shared Networking.

Automatizar y escalar

La solución procesa cada región en paralelo para reducir la duración total de la ejecución.

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormationproporciona una forma de modelar un conjunto de recursos relacionados AWS y de terceros, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de sus ciclos de vida, tratando la infraestructura como código.
- Amazon le CloudWatch ayuda a supervisar las métricas de sus recursos de AWS y las aplicaciones en las que se ejecuta AWS en tiempo real.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que puede utilizar para conectar sus aplicaciones con datos de diversas fuentes. EventBridge recibe un evento, un indicador de un cambio en el entorno, y aplica una regla para enrutar el evento a un objetivo. Las reglas hacen coincidir los eventos con los objetivos o bien en función de la estructura del evento, llamado un patrón de evento, o bien de una programación.

- AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo paga por el tiempo de proceso que consume. No se aplican cargos cuando su código no se está ejecutando.
- AWS Organizationsle ayuda a administrar y gobernar su entorno de forma centralizada a medida que crece y escala sus AWS recursos. Con Organizations, puede crear recursos nuevos Cuentas de AWS y asignarlos mediante programación, agrupar cuentas para organizar sus flujos de trabajo, aplicar políticas a cuentas o grupos para la gobernanza y simplificar la facturación mediante el uso de un único método de pago para todas sus cuentas.
- AWS Step Functionses un servicio de flujo de trabajo visual de bajo código que se utiliza para organizar Servicios de AWS, automatizar los procesos empresariales y crear aplicaciones sin servidor. Los flujos de trabajo gestionan los errores, los reintentos, la paralelización, las integraciones de servicios y la observabilidad para que los desarrolladores puedan centrarse en una lógica empresarial de mayor valor.
- AWS Transit Gatewayconecta VPCs y conecta redes locales a través de un hub central. Esto simplifica su red y pone fin a las complejas relaciones de interconexión. Actúa como un router en la nube, de modo que cada nueva conexión se realiza solo una vez.
- Amazon Virtual Private Cloud (Amazon VPC) es un servicio para lanzar AWS recursos en una red virtual aislada de forma lógica que usted defina.
- AWS X-Ray recopila datos sobre las solicitudes que atiende la aplicación y proporciona herramientas que puede utilizar para consultar, filtrar y obtener información sobre dichos datos para identificar problemas y oportunidades de optimización.

Código

El código fuente de esta solución está disponible en el GitHub repositorio Transit Gateway Attachment Tagger. El repositorio incluye los siguientes archivos:

- `tgw-attachment-tagger-main-stack.yaml` crea todos los recursos necesarios para respaldar esta solución en la cuenta Shared Networking.
- `tgw-attachment-tagger-organizations-stack.yaml` crea un rol en la cuenta de administración de la organización.

Epics

Implemente el conjunto principal de soluciones

Tarea	Descripción	Habilidades requeridas
Reúna la información necesaria sobre los requisitos previos.	Para configurar el acceso entre cuentas desde la función Lambda a AWS Organizations la API, necesita el ID de cuenta de la cuenta de administración de la organización. **Note** El orden en el que se crean las dos CloudFormation pilas es importante. Primero debe implementar los recursos en la cuenta de red compartida. El rol en la cuenta Shared Networking ya debe existir antes de implementar los recursos en la cuenta de administración de la organización. Para obtener más información, consulte la Documentación de AWS.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Inicie la CloudFormation plantilla para la pila de soluciones principal.	La plantilla de la pila de soluciones principal implement ará las funciones de IAM, el flujo de trabajo de Step Functions, las funciones de Lambda y el evento de Amazon CloudWatch . Abra la cuenta Consola de administración de AWS de red compartida y, a continuación, abra la consola: &CFN. Cree la pila con la plantilla `tgw-attachment-tagger-main-stack.yaml` y los siguientes valores: • Nombre de la pila: -stack tgw-attachment-tagger-main • awsOrganizationsRo otAccountId— ID de cuenta de la cuenta de administr ación de la organización • TGWRegionsparámetro: Regiones de AWS para la solución, introducido como una cadena delimitada por comas • TGWListparámetro: puerta de enlace de tránsito IDs que debe excluirse de la solución, introducida en	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	una cadena delimitada por comas Para obtener más información sobre cómo lanzar una CloudFormation pila, consulte la documentación.AWS	
Compruebe que la solución se haya lanzado correctamente.	Espere a que la CloudFormation pila alcance el estado CREATE_COMPLETE. Este proceso no debería tardar más de un minuto. Abra la consola Step Functions y compruebe que se ha creado una nueva máquina de estados con el nombre tgw-attachment-tagger-state-machine.	DevOps ingeniero

Implemente el paquete de AWS Organizations

Tarea	Descripción	Habilidades requeridas
Reúna la información necesaria sobre los requisitos previos.	Para configurar el acceso entre cuentas desde la función de Lambda a la API de AWS Organizations, necesita el ID de cuenta de la cuenta Shared Networking.	DevOps ingeniero
Inicie la CloudFormation plantilla para la pila Organizations	En la plantilla de AWS Organizations stack, se implementará el rol de IAM	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	en la cuenta de gestión de la organización. Acceda a la consola de AWS de la cuenta de administración de la organización y, a continuación, abra la CloudFormation consola. Cree la pila con la plantilla `tgw-attachment-tagger-organizations-stack.yaml` y los siguientes valores: • Nombre de la pila: tgw-attachment-tagger-organizations-stack • NetworkingAccountIdparámetro: ID de cuenta de la cuenta de red compartida Para las demás opciones de creación de pilas, usa los valores predeterminados.	

Tarea	Descripción	Habilidades requeridas
Compruebe que la solución se haya lanzado correctamente.	Espere a que la CloudForm ation pila alcance el estado CREATE_COMPLETE. Este proceso no debería tardar más de un minuto. Abra la consola AWS Identity and Access Management (IAM) y compruebe que se ha creado un nuevo rol con el nombre -query-role. tgw-attac hment-tagger-organization	DevOps ingeniero

Verificación de la solución

Tarea	Descripción	Habilidades requeridas
Ejecuta la máquina de estado.	Abra la consola Step Functions de la cuenta Shared Networking y elija Equipos de estado en el panel de navegación. Seleccione el estado machine tgw-attachment-tagger-state-machine y elija Iniciar ejecución. Como la solución no utiliza la entrada de esta máquina de estados, puede utilizar el valor predeterminado. {	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	<pre>"Comment": "Insert your JSON here"
	}</pre>
	Seleccione Iniciar ejecución.	

Vigile la máquina de estados hasta su finalización.	En la nueva página que se abre, puede ver cómo funciona la máquina de estados. La duración dependerá de la cantidad de conexiones de puerta de enlace de tránsito que se procesen. En esta página, puede examinar cada paso de la máquina de estados. Puede ver las distintas tareas de la máquina de estados y seguir los enlaces a los CloudWatch registros de las funciones de Lambda. Para las tareas que se ejecutan en paralelo dentro del mapa, puede usar la lista desplegable del Índice para ver las implementaciones específicas de cada región.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Compruebe las etiquetas de conexión de puerta de enlace de tránsito.	Abra la consola de VPC de la cuenta Shared Networking y elija Conexiones de puerta de enlace de tránsito. En la consola, se proporcio na una etiqueta de nombre para los archivos adjuntos que cumplen los criterios (el archivo adjunto se propaga a una tabla de enrutamiento de puerta de enlace de tránsito y el propietario del recurso es miembro de la organización).	DevOps ingeniero
Verifique el inicio CloudWatch del evento.	Espere a que se inicie el CloudWatch evento. Está programado para las 06:00 UTC. Abra la consola Step Functions de la cuenta Shared Networking y elija State machines (Máquinas de estado) en el panel de navegación. Seleccione el estado machine tgw-attachment-tagger-state-machine. Compruebe que la solución se haya ejecutado a las 06:00 UTC.	DevOps ingeniero

Recursos relacionados

- AWS Organizations

- AWS Resource Access Manager
- Orquestador de redes de tránsito sin servidor
- Creación de roles de IAM
- Crear una pila en la AWS CloudFormation consola

Más patrones

- Automatice las asignaciones de CIDR, IPAM y IPv4 CIDR de Amazon VPC para nuevos mediante AFT Cuentas de AWS
- Control de los conjuntos de permisos para varias cuentas mediante Account Factory for Terraform
- AWS Service Catalog Aprovisione productos en función de AWS CloudFormation plantillas mediante GitHub acciones
- Aprovisionamiento de roles de IAM con privilegio mínimo mediante la implementación de una solución de máquina expendedora de roles

Aprendizaje & automático con IA

Temas

- Asociar un AWS CodeCommit repositorio de una cuenta Cuenta de AWS a Amazon SageMaker AI Studio Classic de otra cuenta
- Extraer contenido de archivos PDF automáticamente con Amazon Textract
- Cree un modelo de previsión de arranque en frío utilizando DeepAR para series temporales en SageMaker Amazon AI Studio Lab
- Cree un MLOps flujo de trabajo con Amazon SageMaker AI y Azure DevOps
- Configure el registro de invocación de modelos en Amazon Bedrock mediante AWS CloudFormation
- Cree una imagen de contenedor Docker personalizada SageMaker y úsela para el entrenamiento de modelos en AWS Step Functions
- Uso de agentes de Amazon Bedrock para automatizar la creación de controles de entrada de acceso en Amazon EKS mediante peticiones basadas en texto
- Implemente un caso de uso de RAG AWS mediante Terraform y Amazon Bedrock
- Implemente la lógica de preprocesamiento en un modelo de aprendizaje automático en un único punto final mediante una canalización de inferencias en Amazon SageMaker
- Implemente la validación de seguridad de la codificación en tiempo real mediante un servidor MCP con Kiro y otros asistentes de codificación
- Desarrolle asistentes avanzados de IA generativa basados en chat mediante RAG y solicitudes ReAct
- Desarrollo de un asistente basado en el chat totalmente automatizado con los agentes y las bases de conocimiento de Amazon Bedrock
- Documentación del conocimiento institucional a partir de las entradas de voz mediante Amazon Bedrock y Amazon Transcribe
- Genere recomendaciones personalizadas y reclasificadas con Amazon Personalize
- Optimice los flujos de trabajo de aprendizaje automático desde el desarrollo local hasta los experimentos escalables mediante el uso de SageMaker IA e Hydra
- Traduce el lenguaje natural a consultas (DSL) para consultas de Elasticsearch OpenSearch y consultas de Elasticsearch
- Uso de Amazon Q Developer como asistente de codificación para aumentar la productividad

- Utilice el SageMaker procesamiento para la ingeniería de características distribuidas de conjuntos de datos de aprendizaje automático a escala de terabytes
- Visualice los resultados del AI/ML modelo con Flask y AWS Elastic Beanstalk
- Más patrones

Asociar un AWS CodeCommit repositorio de una cuenta Cuenta de AWS a Amazon SageMaker AI Studio Classic de otra cuenta

Laurens van der Maas y Aubrey Oosthuizen, Amazon Web Services

Resumen

Este patrón proporciona instrucciones y código sobre cómo asociar un AWS CodeCommit repositorio de una Cuenta de AWS (cuenta A) con Amazon SageMaker AI Studio Classic de otra Cuenta de AWS (cuenta B). Para configurar la asociación, debe crear una política y un rol AWS Identity and Access Management (de IAM) en la cuenta A y una política en línea de IAM en la cuenta B. A continuación, debe utilizar un script de shell para clonar el CodeCommit repositorio de la cuenta A a Amazon SageMaker AI Classic en la cuenta B.

Requisitos previos y limitaciones

Requisitos previos

- Dos Cuentas de AWS, una que contiene el CodeCommit repositorio y la otra que contiene un dominio de SageMaker IA con un usuario
- Dominio y usuario de SageMaker IA aprovisionados, con acceso a Internet o acceso a CodeCommit y AWS Security Token Service (AWS STS) a través de puntos finales de red privada virtual (VPC)
- Conocimientos básicos de IAM
- Conocimientos básicos de AI Studio Classic SageMaker
- Conocimientos básicos de Git y CodeCommit

Limitaciones

Este patrón se aplica únicamente a SageMaker AI Studio Classic, no RStudio a Amazon SageMaker AI.

Arquitectura

Pila de tecnología

- Amazon SageMaker AI
- Amazon SageMaker AI Studio clásico

- AWS CodeCommit
- AWS Identity and Access Management (IAM)
- Git

Arquitectura de destino

El siguiente diagrama muestra una arquitectura que asocia un CodeCommit repositorio de la cuenta A a SageMaker AI Studio Classic en la cuenta B.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario asume el `MyCrossAccountRepositoryContributorRole` rol en la cuenta A a través del `sts:AssumeRole` rol, mientras que usa el SageMaker rol de ejecución de SageMaker IA en AI Studio Classic en la cuenta B. El rol asumido incluye CodeCommit los permisos para clonar e interactuar con el repositorio especificado.
2. El usuario ejecuta los comandos de Git desde el terminal del sistema en SageMaker AI Studio Classic.

Automatización y escala

Este patrón consiste en pasos manuales que se pueden automatizar mediante el uso de AWS Cloud Development Kit (AWS CDK), AWS CloudFormation, o Terraform.

Tools (Herramientas)

Herramientas de AWS

- Amazon SageMaker AI es un servicio de aprendizaje automático (ML) gestionado que le ayuda a crear y entrenar modelos de aprendizaje automático para luego implementarlos en un entorno hospedado listo para la producción.
- Amazon SageMaker AI Studio Classic es un entorno de desarrollo integrado (IDE) basado en la web para el aprendizaje automático que le permite crear, entrenar, depurar, implementar y supervisar sus modelos de aprendizaje automático.
- AWS CodeCommit es un servicio de control de versiones que permite almacenar y administrar repositorios de Git de forma privada, sin necesidad de administrar su propio sistema de control de origen.

Aviso: ya no AWS CodeCommit está disponible para nuevos clientes. Los clientes actuales de AWS CodeCommit pueden seguir utilizando el servicio con normalidad. Más información

- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.

Otras herramientas

- Git es un sistema de control de versiones distribuido que rastrea los cambios en el código fuente durante el desarrollo del software.

Epics

Cree una política y rol de IAM en la cuenta A

Tarea	Descripción	Habilidades requeridas
Crear una política de IAM de acceso al repositorio en Cuenta A.	1. Inicie sesión en la consola de Consola de administración de AWS IAM y ábrala. 2. En el panel de navegación, seleccione Políticas y, a continuación, Crear política. 3. Seleccione la pestaña JSON. 4. Copie la instrucción de política del ejemplo de política de IAM incluido en la sección de Información adicional de este patrón y, a continuación, pegue la instrucción en el editor de JSON. Asegúrese de reemplazar todos los valores de los marcadores de posición de la política.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	5. Seleccione Next:Tags (Siguiente: etiquetas) y, a continuación, Next:Review (Siguiente: revisar). 6. En Nombre, escriba un nombre para la política. Nota: En este patrón se hace referencia a la política de IAM como `CrossAccountAccessForMySharedDemoRepo`, pero puede elegir el nombre de política que prefiera. 7. Elija Crear política. **Tip** Se recomienda restringir el alcance de las políticas de IAM a los permisos mínimos requeridos para cada caso de uso.	

Tarea	Descripción	Habilidades requeridas
Crear un rol de IAM para el acceso al repositorio en la Cuenta A.	1. En el panel de navegación de la consola de IAM, seleccione Roles y, a continuación, seleccione Crear rol. 2. En Tipo de entidad de confianza, seleccione Cuenta de AWS. 3. En la sección Cuenta de AWS, seleccione Otra cuenta de AWS. 4. En Account ID (ID de cuenta), escriba el ID de la cuenta B. 5. En la página Agregar permisos, busque y seleccione la política `CrossAccountAccessForMySharedDemoRepo` que creó anteriormente. 6. Seleccione Next (Siguiente). 7. En Role name (Nombre de rol), escriba un nombre. Nota: En este patrón se hace referencia al nombre de IAM como `MyCrossAccountRepositoryContributorRole`, pero puede elegir el nombre de rol que prefiera. 8. Seleccione Crear rol y, a continuación, copie el	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Nombre de recurso de Amazon (ARN) del nuevo rol.	

Cree una política de IAM en línea en la cuenta B

Tarea	Descripción	Habilidades requeridas
Adjunte una política en línea a la función de ejecución asociada al usuario de su SageMaker dominio en la cuenta B.	1. En el panel de navegación de la consola de IAM, seleccione Roles. 2. Busca y elige la función de ejecución asociada a tu usuario de SageMaker AI Domain en la cuenta B. 3. Seleccione Agregar permisos y, a continuación, Crear política insertada. 4. Seleccione la pestaña JSON. 5. Copie la siguiente política y péguela en el editor de JSON. `{ "Version": "2012-10-17", "Statement": [ { "Sid": "VisualEditor0", "Effect": "Allow", "Action": "sts:AssumeRole",`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	<pre>"Resource": "arn:aws:iam::<Account_A_ID>:role/<Account_A_Role_Name>"
	}
	]
	}</pre>
	6. Sustituya `<Account_A_ID>` por la ID de cuenta de la cuenta A. Sustituya `<Account_A_Role_Name>` por el nombre del rol de IAM que creó anteriormente.
	7. Seleccione Revisar política.
	8. En Nombre, escriba el nombre de la política insertada.
	9. Elija Crear política.	

Clona el repositorio en SageMaker AI Studio Classic para la cuenta B

Tarea	Descripción	Habilidades requeridas
Crea el script de shell en SageMaker AI Studio Classic en la cuenta B.	1. En el panel de navegación de la SageMaker consola, selecciona Studio. 2. Seleccione su perfil de usuario y, a continuación, seleccione Open Studio. 3. En la sección Inicio, seleccione Open Launcher.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	4. En la sección Utilidades y archivos, seleccione Archivo de texto. 5. Copie el script de Example SageMaker shell script en la sección de información adicional de este patrón y, a continuación, pegue la sentencia en el nuevo archivo. Asegúrese de reemplazar todos los valores de los marcadores de posición en el script. 6. Haga clic derecho en la pestaña untitled.txt del nuevo archivo y, a continuación, seleccione Renombrar texto. En Nuevo nombre, escriba cross_account_git_clone.sh y, a continuación, seleccione Cambiar nombre.	

Tarea	Descripción	Habilidades requeridas
Invoque el script de intérprete de comandos desde el terminal del sistema.	1. En la sección de inicio de la SageMaker consola, selecciona Open Launcher. 2. En la sección Utilidades y archivos, seleccione Terminal del sistema. 3. En el terminal, ejecute el siguiente comando: `chmod u+x ./cross_account_git_clone.sh && ./cross_account_git_clone.sh` Has clonado tu CodeCommit repositorio en una cuenta cruzada de SageMaker AI Studio. Ahora puede ejecutar todos los comandos de Git desde el terminal del sistema.	AWS DevOps

Información adicional

Política de IAM de ejemplo

Para utilizar este ejemplo de política, debe hacer lo siguiente:

- `<CodeCommit_Repository_Region>` Región de AWS Sustitúyalo por el del repositorio.
- Sustituya `<Account_A_ID>` por la ID de cuenta para la cuenta A.
- `<CodeCommit_Repository_Name>`Sustitúyalo por el nombre de tu CodeCommit repositorio en la cuenta A.

```
{
```

```
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "codecommit:BatchGet*",
            "codecommit:Create*",
            "codecommit:DeleteBranch",
            "codecommit:Get*",
            "codecommit:List*",
            "codecommit:Describe*",
            "codecommit:Put*",
            "codecommit:Post*",
            "codecommit:Merge*",
            "codecommit:Test*",
            "codecommit:Update*",
            "codecommit:GitPull",
            "codecommit:GitPush"
        ],
        "Resource": [

 "arn:aws:codecommit:<CodeCommit_Repository_Region>:<Account_A_ID>:<CodeCommit_Repository_Name>
        ]
    }
]
}
```

Ejemplo de script SageMaker AI shell

Para utilizar este ejemplo de script, debe hacer lo siguiente:

- Sustituya <Account_A_ID> por la ID de cuenta para la cuenta A.
- Sustituya <Account_A_Role_Name> por el nombre del rol de IAM que ha creado anteriormente.
- <CodeCommit_Repository_Region>Sustitúyalo Región de AWS por el para el repositorio.
- <CodeCommit_Repository_Name>Sustitúyalo por el nombre de tu CodeCommit repositorio en la cuenta A.

```
#!/usr/bin/env bash
#Launch from system terminal
pip install --quiet git-remote-codecommit
```

```
mkdir -p ~/.aws
touch ~/.aws/config

echo "[profile CrossAccountAccessProfile]
region = <CodeCommit_Repository_Region>
credential_source=EcsContainer
role_arn = arn:aws:iam::<Account_A_ID>:role/<Account_A_Role_Name>
output = json" > ~/.aws/config

echo '[credential "https://git-
codecommit.<CodeCommit_Repository_Region>.amazonaws.com"]
        helper = !aws codecommit credential-helper $@ --profile
 CrossAccountAccessProfile
        UseHttpPath = true' > ~/.gitconfig

git clone codecommit::<CodeCommit_Repository_Region>://
CrossAccountAccessProfile@<CodeCommit_Repository_Name>
```

Extraer contenido de archivos PDF automáticamente con Amazon Textract

Tianxia Jia, Amazon Web Services

Resumen

Muchas organizaciones necesitan extraer información de los archivos PDF que se cargan en sus aplicaciones empresariales. Por ejemplo, una organización podría necesitar extraer con precisión la información de archivos PDF fiscales o médicos para realizar análisis tributarios o procesar reclamaciones médicas.

En la nube de Amazon Web Services (AWS), Amazon Textract extrae automáticamente la información (por ejemplo, texto impreso, formularios y tablas) de los archivos PDF y produce un archivo en formato JSON que contiene información del archivo PDF original. Puede usar Amazon Textract en la consola de administración de AWS o mediante la implementación de llamadas a la API. Le recomendamos que utilice llamadas a la API mediante programación para escalar y procesar automáticamente grandes cantidades de archivos PDF.

Cuando Amazon Textract procesa un archivo, crea la siguiente lista de objetos `Block`: páginas, líneas y palabras de texto, formularios (pares clave-valor), tablas y celdas, y elementos de selección. También se incluye otra información del objeto, por ejemplo, cuadros delimitadores IDs, intervalos de confianza y relaciones. Amazon Textract extrae la información del contenido en forma de cadenas. Es necesario contar con valores de datos correctamente identificados y transformados para que las aplicaciones posteriores puedan utilizarlos más fácilmente.

Este patrón describe un step-by-step flujo de trabajo para usar Amazon Textract para extraer automáticamente el contenido de los archivos PDF y procesarlo para obtener un resultado limpio. El patrón utiliza una técnica de coincidencia de plantillas para identificar correctamente el campo, el nombre clave y las tablas requeridos y, a continuación, aplica correcciones posteriores al procesamiento a cada tipo de datos. Puede utilizar este patrón para procesar distintos tipos de archivos PDF y, a continuación, escalar y automatizar este flujo de trabajo para procesar archivos PDF con un formato idéntico.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.

- Un bucket de Amazon Simple Storage Service (Amazon S3) existente en el que almacenar los archivos PDF una vez convertidos a formato JPEG para su procesamiento por Amazon Textract. Para obtener más información sobre los buckets de S3, consulte la Información general de los buckets en la documentación de Amazon S3.
- El cuaderno de Jupyter `Textract_PostProcessing.ipynb` (adjunto), instalado y configurado. Para obtener más información sobre las libretas Jupyter, consulta Crear una libreta Jupyter en la documentación de Amazon. SageMaker
- Archivos PDF existentes que tengan un formato idéntico.
- Conocimientos de Python.

Limitaciones

- Sus archivos PDF deben ser de buena calidad y claramente legibles. Se recomiendan archivos PDF nativos, pero puede utilizar documentos escaneados y convertidos a formato PDF si todas las palabras individuales se leen con claridad. Para obtener más información al respecto, consulte Preprocesamiento de documentos PDF con Amazon Textract: detección y eliminación de imágenes en el blog de AWS Machine Learning.
- Con los archivos de varias páginas, puede utilizar una operación asíncrona o combinar los archivos PDF en una única página y utilizar una operación síncrona. Para obtener más información sobre estas dos opciones, consulte Detección y análisis de texto en documentos de varias páginas y Detección y análisis de texto en documentos de una sola página en la documentación de Amazon Textract.

Arquitectura

El flujo de trabajo de este patrón ejecuta primero Amazon Textract sobre un archivo PDF de muestra (Primera ejecución) y, a continuación, lo ejecuta en archivos PDF que tengan un formato idéntico al del primer PDF (Ejecución repetida). El siguiente diagrama muestra el flujo de trabajo combinado de la Primera ejecución y la Ejecución repetida que extrae de forma automática y repetida el contenido de archivos PDF con idénticos formatos.

El diagrama muestra el siguiente flujo de trabajo de este patrón:

1. Convierta un archivo PDF a formato JPEG y almacénelo en un bucket de S3.
2. Llame a la API de Amazon Textract y analice el archivo JSON de respuesta de Amazon Textract.

3. Edite el archivo JSON añadiendo el par `KeyName:DataType` correcto para cada campo obligatorio. Cree un archivo `TemplateJSON` para la etapa de Ejecución repetida.
4. Defina las funciones de corrección posterior al procesamiento para cada tipo de datos (por ejemplo, flotante, entero y fecha).
5. Prepare los archivos PDF que tengan un formato idéntico al del primer archivo PDF.
6. Llame a la API de Amazon Textract y analice el JSON de respuesta de Amazon Textract.
7. Haga coincidir el archivo JSON analizado con el archivo `TemplateJSON`.
8. Implemente las correcciones posteriores al procesamiento.

El archivo de salida JSON final tiene el `KeyName` y el `Value` correctos para cada campo obligatorio.

Pila de tecnología de destino

- Amazon SageMaker
- Amazon S3
- Amazon Textract

Automatizar y escalar

Puede automatizar el flujo de trabajo de Ejecución repetida mediante una función de AWS Lambda que inicie Amazon Textract cuando se agregue un nuevo archivo PDF a Amazon S3. A continuación, Amazon Textract ejecuta los scripts de procesamiento y el resultado final se puede guardar en una ubicación de almacenamiento. Para obtener más información al respecto, consulte Uso de un desencadenador de Amazon S3 para invocar una función de Lambda en la documentación de Lambda.

Tools (Herramientas)

- Amazon SageMaker es un servicio de aprendizaje automático totalmente gestionado que le ayuda a crear y entrenar modelos de aprendizaje automático de forma rápida y sencilla y, a continuación, a implementarlos directamente en un entorno hospedado listo para la producción.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Textract facilita la adición de detección y análisis de texto de documentos a sus aplicaciones.

Epics

Primera ejecución

Tarea	Descripción	Habilidades requeridas
Convertir el archivo PDF.	Para preparar el archivo PDF para la primera ejecución , combínelo en una única página y conviértalo a formato JPEG para la operación síncrona (`Syn API`) de Amazon Textract. **Note** También puede utilizar la operación asíncrona (`Asyn API`) de Amazon Textract para archivos PDF de varias páginas.	Científico de datos, desarrollador
Analizar el JSON de respuesta de Amazon Textract.	Abra el cuaderno de Jupyter `Textract_PostProcessing.ipynb` (adjunto) y llame a la API de Amazon Textract mediante el siguiente código: `response = textract.analyze_document( Document={ 'S3Object': { 'Bucket': BUCKET, 'Name': '{}'.format(filename)`	Científico de datos, desarrollador

Tarea	Descripción	Habilidades requeridas

	<pre> }
	                },
	        FeatureTy
	pes=["TABLES",
	 "FORMS"])</pre>
	Analice y transforme el JSON de respuesta en un formulario y una tabla mediante el siguiente código:
	<pre>parseformKV=form_k
	v_from_JSON(response)
	parseformTable
	s=get_tables_fromJ
	SON(response)</pre>	

Editar el archivo de TemplateJSON.	Edite el JSON analizado de cada `KeyName` y el `DataType` correspondiente (por ejemplo, cadena, flotante, entero o fecha) y las cabeceras de las tablas (por ejemplo, `ColumnNames` y `RowNames`). Esta plantilla se usa para cada tipo de archivo PDF individual, lo que significa que la plantilla se puede reutilizar para archivos PDF que tengan un formato idéntico.	Científico de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
Definir las funciones de corrección posterior al procesamiento.	Los valores de la respuesta de Amazon Textract para el archivo `TemplateJSON` son cadenas. No hay diferenciación por fecha, flotante, entero o divisa. Estos valores se deben convertir al tipo de datos correcto para su caso de uso posterior. Corrija cada tipo de datos según el archivo `TemplateJSON` mediante el siguiente código: `finalJSON=postprocessingCorrection(parsedJSON,templateJSON)`	Científico de datos, desarrollador

Ejecución repetida

Tarea	Descripción	Habilidades requeridas
Prepare los archivos PDF.	Para preparar los archivos PDF, combínelos en una sola página y conviértalos a formato JPEG para la operación síncrona (`Syn API`) de Amazon Textract. **Note** También puede utilizar la operación asíncrona	Científico de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	(Asyn API) de Amazon Textract para archivos PDF de varias páginas.	
Llamar a la API de Amazon Textract.	Para llamar a la API de Amazon Textract, utilice el siguiente código: `response = textract.analyze_document( Document={ 'S3Object': { 'Bucket': BUCKET, 'Name': '{}'.format(filename) } }, FeatureTypes=["TABLES", "FORMS"])`	Científico de datos, desarrollador
Analizar el JSON de respuesta de Amazon Textract.	Analice y transforme el JSON de respuesta en un formulario y una tabla mediante el siguiente código: `parseformKV=form_kv_from_JSON(response) parseformTables=get_tables_fromJSON(response)`	Científico de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
Cargar el archivo TemplateJSON y hacerlo coincidir con el JSON analizado.	Utilice el archivo `TemplateJSON` para extraer los pares clave-valor y la tabla correctos mediante los siguientes comandos: `form_kv_corrected= form_kv_correction (parseformKV,templateJSON) form_table_corrected=form_Table_correction(parseformTables, templateJSON) form_kv_table_corrected_final={**form_kv_corrected , **form_table_corrected}`	Científico de datos, desarrollador
Correcciones posteriores al procesamiento.	Use `DataType` en el archivo `TemplateJSON` y funciones de procesamiento posterior para corregir los datos mediante el siguiente código: `finalJSON=postprocessingCorrection(form_kv_table_corrected_final,templateJSON)`	Científico de datos, desarrollador

Recursos relacionados

- Extracción automática de texto y datos estructurados de documentos con Amazon Textract
- Extracción de texto y datos estructurados con Amazon Textract
- Recursos de Amazon Textract

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Cree un modelo de previsión de arranque en frío utilizando DeepAR para series temporales en SageMaker Amazon AI Studio Lab

Ivan Cui y Eyal Shacham, Amazon Web Services

Resumen

No importa si quiere asignar los recursos de manera más eficiente al tráfico web, pronosticar la demanda de personal por parte de los pacientes o anticipar las ventas de los productos de una empresa, la previsión es una herramienta esencial. La previsión en inicio frío crea previsiones para series temporales que contienen pocos datos históricos, como un producto nuevo que acaba de presentarse en el mercado minorista. Este patrón utiliza el algoritmo de previsión DeepAR de Amazon SageMaker AI para entrenar un modelo de previsión de arranque en frío y demuestra cómo realizar previsiones de los elementos de arranque en frío.

DeepAR es un algoritmo de aprendizaje supervisado para series temporales (monodimensionales) escalares y de previsión que emplean redes neuronales recurrentes (RNN). DeepAR se centra en entrenar un único modelo de forma conjunta para todas las series temporales de los productos relacionados.

Los métodos tradicionales de previsión de series temporales, como el promedio móvil integrado autorregresivo (ARIMA) o el suavizado exponencial (ETS), se basan en gran medida en las series temporales históricas de cada producto individual. Por lo tanto, esos métodos no son eficaces para la previsión de inicio en frío. Cuando el conjunto de datos contiene cientos de series temporales relacionadas, DeepAR supera el estándar ARIMA y los métodos ETS. También puede utilizar el modelo entrenado para generar previsiones para series temporales nuevas que son similares a aquellas para las que ha recibido capacitación.

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- Un dominio de Amazon SageMaker AI.
- Una aplicación de Amazon SageMaker AI Studio Lab o Jupiter lab.

- Un bucket de Amazon Simple Storage Service (Amazon S3) con permisos de lectura y escritura.
- Conocimientos de programación en Python.
- Conocimientos sobre el uso de un cuaderno de Jupyter.

Limitaciones

- Si se invoca el modelo de previsión sin ningún dato histórico, se devolverá un error. Si se invoca el modelo con un mínimo de puntos de datos históricos, se obtendrán predicciones inexactas con un alto grado de fiabilidad. Este patrón sugiere un enfoque para resolver estas limitaciones conocidas de la previsión de inicios en frío.
- Algunas Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- Python versión 3.10 o posterior.
- El cuaderno del patrón se probó en Amazon SageMaker AI Studio en una instancia ml.t3.medium con el núcleo Python 3 (Data Science).

Arquitectura

En el siguiente diagrama se muestran los componentes de la arquitectura y el flujo de trabajo de esta aplicación.

El flujo de trabajo realiza las siguientes tareas:

1. Los archivos de entrada de datos de entrenamiento y prueba se sintetizan y luego se cargan en un bucket de Amazon S3. Estos datos incluyen varias series temporales con características categóricas y dinámicas, junto con valores objetivo (por predecir). El cuaderno de Jupyter visualiza los datos para que pueda comprender mejor los requisitos de los datos de entrenamiento y los valores previstos esperados.
2. Se crea un trabajo de optimización de hiperparámetros para entrenar el modelo y encontrar el mejor modelo en función de las métricas predefinidas.

3. Los archivos de entrada se descargan del bucket de Amazon S3 a cada instancia de los trabajos de ajuste de hiperparámetros.
4. Una vez que el trabajo de ajuste selecciona el mejor modelo en función del umbral predefinido del ajustador, el modelo se implementa como un SageMaker punto final de IA.
5. Así pues, el modelo implementado estará listo para la invocación, donde sus predicciones se validan con los datos de la prueba.

El cuaderno muestra la precisión del modelo para predecir los valores objetivo cuando el número adecuado de puntos de datos históricos está disponible. Sin embargo, cuando se invoca al modelo con menos puntos de datos históricos (que representan un producto pasivo), las predicciones del modelo no coinciden con los datos de las pruebas originales, ni siquiera dentro de los niveles de confianza del modelo. En el patrón, se crea un nuevo modelo para productos pasivos en el que la longitud de contexto inicial (puntos pronosticados) se define como la cantidad de puntos históricos disponibles; a continuación, un nuevo modelo se entrena de forma iterativa a medida que se adquieren nuevos puntos de datos. El cuaderno muestra que el modelo tendrá predicciones precisas siempre que la cantidad de puntos de datos históricos se acerque a la longitud de su contexto.

Tools (Herramientas)

Servicios de AWS

- AWS Identity and Access Management (IAM) le ayuda a gestionar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- Amazon SageMaker AI es un servicio de aprendizaje automático (ML) gestionado que le ayuda a crear y entrenar modelos de aprendizaje automático para luego implementarlos en un entorno hospedado listo para la producción.
- Amazon SageMaker AI Studio es un entorno de desarrollo integrado (IDE) basado en la web para el aprendizaje automático que le permite crear, entrenar, depurar, implementar y supervisar sus modelos de aprendizaje automático.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

- Python es un lenguaje de programación informático de uso general.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub DeepAR- ColdProduct -Patern.

Prácticas recomendadas

- Entrene su modelo en un entorno virtual y utilice siempre el control de versiones para lograr la máxima reproducibilidad.
- Incluya tantas características categóricas de alta calidad como pueda para obtener el mejor modelo predictivo.
- Asegúrese de que los metadatos contengan elementos categóricos similares para que el modelo pueda deducir adecuadamente las predicciones de los productos de inicio en frío.
- Ejecute un trabajo de optimización de hiperparámetros para obtener el modelo predictivo más alto.
- En este patrón, el modelo que desarrolle tiene una longitud de contexto de 24 horas, lo que significa que predecirá las próximas 24 horas. Si intenta predecir las próximas 24 horas cuando tiene menos de 24 horas de datos históricos, la precisión de la predicción del modelo se degradará linealmente en función de la cantidad de puntos de datos históricos. Para mitigar este problema, cree un modelo nuevo para cada conjunto de puntos de datos históricos hasta que este número alcance la longitud de predicción (contexto) deseada. Por ejemplo, comience con un modelo de longitud de contexto de 2 horas y, a continuación, aumente el modelo en 4 horas, 8 horas, 16 horas y 24 horas respectivamente.

Epics

Inicie su aplicación SageMaker AI Studio Classic

Tarea	Descripción	Habilidades requeridas
Inicie el entorno del cuaderno.	1. Inicia sesión en la página Consola de administr ación de AWS de inicio de SageMaker AI Studio y ábrela. Luego, seleccione Abrir Studio. 2. En el panel de navegació n izquierdo, elija el ícono	Científico de datos

Tarea	Descripción	Habilidades requeridas
	Studio Classic en Aplicaciones. A continuación, seleccione el botón Abrir en la lista de aplicaciones. Para obtener más información, consulte Lanzamiento de Amazon SageMaker AI Studio en la documentación de SageMaker IA.	

Creación y activación del cuaderno

Tarea	Descripción	Habilidades requeridas
Configure el entorno virtual para el entrenamiento del modelo.	Para configurar el entorno virtual para el entrenamiento del modelo, haga lo siguiente: 1. Descargue el `deepar_synthetic.ipynb` cuaderno desde el GitHub repositorio de este patrón a su máquina local. 2. En Amazon SageMaker AI Studio Classic, elija el icono Cargar archivos en la barra de menús de Studio Classic y seleccione el bloc de notas descargado. 3. En el panel de navegación izquierdo del explorador de archivos, seleccione el cuaderno. Siga las	Científico de datos

Tarea	Descripción	Habilidades requeridas
	instrucciones para configurar un entorno de cuaderno. Seleccione la imagen de Ciencia de datos 3.0 y el núcleo de Python 3 Para obtener más información, consulte Cargar archivos a SageMaker AI Studio Classic en la documentación de SageMaker AI.	
Cree y valide un modelo de previsión.	• Siga las instrucciones del cuaderno para crear los datos de entrenamiento y prueba, entrene el modelo y, a continuación, invóquelo. • Confirme la precisión de las predicciones del modelo cuando se proporcionan los puntos de datos históricos adecuados.	Científico de datos

Recursos relacionados

- Hiperparámetros DeepAR
- Predecir la demanda de lanzamientos de nuevos productos mediante el uso de servicios de aprendizaje automático AWS
- Inicie Amazon SageMaker AI Studio Classic
- Utilice el algoritmo de SageMaker previsión AI DeepAR

Cree un MLOps flujo de trabajo con Amazon SageMaker AI y Azure DevOps

Deepika Kumar, Sara van de Moosdijk y Philips Kokoh Prasetyo, Amazon Web Services

Resumen

Las operaciones de aprendizaje automático (MLOps) son un conjunto de prácticas que automatizan y simplifican los flujos de trabajo y las implementaciones del aprendizaje automático (ML). MLOps se centra en automatizar el ciclo de vida del aprendizaje automático. Ayuda a garantizar que los modelos no solo se desarrollen, sino que también se implementen, supervisen y reentrenen de manera sistemática y repetida. Aporta DevOps principios al ML. MLOps da como resultado un despliegue más rápido de los modelos de aprendizaje automático, una mayor precisión a lo largo del tiempo y una mayor seguridad de que proporcionan un valor empresarial real.

Las organizaciones suelen tener DevOps herramientas y soluciones de almacenamiento de datos existentes antes de iniciar su MLOps viaje. Este patrón muestra cómo aprovechar los puntos fuertes de Microsoft Azure y AWS. Le ayuda a integrar Azure DevOps con Amazon SageMaker AI para crear un MLOps flujo de trabajo.

La solución simplifica el trabajo entre Azure y AWS. Puede usar Azure para el desarrollo y AWS el aprendizaje automático. Favorece un proceso eficaz para crear modelos de machine learning de principio a fin, que incluye la gestión de datos, el entrenamiento y la implementación en AWS. Para aumentar la eficiencia, administra estos procesos a través de las DevOps canalizaciones de Azure. La solución es aplicable a las operaciones de modelos básicos (FMOps) y a las operaciones de modelos de lenguaje de gran tamaño (LLMOps) en la IA generativa, lo que incluye ajustes precisos, bases de datos vectoriales y administración rápida.

Requisitos previos y limitaciones

Requisitos previos

- Suscripción a Azure: acceso a los servicios de Azure, como Azure DevOps, para configurar las canalizaciones de integración e implementación continuas (CI/CD).
- Cuenta de AWS activa: permisos para usar lo que Servicios de AWS se usa en este patrón.
- Datos: acceso a datos históricos para entrenar el modelo de machine learning.
- Familiaridad con los conceptos de ML: comprensión de Python, Jupyter Notebooks y desarrollo de modelos de machine learning.

- Configuración de seguridad: configuración adecuada de los roles, políticas y permisos en Azure y AWS para garantizar la transferencia y el acceso seguros a los datos.
- Base de datos vectorial (opcional): si utiliza un enfoque de generación aumentada por recuperación (RAG) y un servicio de terceros para la base de datos vectorial, necesitará acceder a la base de datos vectorial externa.

Limitaciones

- Esta guía no trata las transferencias de datos seguras entre nubes. Para obtener más información sobre de las transferencias de datos entre nubes, consulte Soluciones de AWS para sistemas híbridos y multinube.
- Las soluciones multinube pueden aumentar la latencia del procesamiento de datos en tiempo real y la inferencia del modelo.
- Esta guía proporciona un ejemplo de una MLOps arquitectura de cuentas múltiples. Los ajustes son necesarios en función del aprendizaje automático y la AWS estrategia.
- Esta guía no describe el uso de AI/ML servicios distintos de Amazon SageMaker AI.
- Algunos Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

Arquitectura de destino

La arquitectura de destino integra Azure DevOps con Amazon SageMaker AI, lo que crea un flujo de trabajo de aprendizaje automático entre nubes. Utiliza Azure para CI/CD los procesos y la SageMaker IA para el entrenamiento y la implementación de modelos de aprendizaje automático. Describe el proceso de obtención de datos (de fuentes como Amazon S3, Snowflake y Azure Data Lake) mediante el desarrollo e implementación de modelos. Los componentes clave incluyen CI/CD las canalizaciones para la creación e implementación de modelos, la preparación de datos, la administración de la infraestructura y Amazon SageMaker AI para el entrenamiento y el ajuste, la evaluación y la implementación de modelos de aprendizaje automático. Esta arquitectura está diseñada para proporcionar flujos de trabajo de ML eficientes, automatizados y escalables en todas las plataformas en la nube.

La arquitectura consta de los siguientes componentes:

1. Los científicos de datos realizan experimentos de ML en la cuenta de desarrollo para explorar diferentes enfoques para los casos de uso de ML mediante diversos orígenes de datos. Los científicos de datos realizan pruebas y ensayos unitarios y, para realizar un seguimiento de sus experimentos, pueden utilizar Amazon SageMaker AI con MLflow. En el desarrollo de modelos de IA generativa, los científicos de datos ajustan los modelos básicos del centro de modelos Amazon SageMaker AI JumpStart . Tras la evaluación del modelo, los científicos de datos insertan el código y lo combinan en el repositorio Model Build, que está alojado en Azure. DevOps Este repositorio contiene código para poder hacer una canalización de creación de modelos de varios pasos.
2. En Azure DevOps, la canalización de creación de modelos, que proporciona una integración continua (CI), se puede activar automática o manualmente al fusionar el código con la rama principal. En la cuenta de automatización, esto activa la canalización de SageMaker IA para el preprocesamiento de los datos, el entrenamiento y el ajuste de los modelos, la evaluación de los modelos y el registro condicional de los modelos en función de la precisión.
3. La cuenta de automatización es una cuenta central en todas las plataformas de aprendizaje automático que aloja entornos de aprendizaje automático (Amazon ECR), modelos (Amazon S3), metadatos de modelos (SageMaker AI Model Registry), funciones (SageMaker AI Feature Store), canalizaciones automatizadas (SageMaker AI Pipelines) e información de registros de aprendizaje automático (). CloudWatch Si se trata de una carga de trabajo de IA generativa, es posible que necesite hacer evaluaciones adicionales para las peticiones de las aplicaciones posteriores. Una aplicación de administración rápida de peticiones le permitirá agilizar y automatizar el proceso. Esta cuenta permite la volver a usar los recursos de ML y aplica las prácticas recomendadas para acelerar la entrega de casos de uso de ML.
4. La última versión del modelo se añade al Registro de modelos de SageMaker IA para su revisión. Realiza un seguimiento de las versiones de los modelos y de los artefactos respectivos (linaje y metadatos). También administra el estado del modelo (aprobado, rechazado o pendiente) y la versión para su implementación posterior.
5. Una vez que se apruebe un modelo entrenado en Model Registry mediante la interfaz del estudio o una llamada a la API, se puede enviar un evento a Amazon EventBridge. EventBridge inicia la canalización de Model Deploy en Azure DevOps.
6. La canalización de la implementación de modelos, que proporciona una implementación continua (CD), extrae la fuente del repositorio de implementación de modelos. El origen contiene el código, la configuración para la implementación del modelo y los scripts de prueba para establecer puntos

de referencia de calidad. La canalización de implementación de modelos se puede adaptar a su tipo de inferencia.

7. Tras realizar las comprobaciones de control de calidad, la canalización de implementación de modelos implementa el modelo en la cuenta transitoria. La cuenta transitoria es una copia de la cuenta de producción y se utiliza para las pruebas y la evaluación de la integración. En el caso de querer realizar una transformación por lotes, la canalización de implementación de modelos puede actualizar automáticamente el proceso de inferencia en lotes para utilizar la última versión aprobada del modelo. Para realizar una inferencia asíncrona, sin servidor o en tiempo real, puede configurar o actualizar el punto de conexión del modelo correspondiente.
8. Tras realizar correctamente las pruebas en la cuenta transitoria, se puede implementar un modelo en la cuenta de producción mediante una aprobación manual a través de la canalización de implementación de modelos. Esta canalización proporciona un punto de conexión de producción en la etapa Implementación y producción, que incluye la supervisión del modelo y un mecanismo de valoración de los datos.
9. Una vez que el modelo esté en producción, utilice herramientas como SageMaker AI Model Monitor y SageMaker AI Clarify para identificar los sesgos, detectar desviaciones y supervisar continuamente el rendimiento del modelo.

Automatización y escala

Utilice infraestructura como código (IaC) para implementar automáticamente en varias cuentas y entornos. Al automatizar el proceso de configuración de un MLOps flujo de trabajo, es posible separar los entornos que utilizan los equipos de aprendizaje automático que trabajan en diferentes proyectos. AWS CloudFormationle ayuda a modelar, aprovisionar y gestionar AWS los recursos al tratar la infraestructura como código.

Tools (Herramientas)

Servicios de AWS

- Amazon SageMaker AI es un servicio de aprendizaje automático gestionado que le ayuda a crear y entrenar modelos de aprendizaje automático para luego implementarlos en un entorno hospedado listo para la producción.
- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos. En este patrón, Amazon S3 se utiliza para el almacenamiento de datos y se integra con la SageMaker IA para el entrenamiento de modelos y los objetos de modelo.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice. En este patrón, Lambda se utiliza para las tareas procesamiento previas y posteriores de los datos.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable. En este patrón, almacena los contenedores Docker que la SageMaker IA utiliza como entornos de entrenamiento e implementación.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Siguiendo este patrón, EventBridge organiza flujos de trabajo basados en eventos o basados en el tiempo que inician el reentrenamiento o la implementación automáticos del modelo.
- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket APIs a cualquier escala. En este patrón, se utiliza para crear un punto de entrada único orientado al exterior para los puntos finales de SageMaker IA.
- En el caso de las aplicaciones RAG, puede Servicios de AWS utilizarlas, como Amazon OpenSearch Service y Amazon RDS for PostgreSQL, para almacenar las incrustaciones vectoriales que proporcionan al LLM sus datos internos.

Otras herramientas

- Azure le DevOps ayuda a administrar las CI/CD canalizaciones y a facilitar la creación, las pruebas y la implementación del código.
- Azure Data Lake Storage o Snowflake son posibles orígenes de datos de entrenamiento de terceros para los modelos de ML.
- Pinecone, Milvus o ChromaDB son posibles bases de datos vectoriales de terceros para almacenar incrustaciones vectoriales.

Prácticas recomendadas

Antes de implementar cualquier componente de este MLOps flujo de trabajo multinube, lleve a cabo las siguientes actividades:

- Defina y comprenda el flujo de trabajo de machine learning y las herramientas necesarias para que funcione adecuadamente. Los diferentes casos de uso requieren diferentes flujos de trabajo y componentes. Por ejemplo, es posible que necesite un almacén de características para la reutilización de características y la inferencia de baja latencia en un caso de uso de personalización, pero puede que no sea necesario para otros casos de uso. Para personalizar correctamente la arquitectura, es necesario comprender el flujo de trabajo objetivo, los requisitos de los casos de uso y los métodos de colaboración preferidos del equipo de ciencia de datos.
- Establezca una separación clara de responsabilidades para cada componente de la arquitectura. La distribución del almacenamiento de datos entre Azure Data Lake Storage, Snowflake y Amazon S3 puede aumentar la complejidad y los costos. Si es posible, elija un mecanismo de almacenamiento coherente. Del mismo modo, evite usar una combinación de DevOps servicios de Azure y AWS, o una combinación de servicios de Azure y AWS ML.
- Elija uno o más modelos y conjuntos de datos existentes para realizar las end-to-end pruebas del MLOps flujo de trabajo. Los artefactos de prueba deben reflejar los casos de uso reales que los equipos de ciencia de datos desarrollen cuando la plataforma entre en la fase de producción.

Epics

Diseñe su arquitectura MLOps

Tarea	Descripción	Habilidades requeridas
Identifique los orígenes de datos	En función de los casos de uso actuales y futuros, las fuentes de datos disponibles y los tipos de datos (como los datos confidenciales), documente las fuentes de datos que deben integrarse con la MLOps plataforma. Los datos se pueden almacenar	Ingeniero de datos, científico de datos, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	en Amazon S3, Azure Data Lake Storage, Snowflake u otros orígenes. En el caso de las cargas de trabajo de IA generativa, los datos también pueden incluir una base de conocimiento en la que se base la respuesta generada. Estos datos se almacenan como incrustaciones vectoriales en bases de datos vectoriales. Cree un plan para integrar estos orígenes con su plataforma y garantizar el acceso a los recursos correctos.	
Elija los servicios aplicables.	Personalice la arquitectura añadiendo o quitando servicios en función del flujo de trabajo que quiera usar el equipo de ciencia de datos, los orígenes de datos aplicables y la arquitectura de nube existente. Por ejemplo, los ingenieros de datos y los científicos de datos pueden realizar el preprocesamiento de datos y la ingeniería de características en SageMaker AI o Amazon EMR. AWS Glue Es poco probable que necesiten usar los tres servicios.	Administrador de AWS, ingeniero de datos, científico de datos, ingeniero de machine learning

Tarea	Descripción	Habilidades requeridas
Analice los requisitos de seguridad.	Reúna y documente los requisitos de seguridad. Esto incluye determinar lo siguiente : • Qué equipos o ingenieros pueden acceder a orígenes de datos específicas • Qué equipos o ingenieros pueden acceder a modelos básicos previamente entrenados • Si los equipos pueden acceder al código y los modelos de otros equipos • Qué permisos (si los hay) deben tener los miembros del equipo para las cuentas que no son de desarrollo • Qué medidas de seguridad deben implementarse para la transferencia de datos entre nubes Para obtener más informaci ón sobre cómo proteger las cargas de trabajo de IA generativa, consulte Cómo proteger la IA generativa: una introducción a la matriz de alcance de la seguridad de la IA generativa (entrada del blog).AWS	Administrador de AWS, arquitecto de la nube

Configurar AWS Organizations

Tarea	Descripción	Habilidades requeridas
Configurar AWS Organizations.	AWS Organizations Configúrelo desde la raíz Cuenta de AWS. Esto le ayuda a administrar las cuentas subsiguientes que cree como parte de una MLOps estrategia de cuentas múltiples. Para obtener más información, consulte la Documentación de AWS Organizations.	Administrador de AWS

Configuración del entorno de desarrollo y control de versiones

Tarea	Descripción	Habilidades requeridas
Crea una cuenta AWS de desarrollo.	Cree un espacio Cuenta de AWS en el que los ingenieros y científicos de datos tengan permisos para experimentar y crear modelos de aprendizaje automático. Para obtener instrucciones, consulte Crear una cuenta de miembro en su organización en la AWS Organizations documentación.	Administrador de AWS
Creación de un repositorio de creación de modelos.	Cree un repositorio de Git en Azure donde los científicos de datos puedan enviar el código de creación e implementación de sus modelos una vez finalizada la fase de	DevOps ingeniero, ingeniero de aprendizaje automático

Tarea	Descripción	Habilidades requeridas
	experimentación. Para obtener instrucciones, consulte Configurar un repositorio de Git en la DevOps documentación de Azure.	
Cree un repositorio de implementación de modelos.	Cree un repositorio de Git en Azure que almacene el código y las plantillas de implementación estándar. Debe incluir código para cada opción de implementación que utilice la organización, tal como se indicó en la fase de diseño. Por ejemplo, debe incluir puntos de conexión en tiempo real, puntos de conexión asíncronos, inferencias sin servidor o transformaciones por lotes. Para obtener instrucciones, consulte Configurar un repositorio de Git en la DevOps documentación de Azure.	DevOps ingeniero, ingeniero de aprendizaje automático

Tarea	Descripción	Habilidades requeridas
Cree un repositorio de Amazon ECR.	Configure un repositorio de Amazon ECR que almacene los entornos de ML aprobados como imágenes de Docker. Permita que los científicos de datos y los ingenieros de ML definan nuevos entornos. Para obtener instrucciones, consulte Creación de un repositorio privado en la documentación de Amazon ECR.	Ingeniero de ML
Configura SageMaker AI Studio.	Configura SageMaker AI Studio en la cuenta de desarrollo de acuerdo con los requisitos de seguridad previamente definidos, las herramientas de ciencia de datos preferidas (como MLflow) y el entorno de desarrollo integrado (IDE) preferido. Utilice las configuraciones del ciclo de vida para automatizar la instalación de las funciones clave y crear un entorno de desarrollo uniforme para los científicos de datos. Para obtener más información, consulte Amazon SageMaker AI Studio y el servidor MLflow de seguimiento en la documentación de SageMaker IA.	Científico de datos, ingeniero de ML, ingeniero de peticiones

Integre las CI/CD canalizaciones

Tarea	Descripción	Habilidades requeridas
Cree una cuenta de Automatio n.	Cree un Cuenta de AWS lugar en el que se ejecuten las canalizaciones y los trabajos automatizados. Puede dar a los equipos de ciencia de datos acceso de lectura a esta cuenta. Para obtener instrucciones, consulte Crear una cuenta de miembro en su organización en la AWS Organizations documentación.	Administrador de AWS
Configure un registro de modelos.	Configura el registro de modelos de SageMaker IA en la cuenta de automatización. Este registro almacena los metadatos de los modelos de ML y permite que determina dos científicos de datos o líderes de equipo aprueben o rechacen modelos. Para obtener más informaci ón, consulte Registrar e implementar modelos con Model Registry en la documentación de SageMaker IA.	Ingeniero de ML
Cree una canalización de creación de modelos.	Cree una CI/CD canalizac ión en Azure que se inicie de forma manual o automática cuando el código se envíe al repositorio de Model Build. La	DevOps ingeniero, ingeniero de ML

Tarea	Descripción	Habilidades requeridas
	canalización debería revisar el código fuente y crear o actualizar una canalización de SageMaker IA en la cuenta de Automation. La canalizac ión debe añadir un modelo nuevo al registro de modelos. Para obtener más informaci ón acerca de la creación de una canalización, consulte la documentación de Azure Pipelines.	

Desaroollo del paquete de implementación.

Tarea	Descripción	Habilidades requeridas
Cree cuentas AWS de puesta en escena y despliegue.	Cree modelos Cuentas de AWS de aprendizaje automático para la puesta en escena y el despliegue de ellos. Estas cuentas deben ser idénticas para poder realizar pruebas precisas de los modelos durante la fase de transición antes de pasar a la fase de producció n. Puede dar a los equipos de ciencia de datos acceso de lectura a esta cuenta transitor ia. Para obtener instrucciones, consulte Crear una cuenta de miembro en su organizac	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	ión en la AWS Organizations documentación.	
Configure los buckets de S3 para la supervisión de modelos.	Complete este paso si desea habilitar la supervisión de modelos para los modelos implementados que crea la canalización de implement ación de modelos. Cree buckets de Amazon S3 para almacenar los datos de entrada y salida. Para más información sobre cómo crear buckets de S3, consulte Creación de un bucket en la documentación de Amazon S3. Configure los permisos entre cuentas para que los trabajos de supervisión de modelos automatizados se ejecuten en la cuenta de Automation. Para obtener más información, consulte Supervisar la calidad de los datos y los modelos en la documentación sobre SageMaker IA.	Ingeniero de ML

Tarea	Descripción	Habilidades requeridas
Cree una canalización de implementación de modelos.	Cree una CI/CD canalización en Azure que comience cuando se apruebe un modelo en el registro de modelos. La canalización debe comprobar el código fuente y el artefacto del modelo, crear las plantillas de infraestructura para implementar el modelo en las cuentas transitorias y de producción, implementar el modelo en la cuenta transitoria, ejecutar pruebas automatizadas, esperar a la aprobación manual e implementar el modelo aprobado en la cuenta de producción. Para obtener más información acerca de la creación de una canalización, consulte la documentación de Azure Pipelines.	DevOps ingeniero, ingeniero de aprendizaje automático

(Opcional) Automatización de la infraestructura del entorno de ML

Tarea	Descripción	Habilidades requeridas
Cree AWS CDK nuestras CloudFormation plantillas.	Defina AWS Cloud Development Kit (AWS CDK) AWS CloudFormation nuestras plantillas para todos los entornos que deban implementarse automáticamente. Esto puede incluir el entorno de desarrollo, el	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	entorno de automatización y los entornos transitorios y de implementación. Para obtener más información, consulte la documentación de AWS CDK y CloudFormation.	
Cree una canalización de infraestructura.	Cree una CI/CD canalización en Azure para el despliegue de la infraestructura. Un administrador puede iniciar esta canalización para crear nuevos entornos Cuentas de AWS y configurar los que necesite el equipo de aprendizaje automático.	DevOps ingeniero

Resolución de problemas

Problema	Solución
Supervisión y detección de desviaciones insuficientes: una supervisión inadecuada puede provocar que no se detecten los problemas de rendimiento del modelo o la deriva de datos.	Refuerce los marcos de monitoreo con herramientas como Amazon CloudWatch, SageMaker AI Model Monitor y SageMaker AI Clarify. Configure alertas para tomar medidas inmediatas en caso de tener alguno de los problemas identificados.
Errores de activación de la canalización de CI: es DevOps posible que la canalización de CI de Azure no se active al fusionar el código debido a una mala configuración.	Comprueba la configuración del DevOps proyecto de Azure para asegurarte de que los webhooks estén correctamente configurados y apunten a los puntos finales de SageMaker IA correctos.

Problema	Solución
Gobernanza: es posible que la cuenta central de Automation no aplique las prácticas recomendadas en todas las plataformas de ML, lo que provocará flujos de trabajo incoherentes.	Audite la configuración de la cuenta de Automation y asegúrese de que todos los entornos y modelos de ML se ajusten a las prácticas recomendadas y políticas predefini das.
Retrasos en la aprobación del registro de modelos: esto ocurre cuando hay un retraso en la comprobación y aprobación del modelo, ya sea porque los usuarios tardan en revisarlo o por problemas técnicos.	Implemente un sistema de notificación para alertar a las partes interesadas sobre los modelos que están pendientes de aprobación y agilice el proceso de revisión.
Errores en los eventos de implementación de modelos: los eventos enviados para iniciar los procesos de implementación del modelo pueden devolver errores y provocar retrasos en el proceso de implementación.	Confirma que Amazon EventBridge tiene los permisos y los patrones de eventos correctos para invocar las DevOps canalizaciones de Azure correctamente.
Cuellos de botella en la implementación de producción: los procesos de aprobació n manual pueden crear cuellos de botella y retrasar la implementación de los modelos en producción.	Para optimizar el flujo de trabajo de aprobació n del proceso de implementación del modelo, favorezca las revisiones oportunas y los canales de comunicación claros.

Recursos relacionados

AWS documentación

- Documentación de Amazon SageMaker AI
- Machine Learning Lens (marco AWS bien diseñado)
- Planificar con éxito MLOps (orientación AWS prescriptiva)

Otros recursos AWS

- MLOps hoja de ruta básica para empresas con Amazon SageMaker AI (AWS entrada del blog)

- AWS Summit ANZ 2022: End-to-end MLOps para arquitectos (YouTube vídeo)
- FMOps/LLMOps: Operacionalice la IA generativa y sus diferencias con ella MLOps (AWS entrada del blog)
- Operacionalice la evaluación de LLM a gran escala con Amazon SageMaker AI Clarify y sus MLOps servicios (AWS entrada de blog)
- El papel de las bases de datos vectoriales en las aplicaciones de IA generativa (AWS entrada del blog)

Documentación de Azure

- Documentación de Azure DevOps
- Documentación de Azure Pipelines

Configure el registro de invocación de modelos en Amazon Bedrock mediante AWS CloudFormation

Vikramaditya Bhatnagar, Amazon Web Services

Resumen

Puede configurar Amazon Bedrock para recopilar registros de invocación y datos de entrada y de salida del modelo para todas las invocaciones del modelo en su Cuenta de AWS. Esta es una práctica recomendada para crear aplicaciones de IA generativa sólidas con Amazon Bedrock. Puede almacenar los registros de invocación de modelos en un grupo de CloudWatch registros de Amazon Logs, en un bucket de Amazon Simple Storage Service (Amazon S3) o en ambos. Tener los datos de registro en CloudWatch Logs le ayuda a crear filtros de métricas, alarmas y paneles personalizados. Amazon S3 es ideal para replicar datos en Regiones de AWS o para almacenamiento a largo plazo, según lo regido por las políticas de su organización.

Este patrón proporciona una AWS CloudFormation plantilla de ejemplo que utiliza un enfoque de infraestructura como código (IaC) para configurar el registro de invocaciones de modelos para Amazon Bedrock. La plantilla configura el almacenamiento de CloudWatch registros tanto en Logs como en Amazon S3.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Los siguientes permisos:
  - Permisos para crear CloudFormation pilas
  - Permisos para acceder a Amazon Bedrock
  - Permisos para crear buckets de Amazon S3 y acceder a ellos
  - Permisos para crear grupos de CloudWatch registros y acceder a ellos
  - Permisos para crear AWS Lambda funciones y acceder a ellas
  - Permisos para crear claves y acceder a AWS Key Management Service ellas AWS KMS

Limitaciones

Este patrón registra las invocaciones de modelos tanto en CloudWatch Logs como en Amazon S3. No permite elegir solo uno de estos dos servicios.

Arquitectura

Arquitectura de destino

La CloudFormation plantilla proporciona los siguientes recursos en su destino Cuenta de AWS:

- Un grupo CloudWatch de registros para almacenar los registros de invocación de modelos
- Un bucket de Amazon S3 para almacenar registros de invocaciones de modelos y una política de bucket correspondiente
- Un bucket de Amazon S3 para almacenar registros de acceso del lado de servidor y una política de bucket correspondiente
- AWS Lambda Función que configura los ajustes de registro en Amazon Bedrock
- Un alias AWS KMS key clave y su correspondiente
- Un rol de servicio AWS Identity and Access Management (IAM) para Amazon Bedrock

El siguiente diagrama muestra cómo se almacenan los registros de invocación después de implementar la CloudFormation pila asociada a este patrón. Amazon Bedrock publica datos de registro cuando el modelo básico entrega texto, una imagen, un video o datos incrustados. Como se muestra en el diagrama, los buckets de Amazon S3 y el grupo de CloudWatch registros Logs se cifran con un AWS KMS key.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario envía una consulta a un modelo básico en Amazon Bedrock.
2. Amazon Bedrock asume el rol de servicio de IAM.
3. Amazon Bedrock genera datos de registro y los almacena en un grupo de CloudWatch registros y en un bucket de Amazon S3.
4. Si un usuario lee, carga o elimina cualquier archivo del bucket de Amazon S3 que contenga los registros de invocación del modelo, esas actividades se registran en otro bucket de Amazon S3 para los registros de acceso del lado del servidor.

Automatización y escala

Para escalar esta solución, puede implementar la CloudFormation plantilla como una pila configurada en varios Regiones de AWS y Cuentas de AWS. Para obtener más información, consulte Administrar pilas en todas las cuentas y regiones StackSets en la CloudFormation documentación.

Tools (Herramientas)

Servicios de AWS

- Amazon Bedrock es un servicio totalmente gestionado que pone a su disposición modelos básicos de alto rendimiento (FMs) de las principales empresas de IA y Amazon a través de una API unificada.
- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en Cuentas de AWS todo el mundo. Regiones de AWS
- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas y aplicaciones Servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento líderes del sector.

Otras herramientas

- Git es un sistema de control de versiones distribuido y de código abierto.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub enable-bedrock-logging-using-cloudformation.

Epics

Crea la pila CloudFormation

Tarea	Descripción	Habilidades requeridas
Descarga la CloudFormation plantilla.	Descarga la CloudFormation plantilla del GitHub repositorio.	Arquitecto de la nube
Implemente la plantilla.	Cree una pila en su cuenta y región de destino. En la sección Parámetros, especifiq ue los valores para los parámetros que se definen en la plantilla. Para obtener instrucciones, consulte Crear una pila en la CloudFormation documentación.	Arquitecto de la nube

Pruebe la solución

Tarea	Descripción	Habilidades requeridas
Habilite el acceso a modelos.	En Amazon Bedrock, añada el acceso a los modelos básicos. Para obtener instrucciones, consulte Adición o eliminaci ón del acceso a los modelos básicos de Amazon Bedrock en la documentación de Amazon Bedrock.	Arquitecto de la nube
Ejecute una petición de muestra.	En el área de pruebas de Amazon Bedrock, ejecute una petición de ejemplo. Para obtener instrucciones, consulte Generación de	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	respuestas en la consola mediante áreas de pruebas la documentación de Amazon Bedrock.	
Revise la configuración de registro.	1. Inicie sesión en la consola de Amazon Bedrock. 2. En la barra de navegación, elige el Región de AWS lugar donde has desplegado la CloudFormation pila. 3. En el panel de navegación de la izquierda, en Configuraciones de Bedrock, elija Configuración. 4. Confirme lo siguiente: • El registro de invocación de modelos está habilitado. • Se seleccionan todos los tipos de datos. • Para los destinos de registro, selecciona tanto S3 como CloudWatch Logs.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Revise el bucket de Amazon S3:	1. En la sección Configuraciones de S3, elija Examinar S3. Esto abre el bucket de destino en la consola de Amazon S3. 2. Confirme que los datos de registro estén presentes en la petición de ejemplo que ejecutó anteriormente.	Arquitecto de la nube
Revise el grupo de registros.	1. Vuelva a la página Configuración en la consola de Amazon Bedrock. 2. En la sección de configuraciones de CloudWatch registros, revise la configuración del grupo de CloudWatch registros. Anote el nombre del grupo de registros. 3. Abra la consola de CloudWatch . 4. En el panel de navegación, en Registros, seleccione Grupos de registros. 5. Elija el nombre del grupo de registros en el que Amazon Bedrock publica los datos del registro. 6. Confirme que los datos de registro estén presentes en la petición de ejemplo que ejecutó anteriormente.	Arquitecto de la nube

Recursos relacionados

AWS documentación

- Acceso a un bucket de Amazon S3 (documentación de Amazon S3)
- Creación y administración de pilas (CloudFormation documentación)
- Invocación del modelo de monitor (documentación de Amazon Bedrock)
- Trabajar con grupos de registros y flujos de CloudWatch registros (documentación de registros)

AWS publicaciones de blog

- Supervisión de aplicaciones de IA generativa mediante la integración de Amazon Bedrock y Amazon CloudWatch
- Prácticas recomendadas para crear aplicaciones sólidas de IA generativa con agentes de Amazon Bedrock (Parte 1)
- Prácticas recomendadas para crear aplicaciones sólidas de IA generativa con agentes de Amazon Bedrock (Parte 2)

Cree una imagen de contenedor Docker personalizada SageMaker y úsela para el entrenamiento de modelos en AWS Step Functions

Julia Bluszcz, Aubrey Oosthuizen, Mohan Gowda Purushothama, Neha Sharma y Mateusz Zaremba, Amazon Web Services

Resumen

Este patrón muestra cómo crear una imagen de contenedor de Docker para Amazon SageMaker y utilizarla como modelo de formación en AWS Step Functions. Al empaquetar algoritmos personalizados en un contenedor, puede ejecutar prácticamente cualquier código del SageMaker entorno, independientemente del lenguaje de programación, el marco o las dependencias.

En la SageMaker libreta de ejemplo proporcionada, la imagen del contenedor Docker personalizado se almacena en Amazon Elastic Container Registry (Amazon ECR). A continuación, Step Functions utiliza el contenedor que está almacenado en Amazon ECR para ejecutar un script de procesamiento de Python. SageMaker A continuación, el contenedor exporta el modelo a Amazon Simple Storage Service (Amazon S3).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un rol de AWS Identity and Access Management (IAM) para SageMaker con permisos de Amazon S3
- Un rol de IAM para Step Functions
- Conocimientos básicos sobre Python
- Familiaridad con el SDK de Amazon SageMaker Python
- Información de la interfaz de la línea de comandos de AWS (AWS CLI)
- Información de AWS SDK para Python (Boto3)
- Amazon ECR
- Familiaridad con Docker

Versiones de producto

- SDK de ciencia de datos de AWS Step Functions versión 2.3.0
- Amazon SageMaker Python SDK versión 2.78.0

Arquitectura

En el siguiente diagrama, se muestra un ejemplo de flujo de trabajo para crear una imagen de contenedor de Docker y utilizarla después como modelo de entrenamiento en Step Functions: SageMaker

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un científico o DevOps ingeniero de datos utiliza un SageMaker bloc de notas de Amazon para crear una imagen de contenedor Docker personalizada.
2. Un científico o DevOps ingeniero de datos almacena la imagen del contenedor de Docker en un repositorio privado de Amazon ECR que se encuentra en un registro privado.
3. Un científico o DevOps ingeniero de datos utiliza el contenedor de Docker para ejecutar un trabajo de SageMaker procesamiento de Python en un flujo de trabajo de Step Functions.

Automatización y escala

El ejemplo de SageMaker cuaderno de este patrón utiliza un tipo de instancia de `ml.m5.xlarge` bloc de notas. Puede cambiar el tipo de instancia para que se ajuste a su caso de uso. Para obtener más información sobre los tipos de instancias de SageMaker notebook, consulta SageMaker los precios de Amazon.

Tools (Herramientas)

- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon SageMaker es un servicio de aprendizaje automático gestionado (ML) que le ayuda a crear y entrenar modelos de aprendizaje automático y, a continuación, a implementarlos en un entorno hospedado listo para la producción.
- Amazon SageMaker Python SDK es una biblioteca de código abierto para entrenar e implementar modelos de aprendizaje automático en. SageMaker

- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de AWS Lambda y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial.
- El SDK de Python de ciencia de datos de AWS Step Functions es una biblioteca de código abierto que lo ayuda a crear flujos de trabajo de Step Functions que procesan y publican modelos de machine learning.

Epics

Crear una imagen de contenedor de Docker personalizada y guardarla en Amazon ECR

Tarea	Descripción	Habilidades requeridas
Configure Amazon ECR y cree un nuevo registro privado.	Si aún no lo ha hecho, configure Amazon ECR siguiendo las instrucciones de Configuración con Amazon ECR de la Guía del usuario de Amazon ECR. Cada cuenta de AWS se proporciona con un registro privado de Amazon ECR predeterminado.	DevOps ingeniero
Crear un repositorio privado de Amazon ECR.	Siga las instrucciones de Creación de un repositorio privado de la Guía del usuario de Amazon ECR. **Note** El repositorio que cree es donde almacenar á sus imágenes de contenedores de Docker personali zadas.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Cree un Dockerfile que incluya las especificaciones necesarias para ejecutar su trabajo de SageMaker procesamiento.	Cree un Dockerfile que incluya las especificaciones necesarias para ejecutar su trabajo de SageMaker procesamiento configurando un Dockerfile. Para obtener instrucciones, consulta Cómo adaptar tu propio contenedor de formación en la Guía para SageMaker desarrolladores de Amazon.
	
	Para obtener más información acerca de los Dockerfiles, consulte Dockerfile Reference (Referencia de Dockerfile) en la documentación de Docker.
	
	Ejemplo de celdas de código de un cuaderno de Jupyter para crear un Dockerfile
	
	Celda 1
	
	`# Make docker folder`
	`!mkdir -p docker`
	
	Celda 2
	
	`%%writefile docker/Dockerfile`
	
	`FROM python:3.7-slim-buster`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	RUN pip3 install pandas==0.25.3 scikit- learn==0.21.3 ENV PYTHONUNBUFFERED=T RUE ENTRYPOINT ["python3"]	

Tarea	Descripción	Habilidades requeridas
Cree la imagen del contenedor de Docker y enviarla a Amazon ECR.	1. Cree la imagen del contenedor con el Dockerfile que creó al ejecutar el comando `docker build` en la AWS CLI. 2. Ejecute el comando `docker push` para enviar la imagen del contenedor a Amazon ECR. Para obtener más información, consulte Crear y registrar el contenedor en Cómo crear su propio contenedor de algoritmos GitHub. Ejemplo de celdas de código del cuaderno de Jupyter para crear y registrar una imagen de Docker **Important** Antes de ejecutar las siguientes celdas, asegúrese de haber creado un Dockerfile y de haberlo almacenado en el directorio denominado `docker`. Además, asegúrese de haber creado un repositorio de Amazon ECR y de sustituir el valor `ecr_repos`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	`itory` de la primera celda por el nombre del repositorio.
	
	Celda 1
	
	`import boto3`
	`tag = ':latest'`
	`account_id = boto3.client('sts').get_caller_identity().get('Account')`
	`region = boto3.Session().region_name`
	`ecr_repository = 'byoc'`
	
	`image_uri = '{}.dkr.ecr.{}.amazonaws.com/{}'.format(account_id, region, ecr_repository + tag)`
	
	Celda 2
	
	`# Build docker image`
	`!docker build -t $image_uri docker`
	
	Celda 3
	
	`# Authenticate to ECR`
	`!aws ecr get-login-password --region {region} | docker login --username AWS --password-stdin`	

Tarea	Descripción	Habilidades requeridas

	`{account_id}.dkr.ecr.{region}.amazonaws.com`
	
	Celda 4
	
	`# Push docker image`
	`!docker push $image_uri`
	
	Note
	Debe autenticar su cliente de Docker en su registro privado para poder utilizar los comandos `docker push` y `docker pull`. Estos comandos envían y extraen imágenes de los repositorios de su registro y las extraen de ellos.	

Cree un flujo de trabajo de Step Functions que utilice su imagen de contenedor de Docker personalizada

Tarea	Descripción	Habilidades requeridas
Cree un script de Python que incluya su procesamiento personalizado y su lógica de capacitación de modelos.	Escriba una lógica de procesamiento personalizada para ejecutarla en su script de procesamiento de datos. A continuación, guárdelo	Científico de datos

Tarea	Descripción	Habilidades requeridas

	como un script de Python denominado `training.py` .
	
	Para obtener más información, consulte Utilice su propio modelo con el modo SageMaker script activado GitHub.
	
	Ejemplo de script de Python que incluye procesamiento personalizado y lógica de capacitación de modelos
	
	`%%writefile training.py`
	`from numpy import empty`
	`import pandas as pd`
	`import os`
	`from sklearn import datasets, svm`
	`from joblib import dump, load`
	
	`if __name__ == '__main__':`
	`digits = datasets.load_digits()`
	`#create classifier object`
	`clf = svm.SVC(gamma=0.001, C=100.)`
	
	`#fit the model`
	`clf.fit(digits.data[:-1], digits.target[:-1])`	

Tarea	Descripción	Habilidades requeridas

	`#model output in binary format`
	`output_path = os.path.join('/opt/ml/processing/model', "model.joblib")`
	`dump(clf, output_path)`	

Tarea	Descripción	Habilidades requeridas

Cree un flujo de trabajo de Step Functions que incluya su trabajo de SageMaker procesamiento como uno de los pasos.	Instale e importe el SDK de ciencia de datos de AWS Step Functions y cargue el archivo training.py en Amazon S3. A continuación, utilice el SDK de Amazon SageMaker Python para definir un paso de procesamiento en Step Functions.
	
	Important
	Asegúrese de haber creado un rol de ejecución de IAM para Step Functions en su cuenta de AWS.
	
	Ejemplo de configuración del entorno y script de capacitación personalizado para cargarlo en Amazon S3
	
	`!pip install stepfunctions`
	
	`import boto3`
	`import stepfunctions`
	`import sagemaker`
	`import datetime`
	
	`from stepfunctions import steps`
	`from stepfunctions.inputs import ExecutionInput`
		Científico de datos

Tarea	Descripción	Habilidades requeridas

	from stepfunct
	ions.steps import (
	    Chain
	)
	from stepfunct
	ions.workflow import
	 Workflow
	from sagemaker
	.processing import
	 ScriptProcessor,
	 ProcessingInput,
	 ProcessingOutput
	
	sagemaker_session =
	 sagemaker.Session()
	bucket = sagemaker
	_session.default_b
	ucket()
	role = sagemaker
	.get_execution_role()
	prefix = 'byoc-tra
	ining-model'
	
	# See prerequisites
	 section to create this
	 role
	workflow_execution_rol
	e = f"arn:aws:iam::
	{account_id}:role/Ama
	zonSageMaker-StepF
	unctionsWorkflowEx
	ecutionRole"
	
	execution_input =
	 ExecutionInput(
	    schema={
	        "Preproce
	ssingJobName": str})
	
	input_code = sagemaker
	_session.upload_data(	

Tarea	Descripción	Habilidades requeridas
	`"training.py", bucket=bucket, key_prefix="preprocessing.py", )` Ejemplo SageMaker de definición de paso de procesamiento que utiliza una imagen personalizada de Amazon ECR y un script de Python **Note** Asegúrese de utilizar el parámetro `execution_input` para especificar el nombre del trabajo. El valor del parámetro debe ser único cada vez que se ejecute el trabajo. Además, el código del archivo training.py se pasa como parámetro `input` a `ProcessingStep` , lo que significa que se copiará dentro del contenedor. El destino del código `ProcessingInput` es el mismo que el del segundo	

Tarea	Descripción	Habilidades requeridas

	argumento incluido en `container_entrypoint` .
	
	`script_processor = ScriptProcessor(command=['python3'], image_uri=image_uri, role=role, instance_count=1, instance_type='ml.m5.xlarge')`
	
	`processing_step = steps.ProcessingStep( "training-step", processor=script_processor, job_name=execution_input["PreprocessingJobName"], inputs=[ ProcessingInput( source=input_code, destination="/opt/ml/processing/input/code", input_name="code", ), ], outputs=[`	

Tarea	Descripción	Habilidades requeridas

	<pre>Processin
	gOutput(
	source='/
	opt/ml/processing/
	model',
	destinati
	on="s3://{}/{}".fo
	rmat(bucket, prefix),
	output_na
	me='byoc-example')
	],
	container_entrypoi
	nt=["python3", "/opt/
	ml/processing/input/c
	ode/training.py"],
	)</pre>	

	Ejemplo de flujo de trabajo de Step Functions que ejecuta un trabajo SageMaker de procesamiento **Note** Este flujo de trabajo de ejemplo incluye solo el paso del trabajo de SageMaker procesamiento, no un flujo de trabajo completo de Step Functions. Para ver un ejemplo completo de flujo de trabajo, consulte Cuadernos de ejemplo SageMaker en la documentación del	

Tarea	Descripción	Habilidades requeridas

	SDK de ciencia de datos de AWS Step Functions.
	
	`workflow_graph = Chain([processing_step])`
	
	`workflow = Workflow(`
	`  name="ProcessingWorkflow",`
	`  definition=workflow_graph,`
	`  role=workflow_execution_role`
	`)`
	
	`workflow.create()`
	`# Execute workflow`
	`execution = workflow.execute(`
	`  inputs={`
	`  "PreprocessingJobName": str(datetime.datetime.now().strftime("%Y%m%d%H%M-%SS")),`
	`  # Each pre processing job (SageMaker processing job) requires a unique name,`
	`  }`
	`)`
	`execution_output = execution.get_output(wait=True)`	

Recursos relacionados

- Procesar datos (Amazon SageMaker Developer Guide)
- Adaptación de tu propio contenedor de formación (Amazon SageMaker Developer Guide)

Uso de agentes de Amazon Bedrock para automatizar la creación de controles de entrada de acceso en Amazon EKS mediante peticiones basadas en texto

Keshav Ganesh y Sudhanshu Saurav, Amazon Web Services

Resumen

Las organizaciones se enfrentan a desafíos al administrar los controles de acceso y el aprovisionamiento de recursos cuando varios equipos necesitan trabajar con un clúster compartido de Amazon Elastic Kubernetes Service (Amazon EKS). Un servicio de Kubernetes administrado, como Amazon EKS, ha simplificado las operaciones de los clústeres. Sin embargo, la sobrecarga administrativa que supone administrar el acceso de los equipos y los permisos de los recursos sigue siendo compleja y es tardada.

Este patrón muestra cómo los agentes de Amazon Bedrock pueden serle útiles para automatizar la administración del acceso a los clústeres de Amazon EKS. Esta automatización permite a los equipos de desarrollo centrarse en el desarrollo de sus aplicaciones principales en lugar de centrarse en la configuración y la administración del control de acceso. Puede personalizar un agente de Amazon Bedrock para que realice acciones para una amplia variedad de tareas mediante instrucciones sencillas en lenguaje natural.

Al utilizar AWS Lambda funciones como grupos de acción, un agente de Amazon Bedrock puede gestionar tareas como la creación de entradas de acceso de usuarios y la gestión de las políticas de acceso. Además, un agente de Amazon Bedrock puede configurar asociaciones de identidad de pods que permiten el acceso a los recursos AWS Identity and Access Management (IAM) para los pods que se ejecutan en el clúster. Con esta solución, las organizaciones pueden optimizar la administración de sus clústeres de Amazon EKS con instrucciones sencillas basadas en texto, reducir la sobrecarga manual y mejorar la eficiencia general del desarrollo.

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- Se establecieron los roles y los permisos de IAM para el proceso de implementación. Esto incluye permisos para acceder a los modelos básicos (FM) de Amazon Bedrock, crear funciones Lambda y cualquier otro recurso necesario en todo el destino. Cuentas de AWS

- El acceso está habilitado en activo Cuenta de AWS a estos haiku Amazon Bedrock FMs: Amazon Titan Text Embeddings V2 y Anthropic Claude 3.
- AWS Command Line Interface (AWS CLI) versión 2.9.11 o posterior, instalada y configurada.
- eksctl 0.194.0 o posterior, instalado.

Limitaciones

- Es posible que se necesiten entrenamiento y documentación para garantizar una adopción fluida y un uso efectivo de estas técnicas. El uso de Amazon Bedrock, Amazon EKS, Lambda, OpenSearch Amazon Service y OpenAPI implica una curva de aprendizaje importante para los desarrolladores y los equipos. DevOps
- Algunas Servicios de AWS no están disponibles en todos. Regiones de AWS Para obtener información sobre la disponibilidad en regiones, consulte AWS services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

En el siguiente diagrama se muestran los componentes de la arquitectura y el flujo de trabajo de esta aplicación.

Esta solución realiza los pasos que se indican a continuación:

1. El usuario interactúa con el agente de Amazon Bedrock, ya que envía una petición o consulta que sirve de entrada para que el agente la procese y tome medidas.
2. Según la petición, el agente de Amazon Bedrock comprueba el esquema de OpenAPI para identificar la API correcta a la que dirigirse. Si el agente de Amazon Bedrock encuentra la llamada a la API correcta, la solicitud se dirige al grupo de acciones asociado a la función de Lambda que implementa estas acciones.
3. Si no encuentra una API relevante, el agente de Amazon Bedrock consulta la OpenSearch colección. La OpenSearch colección utiliza contenido indexado de la base de conocimientos que proviene del depósito de Amazon S3 que contiene la Guía del usuario de Amazon EKS.
4. La OpenSearch colección devuelve la información contextual relevante al agente de Amazon Bedrock.

5. En el caso de las solicitudes prácticas (aquellas que coinciden con una operación de API), el agente de Amazon Bedrock se ejecuta en una nube privada virtual (VPC) y activa la función de Lambda.
6. La función de Lambda realiza una acción que se basa en la entrada del usuario dentro del clúster de Amazon EKS.
7. El bucket de Amazon S3 para el código de Lambda almacena el artefacto que contiene el código y la lógica escritos para la función de Lambda.

Tools (Herramientas)

Servicios de AWS

- Amazon Bedrock es un servicio totalmente gestionado que pone a su disposición modelos básicos de alto rendimiento (FMs) de las principales empresas emergentes de IA y Amazon a través de una API unificada.
- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todo el territorio y. Cuentas de AWS Regiones de AWS
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar AWS Kubernetes sin necesidad de instalar o mantener su propio plano de control o nodos de Kubernetes.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon OpenSearch Service es un servicio gestionado que le ayuda a implementar, operar y escalar OpenSearch clústeres en Nube de AWS. Su característica de colecciones le permite organizar los datos y crear bases de conocimiento integrales que los asistentes de IA, como los agentes de Amazon Bedrock, pueden utilizar.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

- eksctl: es una utilidad sencilla de línea de comandos para crear y administrar clústeres de Kubernetes en Amazon EKS.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub eks-access-controls-bedrock-agent.

Prácticas recomendadas

- Mantenga la mayor seguridad posible al implementar este patrón. Asegúrese de que el clúster de Amazon EKS sea privado, tenga permisos de acceso limitados y que todos los recursos estén dentro de una nube privada virtual (VPC). Para más información, consulte Best practices for security en la documentación de Amazon EKS.
- Utilice claves administradas por el AWS KMS cliente siempre que sea posible y concédales permisos de acceso limitados.
- Cumpla con el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Configuración del entorno

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Para clonar el repositorio de este patrón, ejecute el comando siguiente en la estación de trabajo local: `git clone https://github.com/aws-samples/eks-access-controls-bedrock-agent.git`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Obtenga la Cuenta de AWS identificación.	Para obtener la Cuenta de AWS identificación, sigue los siguientes pasos: 1. Abra un intérprete de comandos en la carpeta raíz del repositorio clonado, `eks-access-controls-bedrock-agent` . 2. Para obtener su Cuenta de AWS ID, vaya al directorio clonado y ejecute el siguiente comando: `AWS_ACCOUNT=$(aws sts get-caller-identity --query "Account" --output text)` Este comando almacena tu Cuenta de AWS ID en la `AWS_ACCOUNT` variable.	AWS DevOps

Tarea	Descripción	Habilidades requeridas

Cree el bucket de S3 para el código de Lambda.	Para implementar esta solución, debe crear tres buckets de Amazon S3 que sirvan para propósitos distintos, como se muestra en el diagrama de arquitectura. Los buckets de S3 son para código de Lambda, una base de conocimientos y un esquema OpenAPI.
	
	Para crear el bucket de Lambda, haga esto:
	
	1. Para crear un bucket de S3 para código de Lambda, ejecute el comando siguiente:
	
	`aws s3 mb s3://bedrock-agent-lambda-artifacts-${AWS_ACCOUNT} --region us-east-1`
	
	2. Para instalar la dependencia del código de Lambda, ejecute el comando siguiente:
	
	`cd eks-lambda`
	`npm install`
	`tsc`
	`cd .. && cd opensearch-lambda`
	`npm install`
	`tsc`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`cd ..`
	3. Para empaquetar el código y cargarlo al bucket de S3 para Lambda, ejecute el comando siguiente:
	`aws cloudformation package \ --template-file eks-access-controls.yaml \ --s3-bucket bedrock-agent-lambda-artifacts-${AWS_ACCOUNT} \ --output-template-file eks-access-controls-template.yaml \ --region us-east-1`
	El comando package crea una nueva CloudFormation plantilla (`eks-access-controls-template.yaml`) que contiene:
	• Referencias al código de la función de Lambda almacenado en el bucket de S3.
	• Definiciones de toda la AWS infraestructura requerida, incluida la VPC, las subredes, el agente de Amazon Bedrock y la recopilación. OpenSearc	

Tarea	Descripción	Habilidades requeridas
	h Puede utilizar esta plantilla para implementar la solución completa mediante. CloudFormation	

Tarea	Descripción	Habilidades requeridas

Cree el bucket de S3 para la base de conocimientos.	Para crear el bucket de Amazon S3 para la base de conocimientos, haga lo siguiente:
	
	1. Para crear el bucket de Amazon S3 para la base de conocimientos, ejecute el comando siguiente:
	
	`aws s3 mb s3://eks-knowledge-base-${AWS_ACCOUNT} --region us-east-1`
	
	2. Para descargar la Guía del usuario de Amazon EKS y almacénela en un directorio, ejecute los comandos siguientes:
	
	`mkdir dataSource`
	`cd dataSource`
	`curl https://docs.aws.amazon.com/pdfs/eks/latest/userguide/eks-ug.pdf -o eks-user-guide.pdf`
	
	3. Para cargar la guía del usuario en el bucket de S3 que creó en el paso 1, ejecute el comando siguiente:
	
	`aws s3 cp eks-user-guide.pdf s3://eks-`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	knowledge-base-${AWS_ACCOUNT} \ --region us-east-1 \ 4. Para volver al directorio raíz, ejecute el siguiente comando: cd ..	
Cree el bucket de S3 para el esquema de OpenAPI.	Para crear el bucket de Amazon S3 para el esquema de OpenAPI, haga lo siguiente: 1. Para crear el bucket de S3, ejecute el comando siguiente: aws s3 mb s3://eks-openapi-schema-${AWS_ACCOUNT} --region us-east-1 2. Para cargar el esquema de OpenAPI en el bucket de S3, ejecute el comando siguiente: aws s3 cp openapi-schema.yaml s3://eks-openapi-schema-${AWS_ACCOUNT} --region us-east-1	AWS DevOps

Implemente la CloudFormation pila

Tarea	Descripción	Habilidades requeridas
Despliegue la CloudFormation pila.	Para implementar la CloudFormation pila, usa el archivo CloudFormation de plantilla `eks-access-controls-template.yaml` que creaste anteriormente. Para obtener instrucciones más detalladas, consulte Crear una pila desde la CloudFormation consola en la CloudFormation documentación. **Note** El aprovisionamiento del OpenSearch índice con la CloudFormation plantilla tarda unos 10 minutos. Una vez creada la pila, anote el valor de `VPC_ID` y `PRIVATE_SUBNET ID` .	AWS DevOps
Cree el clúster de Amazon EKS.	Para crear el clúster de Amazon EKS dentro de la VPC, haga lo siguiente: 1. Cree una copia del archivo de configuración `eks-config.yaml` y asígnele	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	el nombre `eks-deploy.yaml` a la copia.
	2. Abra `eks-deploy.yaml` en un editor de texto. A continuación, sustituya los valores de marcador de posición siguientes por valores de la pila implementada: `VPC_ID`, `PRIVATE_SUBNET1` y `PRIVATE_SUBNET2`
	3. Para crear el clúster mediante la utilidad eksctl, ejecute el comando siguiente:
	`eksctl create cluster -f eks-deploy.yaml`
	Note
	Este proceso de creación del clúster puede tardar entre 15 y 20 minutos en completarse.
	4. Para comprobar que se creó el clúster correctamente, ejecute los comandos siguientes:
	`aws eks describe-cluster --name`	

Tarea	Descripción	Habilidades requeridas

	`--query "cluster.status"`
	`aws eks update-kubeconfig --name --region`
	`kubectl get nodes`
	
	Los resultados esperados son los siguientes:
	• El estado del clúster es `ACTIVE`.
	• El comando `kubectl get nodes` muestra que todos los nodos se encuentran en el estado `Ready`.	

Conexión de la función de Lambda y el clúster de Amazon EKS

Tarea	Descripción	Habilidades requeridas
Cree una conexión entre el clúster de Amazon EKS y la función de Lambda.	Para configurar los permisos de red e IAM para permitir que la función de Lambda se comunique con el clúster de Amazon EKS, haga lo siguiente: 1. Para identificar la función de IAM asociada a la función Lambda, abra y localice Consola de administración de AWS la función Lambda denominada. `bedrock-agent-`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`eks-access-control` Anote el nombre de recurso de Amazon (ARN) del rol de IAM.
	2. Para crear una entrada de acceso en el clúster de Amazon EKS para el rol de IAM de la función de Lambda, ejecute el comando siguiente:
	`aws eks create-access-entry --cluster-name eks-testing-cluster --principal-arn <principal-Role-ARN>`
	3. Para asignar los permisos de `AmazonEKSClusterAdminPolicy` a este rol, ejecute el comando siguiente:
	`aws eks associate-access-policy --cluster-name eks-testing-cluster --principal-arn <principal-Role-ARN> --policy-arn arn:aws:eks::aws:cluster-access-policy/AmazonEKSClusterAdminPolicy --access-scope type=cluster`	

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte Asociar políticas de acceso a entradas de acceso y Amazon EKSCluster AdminPolicy en la documentación de Amazon EKS. 4. Encuentre el grupo de seguridad del clúster de Amazon EKS. Agregue una regla de entrada para permitir el tráfico de red entrante de la función de Lambda al clúster de Amazon EKS. Utilice los valores siguientes para la regla de entrada: • Tipo: HTTPS • Intervalo de puertos: 443 • Origen: grupo de seguridad de Lambda Para más información, consulte Configuración de reglas de grupo de seguridad en la documentación de Amazon VPC.	

Pruebe la solución

Tarea	Descripción	Habilidades requeridas
Pruebe el agente de Amazon Bedrock.	Antes de hacer pruebas con el agente de Amazon Bedrock, asegúrese de hacer lo siguiente: • Pruebe primero con roles que no sean de producción. • Documente los cambios hechos en el acceso al clúster. • Tenga un plan para revertir los cambios si es necesario. Para acceder al agente de Amazon Bedrock, haga lo siguiente: 1. Inicie sesión en el rol de Consola de administración de AWS uso de IAM con los permisos de Amazon Bedrock y abra la consola de Amazon Bedrock en. https://console.aws.amazon.com/bedrock/ 2. En el panel de navegación de la izquierda, seleccione Agentes. A continuación, elija el agente configurado en la sección Agentes. 3. Para probar el agente, intente los ejemplos de	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	instrucciones siguiente s, en los que lo sustituirá `Principal-ARN-OF-R OLE` por un ARN de rol de IAM real: • Para crear una entrada de acceso para cualquier rol de IAM al que quiere proporcionar acceso al clúster de EKS, utilice la petición siguiente: `Create an access entry in cluster eks-testi ng-new for a role whose principal arn is <Principal-ARN-OF-ROLE> with access policy as AmazonEKS AdminPolicy` Resultado esperado: • El agente debe confirmar la creación de la entrada de acceso. • Para verificarlo, Consola de administración de AWS compruébelo o utilice la API Amazon EKS y ejecute el siguiente comando: `aws eks list-access-entrie s --cluster-name ekscluster`	

Tarea	Descripción	Habilidades requeridas
	• Para describir la entrada de acceso que creó, utilice la petición siguiente: `Describe an access entry in cluster eks-testing-new whose principal arn is <Principal-ARN-OF-ROLE>` Resultado esperado: • El agente debe devolver los detalles acerca de la entrada de acceso. • Los detalles deben coincidir con los que configuró anteriorm ente para la entrada de acceso. • Para eliminar la entrada de acceso que creó, utilice la petición siguiente: `Delete the access entry in cluster eks-testing-new whose principal arn is <Principal-ARN-OF-ROLE>` Resultado esperado: • El agente debe confirmar la eliminación de la entrada de acceso. • Para verificarlo, Consola de administración de	

Tarea	Descripción	Habilidades requeridas
	AWS compruébelo o utilice la API Amazon EKS y ejecute el siguiente comando: `aws eks list-access-entries --cluster-name ekscluster` También puede pedirle al agente que realice acciones para las asociaciones de Pod Identity de EKS. Para más información, consulte Más información sobre cómo Pod Identity de EKS concede a los pods acceso a los Servicios de AWS en la documentación de Amazon EKS.	

Limpieza

Tarea	Descripción	Habilidades requeridas
Eliminación de recursos.	Para limpiar los recursos que creó este patrón, siga el procedimiento siguiente. Espere a que cada paso de eliminación termine antes de ir al paso siguiente. ⚠ Warning Este procedimiento eliminará de manera	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	permanente todos los recursos creados por estas pilas. Asegúrese de que hizo una copia de seguridad de los datos importantes antes de continuar.
	
	1. Para eliminar el clúster de Amazon EKS, ejecute el comando siguiente:
	
	`eksctl delete cluster -f eks-deploy.yaml`
	
	Note
	Esta operación puede tardar entre 15 y 20 minutos en completarse.
	
	2. Para eliminar los buckets de Amazon S3, ejecute los comandos siguientes:
	• Para vaciar el bucket de Lambda:
	
	`aws s3 rm s3://bedrock-agent-lambda-artifacts-${AWS_ACCOUNT} --recursive`	

Tarea	Descripción	Habilidades requeridas

	• Para vaciar el bucket de la base de conocimientos:
	`aws s3 rm s3://eks-knowledge-base-${AWS_ACCOUNT} –recursive`
	• Para vaciar el bucket de esquemas de OpenAPI:
	`aws s3 rm s3://bedrock-agent-openapi-schema-${AWS_ACCOUNT} –recursive`
	• Para eliminar los buckets vacíos:
	`aws s3 rb s3://bedrock-agent-lambda-artifacts-${AWS_ACCOUNT}`
	`aws s3 rb s3://eks-knowledge-base-${AWS_ACCOUNT}`
	`aws s3 rb s3://bedrock-agent-openapi-schema-${AWS_ACCOUNT}`
	3. Para eliminar la CloudFormation pila, ejecute el siguiente comando:
	`aws cloudformation delete-stack \ --stack-name`	

Tarea	Descripción	Habilidades requeridas

	4. Para verificar la eliminación del clúster de Amazon EKS, ejecute el comando siguiente:
	`eksctl get clusters`
	5. Para verificar la eliminación los buckets de Amazon S3, ejecute los comandos siguientes:
	• Para verificar la eliminación del bucket de Lambda:
	`aws s3 ls | grep "bedrock-agent-lambda-artifacts"`
	• Para verificar la eliminación del bucket de la base de conocimientos:
	`aws s3 ls | grep "eks-knowledge-base"`
	• Para verificar la eliminación del bucket de esquemas de OpenAPI:
	`aws s3 ls | grep "bedrock-agent-openapi-schema"`
	6. Para verificar la eliminación de la pila, ejecute el comando siguiente:	

Tarea	Descripción	Habilidades requeridas
	`aws cloudformation list-stacks \--query 'StackSummaries[?StackName==``]'` Si la pila no se elimina, consulte Troubleshooting.	

Resolución de problemas

Problema	Solución
Durante la configuración del entorno, se devuelve un código de error distinto de cero.	Compruebe que está utilizando la carpeta correcta al ejecutar los comandos para implementar esta solución. Para más información, consulte el archivo FIRST_DEPLOY.md del repositorio de este patrón.
La función de Lambda no puede hacer la tarea.	Asegúrese de que la conectividad esté configurada correctamente desde la función de Lambda al clúster de Amazon EKS.
Las indicaciones del agente no reconocen el APIs.	Implementar la solución. Para más información, consulte el archivo RE_DEPLOY.md del repositorio de este patrón.
La pila no se puede eliminar.	Es posible que se produzca un error al intentar eliminar la pila por primera vez. Este error puede producirse debido a problemas de dependencia con el recurso personalizado que se creó para la OpenSearch colección, que se encarga de la indexación de la base de conocimientos. Para eliminar la pila, vuelva a

Problema	Solución
	intentar la operación de eliminación conservando el recurso personalizado.

Recursos relacionados

AWS Blog

- A deep dive into simplified Amazon EKS access management controls

Documentación de Amazon Bedrock

- Automate tasks in your application using AI agents
- Cómo funciona Amazon Bedrock Agents
- Pruebe y solucione los problemas del comportamiento de los agentes
- Utilice grupos de acciones para definir las acciones que debe realizar su agente

Documentación de Amazon EKS

- Descubra cómo funciona el control de acceso en Amazon EKS

Implemente un caso de uso de RAG AWS mediante Terraform y Amazon Bedrock

Martin Maritsch, Nicolas Jacob Baer, Olivier Brique, Julian Ferdinand Grueber, Alice Morano y Nicola D Orazio, Amazon Web Services

Resumen

AWS ofrece varias opciones para crear sus casos de uso de IA generativa habilitados para la generación aumentada de recuperación (RAG). Este patrón le proporciona una solución para una aplicación basada en RAG basada en LangChain y compatible con Amazon Aurora PostgreSQL como almacén vectorial. Puede implementar directamente esta solución con Terraform en su RAG Cuenta de AWS e implementar el siguiente caso de uso sencillo:

1. El usuario carga un archivo de forma manual en un bucket de Amazon Simple Storage Service (Amazon S3), como un archivo de Microsoft Excel o un documento PDF. (Para obtener más información sobre los tipos de archivos compatibles, consulte la documentación de Unstructured [Sin estructurar]).
2. El contenido del archivo se extrae y se incrusta en una base de datos de conocimiento basada en Aurora sin servidor compatible con PostgreSQL, que permite la ingesta de documentos casi en tiempo real en el almacén vectorial. Este enfoque permite al modelo de RAG acceder a la información relevante y recuperarla para casos de uso en los que las bajas latencias son importantes.
3. Cuando el usuario utiliza el modelo de generación de texto, mejora la interacción al recuperar y aumentar el contenido relevante de los archivos cargados anteriormente.

El patrón utiliza Amazon Titan Text Embeddings v2 como modelo de incrustación y Anthropic Claude 3 Sonnet como modelo de generación de texto, ambos disponibles en Amazon Bedrock.

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- AWS Command Line Interface (AWS CLI) instalado y configurado con su Cuenta de AWS. Para obtener instrucciones de instalación, consulte Instalar o actualizar a la última versión de AWS

CLI en la AWS CLI documentación. Para revisar sus AWS credenciales y el acceso a su cuenta, consulte los ajustes de configuración y del archivo de credenciales en la AWS CLI documentación.

- Acceso al modelo que está habilitado para los modelos de idiomas grandes requeridos (LLMs) en la consola Amazon Bedrock de su Cuenta de AWS. Este patrón requiere lo siguiente: LLMs
  - `amazon.titan-embed-text-v2:0`
  - `anthropic.claude-3-sonnet-20240229-v1:0`

Limitaciones

- Esta arquitectura de ejemplo no incluye una interfaz para responder preguntas mediante programación con la base de datos vectorial. Si su caso de uso requiere una API, considere añadir Amazon API Gateway con una AWS Lambda función que ejecute tareas de recuperación y respuesta a preguntas.
- Este ejemplo de arquitectura no incluye características de supervisión para la infraestructura implementada. Si su caso de uso requiere supervisión, considere la posibilidad de añadir servicios de supervisión de AWS.
- Si carga muchos documentos en poco tiempo al bucket de Amazon S3, es posible que la función de Lambda encuentre límites de tasas. Como solución, puede desacoplar la función de Lambda de una cola de Amazon Simple Queue Service (Amazon SQS) donde pueda controlar la frecuencia de las invocaciones de Lambda.
- Algunas Servicios de AWS no están disponibles en todos. Regiones de AWS Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- AWS CLI versión 2 o posterior
- La versión 26.0.0 o posterior de Docker
- Poetry versión 1.7.1 o posterior
- Python versión 3.10 o posterior
- La versión 1.8.4 o posterior de Terraform

Arquitectura

En el siguiente diagrama se muestran los componentes de la arquitectura y el flujo de trabajo de esta aplicación.

Este diagrama ilustra lo siguiente:

1. Cuando se crea un objeto en el bucket `bedrock-rag-template-<account_id>` de Amazon S3, una notificación de Amazon S3 invoca la función de Lambda `data-ingestion-processor`.
2. La función de Lambda `data-ingestion-processor` se basa en una imagen de Docker almacenada en el repositorio Amazon Elastic Container Registry (Amazon ECR) `bedrock-rag-template`.

   La función usa el LangChain S3 FileLoader para leer el archivo como un documento. LangChain Luego, divide LangChain RecursiveCharacterTextSplittercada documento, con una `CHUNK_SIZE` y una `CHUNK_OVERLAP` que dependen del tamaño máximo del token del modelo de incrustación Amazon Titan Text Embedding V2. A continuación, la función de Lambda invoca el modelo de incrustación de Amazon Bedrock para incrustar los fragmentos en representaciones vectoriales numéricas. Por último, estos vectores se almacenan en la base de datos de Aurora PostgreSQL. Para acceder a la base de datos, la función Lambda recupera primero el nombre de usuario y la contraseña de. AWS Secrets Manager
3. En la instancia de Amazon SageMaker AI notebook`aws-sample-bedrock-rag-template`, el usuario puede escribir un mensaje de pregunta. El código invoca Claude 3 en Amazon Bedrock y añade la información de la base de conocimientos al contexto de la petición. Como resultado, Claude 3 proporciona respuestas utilizando la información de los documentos.

El enfoque de este patrón con respecto a las redes y la seguridad es el siguiente:

- La función de Lambda `data-ingestion-processor` se encuentra en una subred privada dentro de la nube privada virtual (VPC). La función de Lambda no puede enviar tráfico a la Internet pública debido a su grupo de seguridad. Como resultado, el tráfico a Amazon S3 y Amazon Bedrock se enruta únicamente a través de los puntos de conexión de VPC. Por lo tanto, el tráfico no atraviesa la red pública de Internet, lo que reduce la latencia y añade una capa adicional de seguridad a nivel de red.
- Todos los recursos y datos se cifran siempre que sea posible mediante la clave AWS Key Management Service (AWS KMS) con el alias`aws-sample/bedrock-rag-template`.

Automatización y escala

Este patrón utiliza Terraform para implementar la infraestructura del repositorio de código en una Cuenta de AWS.

Tools (Herramientas)

Servicios de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL. En este patrón, Aurora compatible con PostgreSQL utiliza el complemento pgvector como base de datos vectorial.
- Amazon Bedrock es un servicio totalmente gestionado que pone a su disposición modelos básicos de alto rendimiento (FMs) de las principales empresas emergentes de IA y Amazon a través de una API unificada.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar Servicios de AWS mediante comandos en su consola de línea de comandos.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable. En este patrón, Amazon ECR aloja la imagen de Docker para la función de Lambda `data-ingestion-processor`.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Key Management Service (AWS KMS) lo ayuda a crear y controlar claves criptográficas que ayudan a proteger los datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice. En este patrón, Lambda ingiere datos en el almacén vectorial.
- Amazon SageMaker AI es un servicio de aprendizaje automático (ML) gestionado que le ayuda a crear y entrenar modelos de aprendizaje automático para luego implementarlos en un entorno hospedado listo para la producción.
- AWS Secrets Manager lo ayuda a reemplazar las credenciales codificadas en su código, incluidas contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS. La VPC incluye subredes y tablas de enrutamiento para controlar el flujo de tráfico.

Otras herramientas

- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización a nivel del sistema operativo para entregar software en contenedores.
- HashiCorp Terraform es una herramienta de infraestructura como código (IaC) que facilita usar el código para aprovisionar y administrar los recursos y la infraestructura en la nube.
- Poetry es una herramienta de empaquetado y administración de dependencias de Python.
- Python es un lenguaje de programación informático de uso general.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub terraform-rag-template-using-amazon-bedrock.

Prácticas recomendadas

- Aunque este ejemplo de código se puede implementar en cualquier Región de AWS lugar, le recomendamos que utilice US East (North Virginia) `us-east-1` o US West (North California). `us-west-1` Esta recomendación se basa en la disponibilidad de modelos de incrustación y fundacionales en Amazon Bedrock en el momento de la publicación de este patrón. Para obtener una up-to-date lista del soporte del modelo base de Amazon Bedrock Regiones de AWS, consulte Soporte de modelos Región de AWS en la documentación de Amazon Bedrock. Para obtener información sobre cómo implementar este ejemplo de código en otras regiones, consulte la información adicional.
- Este patrón solo proporciona una proof-of-concept demostración (PoC) o piloto. Si desea llevar el código a producción, asegúrese de seguir las siguientes prácticas recomendadas:
  - Habilite el registro de acceso al servidor de Amazon S3.
  - Configure la supervisión y las alertas para la función de Lambda.

  - Si su caso de uso requiere una API, considere añadir Amazon API Gateway con una función de Lambda que ejecute tareas de recuperación y respuesta a preguntas.
- Siga el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Implemente la solución en un Cuenta de AWS

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Para clonar el GitHub repositorio proporcionado con este patrón, utilice el siguiente comando: `git clone https://github.com/aws-samples/terraform-rag-template-using-amazon-bedrock`	AWS DevOps
Configure las variables.	Para configurar los parámetros de este patrón, haga lo siguiente: 1. En su ordenador, en el GitHub repositorio, utilice el siguiente comando para abrir la `terraform` carpeta: `cd terraform` 2. Abra el archivo `commons.tfvars` y personalice los	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	parámetros según sus necesidades.	

Implemente la solución.	Para implementar la solución, haga lo siguiente:
	1. En la carpeta `terraform`, use el siguiente comando para ejecutar Terraform y pasar las variables que ha personalizado:
	`terraform init`
	`terraform apply -var-file=commons.tfvars`
	2. Confirme que los recursos que se muestran en el diagrama de arquitectura se implementaron correctamente.
	
	La implementación de la infraestructura aprovisiona una instancia de SageMaker IA dentro de la VPC y con los permisos para acceder a la base de datos PostgreSQL de Aurora.
		AWS DevOps

Pruebe la solución

Tarea	Descripción	Habilidades requeridas
Ejecute la demostración.	Una vez que la implement ación anterior de la infraestr uctura se haya realizado correctamente, siga estos pasos para ejecutar la demostración en cuaderno de Jupyter: 1. Inicie sesión en el Consola de administración de AWS lugar Cuenta de AWS donde está implementada la infraestructura. 2. Abre la instancia de SageMaker AI Notebook`aws-sample-bedrock-rag-template` . 3. Mueva el cuaderno `rag_demo.ipynb` Jupyter a la instancia del cuaderno SageMaker AI arrastrando y soltando. 4. Abre `rag_demo.ipynb` la instancia del cuaderno SageMaker AI y elige el `conda_python3` núcleo. 5. Para ejecutar la demostrac ión, ejecute las celdas del cuaderno.	AWS general

Tarea	Descripción	Habilidades requeridas
	El cuaderno de Jupyter le guía a través del siguiente proceso: • Requisitos de instalación • Definición de incrustación • Conexión a la base de datos • Ingesta de datos • Generación aumentada por recuperación • Consultas de documentos relevantes	

Limpieza de la infraestructura

Tarea	Descripción	Habilidades requeridas
Limpie la infraestructura.	Para eliminar todos los recursos que creó cuando ya no sean necesarios, utilice el siguiente comando: `terraform destroy -var-file=commons.tfvars`	AWS DevOps

Recursos relacionados

AWS resources

- Creación de funciones de Lambda con Python
- Parámetros de inferencia para modelos básicos
- Acceso a los modelos fundacionales de Amazon Bedrock
- El papel de las bases de datos vectoriales en las aplicaciones de IA generativa (blog de bases AWS de datos)

- Uso de Amazon Aurora PostgreSQL

Otros recursos

- Documentación de pgvector

Información adicional

Implementación de una base de datos vectorial

Este patrón utiliza Aurora compatible con PostgreSQL para implementar una base de datos vectorial para RAG. Como alternativa a Aurora PostgreSQL AWS , ofrece otras capacidades y servicios para RAG, como Amazon Bedrock Knowledge Bases y Amazon Service. OpenSearch Puede elegir la solución que mejor se adapte a sus requisitos específicos:

- Amazon OpenSearch Service proporciona motores de búsqueda y análisis distribuidos que puede utilizar para almacenar y consultar grandes volúmenes de datos.
- Las bases de conocimiento de Amazon Bedrock están diseñadas para crear e implementar bases de conocimiento como una abstracción adicional para simplificar el proceso de ingesta y recuperación de RAG. Las bases de conocimiento de Amazon Bedrock funcionan tanto con Aurora PostgreSQL como con Amazon Service. OpenSearch

¿Implementar en otros Regiones de AWS

Como se describe en Arquitectura, le recomendamos que utilice la región Este de EE. UU. (Norte de Virginia):`us-east-1` u Oeste de EE. UU. (Norte de California):`us-west-1` para implementar este ejemplo de código. Sin embargo, hay dos formas posibles de implementar este ejemplo de código en regiones distintas de `us-east-1` y `us-west-1`. Puede configurar la región de implementación en el archivo `commons.tfvars`. Para el acceso al modelo fundacional entre regiones, tenga en cuenta las opciones siguientes:

- Atravesar la Internet pública: si el tráfico puede atravesar la Internet pública, añada puertas de enlace de Internet a la VPC. A continuación, ajuste el grupo de seguridad asignado a la función Lambda `data-ingestion-processor` y a la instancia de SageMaker AI notebook para permitir el tráfico saliente a la Internet pública.
- No atravesar la Internet pública: para implementar este ejemplo en cualquier otra región que no sea `us-east-1` ni `us-west-1`, haga lo siguiente:

1. En la región `us-east-1` o `us-west-1`, cree una VPC adicional que incluya un punto de conexión de VPC para `bedrock-runtime`.
2. Cree una conexión de emparejamiento mediante el emparejamiento de VPC o una puerta de enlace de tránsito a la VPC de la aplicación.
3. Al configurar el cliente `bedrock-runtime` de boto3 en cualquier función de Lambda fuera de `us-east-1` o `us-west-1`, pase el nombre de DNS privado del punto de conexión de VPC para `bedrock-runtime` en `us-east-1` o us-west-1 como `endpoint_url` al cliente de boto3.

Implemente la lógica de preprocesamiento en un modelo de aprendizaje automático en un único punto final mediante una canalización de inferencias en Amazon SageMaker

Mohan Gowda Purushothama, Gabriel Rodriguez Garcia y Mateusz Zaremba, Amazon Web Services

Resumen

Este patrón explica cómo implementar varios objetos del modelo de canalización en un único punto final mediante una canalización de inferencia en Amazon SageMaker. El objeto del modelo de canalización representa diferentes etapas del flujo de trabajo del machine learning (ML), como el preprocesamiento, la inferencia de modelos y el posprocesamiento. Para ilustrar el despliegue de objetos del modelo de canalización conectados en serie, este patrón muestra cómo implementar un contenedor Scikit-learn de preprocesamiento y un modelo de regresión basado en el algoritmo de aprendizaje lineal incorporado en él. SageMaker La implementación se aloja en un único punto final. SageMaker

> **Note**
>
> La implementación de este patrón utiliza el tipo de instancia ml.m4.2xlarge. Le recomendamos usar un tipo de instancia que se ajuste a sus requisitos de tamaño de datos y a la complejidad de su flujo de trabajo. Para obtener más información, consulta los SageMaker precios de Amazon. Este patrón usa imágenes de Docker prediseñadas para Scikit-learn, pero puede usar sus propios contenedores de Docker e integrarlos en su flujo de trabajo.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Python 3.9
- Amazon SageMaker Python SDK y biblioteca Boto3
- Función de AWS Identity and Access Management (AWS IAM) con SageMaker permisos básicos y permisos de Amazon Simple Storage Service (Amazon S3)

Versiones de producto

- Amazon SageMaker Python SDK 2.49.2

Arquitectura

Pila de tecnología de destino

- Amazon Elastic Container Registry (Amazon ECR)
- Amazon SageMaker
- Amazon SageMaker Studio
- Amazon Simple Storage Service (Amazon S3)
- Punto final de inferencia en tiempo real para Amazon SageMaker

Arquitectura de destino

El siguiente diagrama muestra la arquitectura para el despliegue de un objeto del modelo de SageMaker canalización de Amazon.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un SageMaker cuaderno despliega un modelo de canalización.
2. Un bucket de S3 almacena los artefactos del modelo.
3. Amazon ECR obtiene las imágenes del contenedor de origen del bucket de S3.

Tools (Herramientas)

Herramientas de AWS

- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon SageMaker es un servicio de aprendizaje automático gestionado que le ayuda a crear y entrenar modelos de aprendizaje automático y, a continuación, a implementarlos en un entorno hospedado listo para la producción.

- Amazon SageMaker Studio es un entorno de desarrollo integrado (IDE) basado en la web para el aprendizaje automático que le permite crear, entrenar, depurar, implementar y supervisar sus modelos de aprendizaje automático.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Código

El código de este patrón está disponible en GitHub Inference Pipeline con los repositorios Scikit-learn y Linear Learner.

Epics

Prepare el conjunto de datos

Tarea	Descripción	Habilidades requeridas

Prepare el conjunto de datos para la tarea de regresión.	Abre una libreta en Amazon SageMaker Studio.
	
	Para importar todas las bibliotecas necesarias e inicializar su entorno de trabajo, utilice el siguiente código de ejemplo en su bloc de notas:
	
	`import sagemaker`
	`from sagemaker import get_execution_role`
	
	`sagemaker_session = sagemaker.Session()`
	
	`# Get a SageMaker-compatible role used by this Notebook Instance.`
	`role = get_execution_role()`
		Científico de datos

Tarea	Descripción	Habilidades requeridas

	<pre>```
	# S3 prefix
	bucket = sagemaker
	_session.default_b
	ucket()
	prefix = "Scikit-L
	inearLearner-pipel
	ine-abalone-example"
	``</pre>
	Para descargar un conjunto de datos de muestra, añada el siguiente código a su bloc de notas:
	<pre>```
	! mkdir abalone_data
	! aws s3 cp s3://sage
	maker-sample-files
	/datasets/tabular/
	uci_abalone/abalon
	e.csv ./abalone_data
	``</pre>
	Note
	El ejemplo de este patrón utiliza el conjunto de datos Abalone del repositorio de machine learning de UCI.	

Tarea	Descripción	Habilidades requeridas

Cargue el conjunto de datos en un bucket de S3.	En el bloc de notas en el que preparó su conjunto de datos anteriormente, añada el siguiente código para cargar los datos de muestra en un bucket de S3:
	`WORK_DIRECTORY = "abalone_data"`
	`train_input = sagemaker_session.upload_data( path="{}/{}".format(WORK_DIRECTORY, "abalone.csv"), bucket=bucket, key_prefix="{}/{}".format(prefix, "train"), )`
		Científico de datos

Cree el preprocesador de datos mediante SKLearn

Tarea	Descripción	Habilidades requeridas
Prepare el script preprocesor.py.	1. Copie la lógica de preprocesamiento del archivo de Python en el repositorio GitHub sklearn_abalone_featurizer.py y, a continuación, pegue el código en un archivo de Python independiente denominado `sklearn_abalone_featurizer.py` . Puede modificar el	Científico de datos

Tarea	Descripción	Habilidades requeridas
	código para que se adapte a su conjunto de datos y flujo de trabajo personalizados. 2. Guarde el `sklearn_abalone_featurizer.py` archivo en el directorio raíz del proyecto (es decir, en la misma ubicación en la que ejecuta el SageMaker bloc de notas).	

Tarea	Descripción	Habilidades requeridas

Cree el objeto del SKLearn preprocesador.	Para crear un objeto SKLearn preprocesador (denominado SKLearn Estimator) que pueda incorporar a su proceso de inferencia final, ejecute el siguiente código en su bloc de notas: SageMaker
	`from sagemaker.sklearn.estimator import SKLearn`
	
	`FRAMEWORK_VERSION = "0.23-1"`
	`script_path = "sklearn_abalone_featurizer.py"`
	
	`sklearn_preprocessor = SKLearn(`
	`entry_point=script_path,`
	`role=role,`
	`framework_version=FRAMEWORK_VERSION,`
	`instance_type="ml.c4.xlarge",`
	`sagemaker_session=sagemaker_session,`
	`)`
	`sklearn_preprocessor.fit({"train": train_input})`
		Científico de datos

Tarea	Descripción	Habilidades requeridas

Pruebe la inferencia del preprocesador.	Para confirmar que el preprocesador está definido correctamente, inicie un trabajo de transformación por lotes introduciendo el siguiente código en su bloc de notas: SageMaker
	
	`# Define a SKLearn Transformer from the trained SKLearn Estimator`
	`transformer = sklearn_preprocessor.transformer(`
	`instance_count=1, instance_type="ml.m5.xlarge", assemble_with="Line", accept="text/csv"`
	`)`
	
	`# Preprocess training input`
	`transformer.transform(train_input, content_type="text/csv")`
	`print("Waiting for transform job: " + transformer.latest_transform_job.job_name)`
	`transformer.wait()`
	`preprocessed_train = transformer.output_path`	

Cree un modelo de machine learning

Tarea	Descripción	Habilidades requeridas

Cree un objeto modelo.	Para crear un objeto modelo basado en el algoritmo de aprendizaje lineal, introduzca el siguiente código en su SageMaker bloc de notas:
	`import boto3 from sagemaker .image_uris import retrieve`
	
	`ll_image = retrieve( "linear-learner", boto3.Session().region_name) s3_ll_output_key_prefix = "ll_training_output" s3_ll_output_location = "s3://{}/{}/{}/{}" .format( bucket, prefix, s3_ll_output_key_prefix, "ll_model" )`
	
	`ll_estimator = sagemaker.estimator.Estimator( ll_image, role, instance_count=1, instance_type="ml.m4.2xlarge", volume_size=20, max_run=3600, input_mode="File",`
		Científico de datos

Tarea	Descripción	Habilidades requeridas

	`output_path=s3_ll_output_location, sagemaker_session=sagemaker_session, )`
	
	`ll_estimator.set_hyperparameters(feature_dim=10, predictor_type="regressor", mini_batch_size=32)`
	
	`ll_train_data = sagemaker.inputs.TrainingInput( preprocessed_train, distribution="FullyReplicated", content_type="text/csv", s3_data_type="S3Prefix", )`
	
	`data_channels = {"train": ll_train_data} ll_estimator.fit(inputs=data_channels, logs=True)`
	
	El código anterior recupera la imagen de Docker de Amazon ECR correspondiente del registro público de Amazon ECR del modelo, crea un objeto estimador y, a continuación, utiliza ese objeto	

Tarea	Descripción	Habilidades requeridas
	para entrenar el modelo de regresión.	

Implemente la canalización final

Tarea	Descripción	Habilidades requeridas

Implemente el modelo de canalización.	Para crear un objeto de modelo de canalización (es decir, un objeto de preproces ador) e implementar el objeto, introduzca el siguiente código en su SageMaker bloc de notas:
	`from sagemaker.model import Model`
	`from sagemaker.pipeline import PipelineModel`
	`import boto3`
	`from time import gmtime, strftime`
	
	`timestamp_prefix = strftime("%Y-%m-%d-%H-%M-%S", gmtime())`
	
	`scikit_learn_inferencee_model = sklearn_preprocessor.create_model()`
	`linear_learner_model = ll_estimator.create_model()`
		Científico de datos

Tarea	Descripción	Habilidades requeridas

	`model_name = "inferenc e-pipeline-" + timestamp_prefix endpoint_name = "inference-pipeline- ep-" + timestamp_prefix sm_model = PipelineM odel( name=model_name, role=role, models= [scikit_learn_infe rencee_model, linear_learner_model] )`
	
	`sm_model.deploy(init ial_instance_count =1, instance_type="ml. c4.xlarge", endpoint_ name=endpoint_name)`
	
	Note
	Puede ajustar el tipo de instancia utilizado en el objeto modelo para adaptarlo a sus necesidades.	

Tarea	Descripción	Habilidades requeridas

Pruebe la inferencia.	Para confirmar que el punto final funciona correctamente, ejecute el siguiente código de inferencia de ejemplo en su SageMaker bloc de notas:
	`from sagemaker.predicto r import Predictor from sagemaker.serializ ers import CSVSerial izer`
	
	`payload = "M, 0.44, 0.365, 0.125, 0.516, 0.2155, 0.114, 0.155" actual_rings = 10 predictor = Predictor( endpoint_name=endp oint_name, sagemaker _session=sagemaker _session, serialize r=CSVSerializer() )`
	
	`print(predictor .predict(payload))`
		Científico de datos

Recursos relacionados

- Procese previamente los datos de entrada antes de realizar predicciones mediante las canalizaciones de SageMaker inferencia de Amazon y Scikit-learn (blog de AWS Machine Learning)
- Machine Learning de principio a fin con Amazon SageMaker (GitHub)

Implemente la validación de seguridad de la codificación en tiempo real mediante un servidor MCP con Kiro y otros asistentes de codificación

Ivan Girardi e Iker Reina Fuente, Amazon Web Services

Resumen

Este patrón describe cómo implementar un servidor de Model Context Protocol (MCP) que integre tres herramientas de escaneo de seguridad estándar del sector para proporcionar un análisis exhaustivo de la seguridad del código. El servidor permite a los asistentes de codificación de IA (como Kiro, Amazon Q Developer y Cline) escanear automáticamente fragmentos de código y configuraciones de infraestructura como código (IaC). Con estos escaneos, los asistentes de codificación pueden ayudar a identificar las vulnerabilidades de seguridad, los errores de configuración y las infracciones de conformidad.

Los generadores de códigos de IA entrenados con millones de fragmentos de código crean un punto ciego en materia de seguridad. ¿Cuán seguros estaban los datos de entrenamiento? Este patrón proporciona una validación de seguridad en tiempo real durante la generación del código, lo que ayuda a los desarrolladores a identificar y comprender los posibles problemas de seguridad a medida que codifican. Este enfoque ayuda a los desarrolladores a abordar tanto las vulnerabilidades directas como los riesgos heredados de las dependencias. Al cerrar la brecha entre la eficiencia de la IA y el cumplimiento de las normas de seguridad, este patrón ayuda a permitir la adopción segura de herramientas de desarrollo impulsadas por la IA.

Este patrón ayuda a las organizaciones a mejorar sus prácticas de seguridad de desarrollo mediante herramientas de codificación asistidas por IA, que proporcionan capacidades de escaneo de seguridad continuo en varios lenguajes de programación y definiciones de infraestructura. La solución combina las capacidades de las siguientes herramientas:

- Compruebe si puede escanear archivos de IaC, incluidos los manifiestos de Terraform y AWS CloudFormation Kubernetes
- Semgrep para analizar múltiples lenguajes de programación como Python JavaScript, Java y otros
- Bandit para el escaneo de seguridad especializado en Python

Entre las principales características de esta solución se incluyen las siguientes:

- Escaneo delta de nuevos segmentos de código, lo que reduce la sobrecarga computacional
- Entornos de herramientas de seguridad aislados, lo que evita la contaminación entre herramientas
- Integración perfecta con los asistentes de codificación de IA (Kiro, Amazon Q Developer, Cline y otros)
- Comentarios de seguridad en tiempo real durante la generación de código
- Reglas de escaneo personalizables para el cumplimiento organizacional

El patrón proporciona una interfaz unificada para el escaneo de seguridad con formatos de respuesta estandarizados, lo que facilita la integración de los controles de seguridad en los flujos de trabajo de desarrollo. El patrón utiliza Python y el marco MCP para ofrecer comentarios de seguridad automatizados. Este enfoque ayuda a los desarrolladores a identificar y abordar los problemas de seguridad al principio del proceso de desarrollo, a la vez que aprenden sobre las mejores prácticas de seguridad a través de hallazgos detallados.

Requisitos previos y limitaciones

Requisitos previos

- Un desarrollador activo Cuenta de AWS con acceso a Kiro o Amazon Q, si quieres usar alguno de esos asistentes de codificación
- Python versión 3.10 o posterior instalada
- uvadministrador de paquetes instalado
- Familiaridad con las herramientas y conceptos de escaneo de seguridad
- Comprensión básica de la IaC y la seguridad de las aplicaciones

Limitaciones

- El escaneo de bandidos se limita únicamente a los archivos de Python.
- El escaneo en tiempo real puede afectar al rendimiento de bases de código grandes.
- Las limitaciones específicas de la herramienta se basan en los formatos de archivo y los idiomas compatibles.
- Se requiere una revisión manual para validar los hallazgos de seguridad.
- Los resultados de los escaneos de seguridad requieren experiencia en seguridad para una interpretación adecuada.

- Algunos Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- Python versión 3.10 o posterior
- Checkov versión 3.0.0 o posterior
- Semgrep versión 1.45.0 o posterior
- Bandit, versión 1.7.5 o posterior
- MCP [cli] versión 1.11.0 o posterior
- Pydantic, versión 1.10.0 o posterior
- Loguru versión 0.6.0 o posterior

Arquitectura

En el siguiente diagrama se muestra la arquitectura para esta solución.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El desarrollador utiliza asistentes de IA (por ejemplo, Kiro, Cline, Amazon Q Developer o Roo Code) para generar o analizar el código. El asistente de IA envía el código para escanearlo de seguridad.
2. El servidor de escáner de seguridad MCP procesa la solicitud enrutándola al escáner especializado apropiado: Checkov para archivos IAC, Semgrep para el análisis de múltiples lenguajes de programación o Bandit para el escaneo de seguridad específico de Python.
3. El asistente de IA envía al desarrollador los resultados del escáner, con los datos de seguridad, los niveles de gravedad, las descripciones detalladas y las correcciones sugeridas.
4. Se establece un circuito de retroalimentación continuo en el que el desarrollador recibe una validación de seguridad en tiempo real, lo que permite realizar correcciones automatizadas mediante asistentes de IA y promueve las mejores prácticas de seguridad durante el desarrollo.

La arquitectura mitiga los siguientes riesgos de seguridad comunes:

- Inyección de comandos
- Inyección rápida
- Recorrido de trayectoria
- Ataques de dependencia
- Agotamiento de recursos

La arquitectura mitiga estos riesgos de seguridad comunes mediante la implementación de las siguientes prácticas recomendadas:

- Todas las entradas del usuario y del modelo de IA se escriben en archivos temporales.
- No se proporcionan entradas directas a los comandos de la interfaz de línea de comandos (CLI).
- El acceso al sistema de archivos está restringido únicamente a los directorios y archivos temporales.
- Los archivos temporales se limpian automáticamente.
- Las respuestas de escaneo están desinfectadas.
- Se aplica un aislamiento del proceso que restringe las capacidades del proceso.
- Se registran todas las actividades de escaneo.

Automatización y escala

El patrón admite la automatización a través de las siguientes capacidades:

- Integración con asistentes de codificación de IA para el escaneo automático de códigos
- Respuestas de API estandarizadas para el procesamiento automatizado
- Configuración mediante archivos de configuración MCP
- Support para el procesamiento por lotes de varios archivos
- Escaneo escalable en varios lenguajes de programación y formatos IaC

El proceso de escaneo se puede automatizar a través de los puntos finales de la API proporcionados:

- `scan_with_checkov`para escanear iAC
- `scan_with_semgrep`para escanear códigos en varios idiomas

- `scan_with_bandit`para escaneos específicos de Python
- `get_supported_formats`para la validación del formato

Al ampliar las herramientas de digitalización, siga los principios de diseño y las prácticas recomendadas descritos anteriormente en esta sección. Consulte también las prácticas recomendadas.

Tools (Herramientas)

Servicios de AWS

- Kiro es un servicio de programación agencial que trabaja junto con los desarrolladores para convertir las indicaciones en especificaciones detalladas y, luego, en código funcional, documentos y pruebas. Los agentes de Kiro ayudan a los desarrolladores a resolver problemas complejos y a automatizar tareas como la generación de documentación y las pruebas unitarias.
- Amazon Q Developer es un asistente conversacional generativo basado en inteligencia artificial que puede ayudarlo a comprender, crear, ampliar y operar aplicaciones. AWS

Otras herramientas

- Bandit es una herramienta de escaneo de seguridad especializada en Python. Detecta problemas de seguridad comunes de Python, como funciones inseguras, secretos codificados y vulnerabilidades de inyección. Bandit proporciona índices detallados de confianza y gravedad.
- Checkov es una herramienta de análisis de código estático que comprueba si el IaC está mal configurado en materia de seguridad y conformidad. Además, Checkov detecta las infracciones de conformidad y las mejores prácticas de seguridad.
- Cline es un asistente de codificación impulsado por IA que se ejecuta en VS Code.
- Loguru es una biblioteca de validación de datos para Python.
- El Model Context Protocol (MCP) es un marco de código abierto para crear herramientas de desarrollo asistidas por IA.
- Pydantic es una biblioteca de validación de datos para Python.
- Semgrep analiza el código fuente en busca de vulnerabilidades y errores de seguridad. Es compatible con varios lenguajes de programación. Semgrep utiliza conjuntos de reglas centrados en la seguridad para un análisis exhaustivo. Proporciona calificaciones detalladas de confianza y gravedad.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub MCP Security Scanner: Real-Time Protection for AI Code Assistants. El repositorio incluye la implementación del servidor MCP, detalles sobre la configuración del MCP para Kiro, Amazon Q Developer, Cline y otros, ejemplos de configuración y utilidades de prueba.

La estructura del repositorio incluye lo siguiente:

- `security_scanner_mcp_server/`- Implementación del servidor principal
- `docs/`- Documentación y materiales de demostración
- `tests/`- Archivos de prueba
- `mcp-config-example.json`- Ejemplo de configuración de MCP
- `requirements.txt`- Dependencias del proyecto

Prácticas recomendadas

Implementación de escaneos de seguridad

- Revise los hallazgos de seguridad para validar y priorizar los problemas.
- Mantenga las herramientas de escaneo (Checkov, Semgrep y Bandit) actualizadas a las versiones más recientes.
- Utilice la herramienta de seguridad MCP de este patrón junto con otras medidas y herramientas de seguridad.
- Actualice los conjuntos de reglas y políticas de seguridad con regularidad.

Administración de la configuración

- Utilice los archivos de configuración del MCP de la fuente oficial de control de versiones.
- Documente las reglas y configuraciones personalizadas.

Integration

- Integre el escaneo de seguridad al principio del ciclo de desarrollo.
- Configure el escaneo automatizado en enlaces previos a la confirmación o en canalizaciones de integración e implementación continuas (CI/CD).

- Configure los umbrales de gravedad adecuados para su entorno.
- Establezca procedimientos claros para gestionar los hallazgos de seguridad.

Consideraciones operativas

- Supervise el rendimiento del escaneo y el uso de los recursos.
- Implemente un manejo y registro de errores adecuados.
- Mantenga la documentación de las configuraciones personalizadas.
- Establezca un proceso para revisar y actualizar las reglas de seguridad.

Además, tenga en cuenta las siguientes prácticas recomendadas:

- Valide siempre los hallazgos de seguridad en su contexto específico.
- Mantenga actualizadas las dependencias y las herramientas de seguridad.
- Utilice varias herramientas de seguridad para obtener una cobertura integral.
- Siga las mejores prácticas de seguridad en su proceso de desarrollo.

Epics

(Usuarios de Kiro) Configure el servidor del escáner de seguridad MCP

Tarea	Descripción	Habilidades requeridas
Configure los ajustes del MCP.	Puede editar los archivos de configuración en Kiro (opción 1) localizándolos manualmente o (opción 2) utilizando el IDE de Kiro. • (Opción 1) Localice y edite los archivos de configuración manualmente de la siguiente manera: • Ruta: `.kiro/settings/mcp.json`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	(local) o `~/.kiro/settings/mcp.json` (global)
	• (Opción 2) Modifique los archivos de configuración mediante el IDE de Kiro de la siguiente manera:
	  • Elija el símbolo de Kiro en el menú de navegación de la izquierda.
	  • Navegue hasta la sección «SERVIDORES MCP».
	  • Edite los ajustes de configuración. Los cambios realizados con el IDE de Kiro se guardarán en uno de estos archivos de configuración: `.kiro/settings/mcp.json` (local) o `~/.kiro/settings/mcp.json` (global)
	• (Ambas opciones) Tras completar la opción 1 o la opción 2, añada la configuración del escáner de seguridad `.kiro/settings/mcp.json` (local) o `~/.kiro/settings/mcp.json` (global):
	`{`
	`  "mcpServers": {`	

Tarea	Descripción	Habilidades requeridas

	<pre>"security-scanner"
	: {
	"command": "uvx",
	"args": [
	"--from",
	"git+http
	s://github.com/aws
	-samples/sample-mc
	p-security-scanner
	.git@main",
	"security
	_scanner_mcp_server"
	],
	"env": {
	"FASTMCP_
	LOG_LEVEL": "ERROR"
	},
	"disabled":
	false,
	"autoApprove": []
	}
	}
	}</pre>	

(Usuarios desarrolladores de Amazon Q) Configurar el servidor del escáner de seguridad MCP

Tarea	Descripción	Habilidades requeridas
Configure los ajustes del MCP.	Para configurar los ajustes del MCP manualmente, siga estos pasos: 1. Edite el archivo de configuración del MCP en `~/.aws/amazonq/mcp.json` (global) o `.amazonq/mcp.json` (local).	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	2. Añada la siguiente configuración de escáner de seguridad `~/.aws/amazonq/mcp.json` (global) o `.amazonq/mcp.json` (local): `{ "mcpServers": { "security-scanner" : { "command": "uvx", "args": [ "--from", "git+https://github.com/aws-samples/sample-mcp-security-scanner.git@main", "security_scanner_mcp_server" ], "env": { "FASTMCP_LOG_LEVEL": "ERROR" } } } }`	

(Usuarios de Cline) Configure el servidor del escáner de seguridad MCP

Tarea	Descripción	Habilidades requeridas
Configure los ajustes del MCP.	Para configurar los ajustes del MCP manualmente, siga estos pasos:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	1. Elija la extensión para abrirla y, a continuación, seleccione Servidores MCP. 2. Seleccione la pestaña Instalado y, a continuación, elija Configurar servidores MCP para abrir el `cline_mcp_settings.json` archivo. 3. Agregue la siguiente configuración de escáner de seguridad: `cline_mcp_settings.json` `{ "mcpServers": { "security-scanner": { "command": "uvx", "args": [ "--from", "git+https://github.com/aws-samples/sample-mcp-security-scanner.git@main", "security_scanner_mcp_server" ], "env": { "FASTMCP_LOG_LEVEL": "ERROR" }, "disabled": false, "autoApprove": []`	

Tarea	Descripción	Habilidades requeridas
	<pre> } } }</pre>	

Ejemplo de análisis de código con Python y Bandit

Tarea	Descripción	Habilidades requeridas

Realice el análisis del código.	Para realizar un análisis de código mediante Python y Bandit, siga los siguientes pasos:
	
	1. Cree un nuevo archivo de Python denominado `bandit_test.py` con el siguiente contenido:
	
	<pre>import pickle
	import yaml
	import subprocess
	from flask import
	 Flask, request
	import hashlib
	
	app = Flask(__n
	ame__)
	
	@app.route("/unsafe
	_pickle", methods=[
	"POST"])
	def unsafe_pi
	ckle_usage():
	    data = request.g
	et_data()
	    return pickle.lo
	ads(data)</pre>
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	``
	@app.route("/com
	mand_injection",
	 methods=["GET"])
	def command_i
	njection():
	    command =
	 request.args.get("
	cmd")
	    return subproces
	s.Popen(command,
	 shell=True)
	
	def weak_crypto():
	    password =
	 "secret_password"
	    return hashlib.m
	d5(password.encode
	()).hexdigest()
	
	PASSWORD = "super_se
	cret_password123"
	``
	2. Abre el asistente de codificación. Solicita las siguientes acciones en el chat: Escanea el script actual y dime los resultados.	

Ejemplo de análisis de código con Terraform y Checkov

Tarea	Descripción	Habilidades requeridas
Realice el análisis del código.	Para realizar un análisis de código mediante Terraform y Checkov, siga los siguientes pasos:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	1. Cree un nuevo archivo de Terraform llamado `terraform_test.tf` con el siguiente contenido:
	
	`resource "aws_s3_bucket" "insecure_bucket" {`
	`bucket = "my-insecure-bucket"`
	`acl = "public-read"`
	`}`
	
	`resource "aws_security_group" "wide_open" {`
	`name = "allow_all"`
	`description = "Allow all inbound traffic"`
	
	`ingress {`
	`from_port = 0`
	`to_port = 0`
	`protocol = "-1"`
	`cidr_blocks = ["0.0.0.0/0"]`
	`}`
	`}`
	
	2. Abre el asistente de codificación. Solicita las siguientes acciones en	

Tarea	Descripción	Habilidades requeridas
	el chat: Escanea el script actual y dime los resultados.	

Ejemplo de capacidades de escaneo avanzadas

Tarea	Descripción	Habilidades requeridas
Realice un escaneo específico.	A continuación, se muestran algunos ejemplos de solicitudes que puede utilizar para realizar un análisis específico: • Escanea el proyecto actual y dime los resultados. • Escanea las líneas 6 a 10 del script actual.	Desarrollador de aplicaciones
Utilice el escaneo de seguridad con la generación de código.	Para resolver los problemas de seguridad mediante bucles de generación de código, siga los siguientes pasos (en este ejemplo se utiliza Kiro como asistente de codificación): 1. En Kiro, pregunte: cree una tabla de DynamoDB en Terraform y escanee el código con el escáner de seguridad. 2. En Kiro, pregunte: revise el código generado y los resultados del escaneo de seguridad y siga los bucles de generación de código	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	para resolver los problemas de seguridad.	

Resolución de problemas

Problema	Solución
Problemas de configuración del entorno	• Compruebe que esté instalada la versión 3.10 o posterior de Python. • Asegúrese de que el administrador de `uv` paquetes esté instalado.
Problemas con el escáner	• Compruebe que los formatos de archivo sean compatibles. • Compruebe que la sintaxis del archivo sea válida. • Asegúrese de que se utilizan las extensiones de archivo adecuadas. • Revise la configuración del tiempo de espera del escaneo.
Problemas de integración	• Compruebe que el servidor MCP esté funcionando. • Compruebe que el archivo de configuración es correcto. • Valide los puntos finales de la API. • Asegúrese de que el formato de respuesta sea válido.
Compatibilidad adicional	• Revise los registros para ver los mensajes de error detallados. • Consulte la documentación específica de la herramienta.

Problema	Solución
	• Crea una edición en el repositorio.

Recursos relacionados

AWS documentación

- La infraestructura como código (AWS documento técnico: introducción a DevOps On) AWS

Otros recursos AWS

- Prácticas recomendadas para seguridad, identidad y conformidad

Otros recursos

- Documentación sobre bandidos
- Consulte la documentación
- Documentación del Protocolo de contexto modelo (MCP)
- Prácticas de codificación segura de OWASP (sitio web de la Fundación OWASP)
- Documentación de Semgrep

Información adicional

Ejemplo de configuración de MCP con la aprobación automática habilitada

Si no `autoApprove` está configurado, el usuario debe aprobar el envío del código al servidor de seguridad MCP para su escaneo. Cuando `autoApprove` está configurado, el asistente de código puede invocar las herramientas sin la aprobación del usuario. Estas herramientas se ejecutan localmente en la máquina, no se envían datos y solo se escanea el código.

La siguiente configuración permite la ejecución automática de todas las funciones de escaneo de seguridad:

```
{
  "mcpServers": {
    "security-scanner": {
```

```
      "command": "uvx",
      "args": [
        "--from",
        "git+https://github.com/aws-samples/sample-mcp-security-scanner.git@main",
        "security_scanner_mcp_server"
      ],
      "env": {
        "FASTMCP_LOG_LEVEL": "ERROR"
      },
      "disabled": false,
      "autoApprove": [
        "scan_with_checkov",
        "scan_with_semgrep",
        "scan_with_bandit",
        "get_supported_formats"
      ]
    }
  }
}
```

Para habilitar el registro de depuración, establézcalo en`"FASTMCP_LOG_LEVEL"`. `"DEBUG"`

Formatos de archivo compatibles con las herramientas de análisis de seguridad

Cada herramienta de análisis de seguridad de esta solución admite los siguientes formatos de archivo:

Checkov (iAC)

- Terraform: .tf, .tfvars, .tfstate
- CloudFormation — .yaml, .yml, .json, .template
- Kubernetes: .yaml, .yml
- Dockerfile — Dockerfile
- ARM — .json (administrador de recursos de Azure)
- Bíceps: .bicep
- Sin servidor: .yml, .yaml
- Helm: .yaml, .yml, .tpl
- GitHub Acciones: .yml, .yaml
- GitLab_ci: .yml, .yaml

- Ansible: .yml, .yaml

Semgrep (código fuente)

- Python — .py
- JavaScript — .js
- TypeScript — .ts
- Java — .java
- Ir — .go
- C — c.
- C++ — .cpp
- C# — .cs
- Ruby — .rb
- PHP — .php
- Scala — .scala
- Kotlin — .kt
- Rust — .rs

Bandit (solo en Python)

- Python — .py

Demostraciones

Para escanear códigos, prueba los siguientes ejemplos de instrucciones con tu asistente de IA:

- «Escanea el script actual y dime los resultados».
- «Escanea las líneas 20 a 60 y dime los resultados».
- «Escanee este recurso de tabla de Amazon DynamoDB y dígame el resultado».

Para obtener más información, consulte esta demostración de escaneo de código en el repositorio de GitHub este patrón.

Para generar código seguro, prueba los siguientes ejemplos de instrucciones:

- «Genere una configuración de Terraform para crear una tabla de DynamoDB con el cifrado activado y escanéela para detectar problemas de seguridad».
- «Cree una función Lambda de Python que escriba en DynamoDB y analícela en busca de vulnerabilidades».
- «Genere una CloudFormation plantilla para un bucket de S3 con la configuración de seguridad adecuada y compruebe que supera las comprobaciones de seguridad».
- «Escriba un script de Python para consultar DynamoDB con paginación y busque las mejores prácticas de seguridad».
- «Cree un manifiesto de despliegue de Kubernetes para un microservicio que refuerce la seguridad y valídelo».

Para obtener más información, consulta esta demostración de generación de código con escaneo de seguridad en el repositorio de este patrón. GitHub

Desarrolle asistentes avanzados de IA generativa basados en chat mediante RAG y solicitudes ReAct

Praveen Kumar Jeyarajan, Shuai Cao, Noah Hamilton, Kiowa Jackson, Jundong Qiao y Kara Yang, Amazon Web Services

Resumen

Una empresa típica tiene el 70 por ciento de sus datos atrapados en sistemas aislados. Puede utilizar asistentes basados en el chat de IA generativa para obtener información y relaciones entre estos silos de datos mediante interacciones en lenguaje natural. Para aprovechar al máximo la IA generativa, los resultados deben ser fiables, precisos e incluir los datos corporativos disponibles. El éxito de los asistentes basados en el chat depende de lo siguiente:

- Modelos de IA generativa (como Anthropic Claude 2)
- Vectorización de orígenes de datos
- Técnicas de razonamiento avanzadas, como el ReAct marco, para impulsar el modelo

Este patrón proporciona enfoques de recuperación de datos desde orígenes de datos como los buckets de Amazon Simple Storage Service (Amazon S3), AWS Glue y Amazon Relational Database Service (Amazon RDS). El valor se obtiene de esos datos intercalando la generación aumentada de recuperación (RAG) con los métodos. chain-of-thought Los resultados permiten mantener conversaciones complejas con asistentes basados en el chat que utilizan la totalidad de los datos almacenados en su empresa.

Este patrón utiliza los SageMaker manuales de Amazon y las tablas de datos de precios como ejemplo para explorar las capacidades de un asistente generativo basado en el chat de IA. Crearás un asistente basado en el chat que ayude a los clientes a evaluar el SageMaker servicio respondiendo a preguntas sobre los precios y las capacidades del servicio. La solución utiliza una biblioteca Streamlit para crear la aplicación frontend y el LangChain marco para desarrollar el backend de la aplicación con la tecnología de un gran modelo de lenguaje (LLM).

Las consultas al asistente basado en el chat se responden con una clasificación inicial de intenciones para redirigirlas a uno de los tres posibles flujos de trabajo. El flujo de trabajo más sofisticado combina una orientación de asesoramiento general con un análisis de precios complejo. Puede adaptar el patrón para que se ajuste a los casos de uso empresarial, corporativo e industrial.

Requisitos previos y limitaciones

Requisitos previos

- La Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada.
- Kit de herramientas AWS Cloud Development Kit (AWS CDK) 2.114.1 o posterior instalado y configurado.
- Conocimientos básicos sobre Python y AWS CDK.
- Git instalado
- Docker instalado
- Python 3.11 o posterior instalado y configurado (para obtener más información, consulte la sección Herramientas).
- Una cuenta de AWS activa iniciada mediante AWS CDK.
- El acceso a los modelos de Amazon Titan y Anthropic Claude habilitado en el servicio Amazon Bedrock.
- Credenciales de seguridad de AWS, incluida `AWS_ACCESS_KEY_ID`, correctamente configuradas en su entorno de terminal

Limitaciones

- LangChain no es compatible con todos los LLM para la transmisión. Los modelos Anthropic Claude son compatibles, pero los modelos de AI21 Labs no.
- Esta solución se implementa en una única cuenta de AWS.
- Esta solución solo se puede implementar en las regiones de AWS en las que estén disponibles Amazon Bedrock y Amazon Kendra. Para obtener información sobre la disponibilidad, consulte la documentación de Amazon Bedrock y Amazon Kendra.

Versiones de producto

- Python versión 3.11 o posterior
- Streamlit versión 1.30.0 o posterior
- Streamlit versión de chat 0.1.1 o posterior
- LangChain versión 0.1.12 o posterior
- AWS CDK versión 2.132.1 o posterior

Arquitectura

Pila de tecnología de destino

- Amazon Athena
- Amazon Bedrock
- Amazon Elastic Container Service (Amazon ECS)
- AWS Glue
- AWS Lambda
- Amazon S3
- Amazon Kendra
- Elastic Load Balancing

Arquitectura de destino

El código de AWS CDK implementará todos los recursos necesarios para configurar la aplicación de asistente basado en el chat en una cuenta de AWS. La aplicación de asistente basada en el chat que se muestra en el siguiente diagrama está diseñada para responder a las consultas SageMaker relacionadas de los usuarios. Los usuarios se conectan a través de un equilibrador de carga de aplicación a una VPC que contiene un clúster de Amazon ECS que aloja la aplicación Streamlit. Una función de Lambda de orquestación se conecta a la aplicación. Los orígenes de datos del bucket de S3 proporcionan datos a la función de Lambda a través de Amazon Kendra y AWS Glue. La función de Lambda se conecta a Amazon Bedrock para responder a las consultas (preguntas) de los usuarios de asistentes basados en el chat.

1. La función de Lambda de orquestación envía la solicitud de petición LLM al modelo de Amazon Bedrock (Claude 2).
2. Amazon Bedrock devuelve la respuesta LLM a la función de Lambda de orquestación.

Flujo lógico dentro de la función de Lambda de orquestación

Cuando los usuarios hacen una pregunta a través de la aplicación Streamlit, esta invoca directamente la función de Lambda de orquestación. El siguiente diagrama muestra el flujo lógico cuando se invoca la función de Lambda.

- Paso 1: la entrada `query` (pregunta) se clasifica en una de las tres intenciones:
  - Preguntas de SageMaker orientación general
  - Preguntas generales SageMaker sobre precios (formación/inferencia)
  - Preguntas complejas relacionadas con los precios SageMaker
- Paso 2: la entrada `query` inicia uno de los tres servicios:
  - `RAG Retrieval service`, que recupera el contexto relevante de la base de datos vectorial de Amazon Kendra y llama al LLM a través de Amazon Bedrock para resumir el contexto recuperado como respuesta.
  - `Database Query service`, que utiliza el LLM, los metadatos de la base de datos y las filas de muestra de las tablas relevantes para convertir la entrada `query` en una consulta SQL. El servicio Database Query ejecuta la consulta SQL en la base de datos de SageMaker precios a través de Amazon Athena y resume los resultados de la consulta como respuesta.
  - `In-context ReACT Agent service`, que divide la entrada `query` en varios pasos antes de proporcionar una respuesta. El agente utiliza `RAG Retrieval service` y `Database Query service` como herramientas para recuperar información relevante durante el proceso de razonamiento. Una vez completados los procesos de razonamiento y acción, el agente genera la respuesta final como respuesta.
- Paso 3: la respuesta de la función de Lambda de orquestación se envía a la aplicación Streamlit como salida.

Tools (Herramientas)

Servicios de AWS

- Amazon Athena es un servicio interactivo de consultas que le permite analizar datos directamente en Amazon Simple Storage Service (Amazon S3) usando SQL estándar.
- Amazon Bedrock es un servicio totalmente gestionado que pone a su disposición modelos básicos de alto rendimiento (FMs) de las principales empresas emergentes de IA y Amazon a través de una API unificada.
- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- La Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de la línea de comandos.

- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores escalable y rápido que ayuda a ejecutar, detener y administrar contenedores en un clúster.
- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos. Este patrón emplea un rastreador de AWS Glue y una tabla del catálogo de datos de AWS Glue.
- Amazon Kendra es un servicio de búsqueda inteligente que usa el procesamiento del lenguaje natural y algoritmos avanzados de machine learning para devolver respuestas específicas a las preguntas de búsqueda a partir de sus datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos. Así, por ejemplo, puede distribuir el tráfico a través de instancias de Amazon Elastic Compute Cloud (Amazon EC2), contenedores y direcciones IP de una o varias zonas de disponibilidad.

Repositorio de código

El código de este patrón está disponible en el GitHub genai-bedrock-chatbotrepositorio.

El repositorio de código contiene los siguientes archivos y carpetas:

- Carpeta `assets`: los activos estáticos, el diagrama de arquitectura y el conjunto de datos público.
- Carpeta `code/lambda-container`: el código Python que se ejecuta en la función de Lambda.
- Carpeta `code/streamlit-app`: el código Python que se ejecuta como imagen de contenedor en Amazon ECS.
- Carpeta `tests`: los archivos de Python que se ejecutan para realizar pruebas unitarias de los constructos de AWS CDK.
- Carpeta `code/code_stack.py`: los archivos de Python de constructo de AWS CDK usados para crear los recursos de AWS.

- `app.py`: los archivos de Python de la pila de AWS CDK que se utilizan para implementar los recursos de AWS en la cuenta de AWS de destino.
- `requirements.txt`: la lista de todas las dependencias de Python que se deben instalar para AWS CDK.
- `requirements-dev.txt`: la lista de todas las dependencias de Python que se deben instalar para AWS CDK para ejecutar el conjunto de pruebas unitarias.
- `cdk.json` – El archivo de entrada que proporciona los valores necesarios para activar los recursos

Nota: El código de AWS CDK utiliza constructos de nivel 3 (capa 3) y políticas de AWS Identity and Access Management (IAM) administradas por AWS para implementar la solución.

Prácticas recomendadas

- El ejemplo de código que se proporciona aquí es solo para una demostración proof-of-concept (PoC) o piloto. Si desea llevar el código a producción, asegúrese de seguir las siguientes prácticas recomendadas:
  - El registro de acceso a Amazon S3 está activado.
  - Los registros de flujos de VPC están activados.
  - El índice Enterprise Edition de Amazon Kendra está activado.
- Configure la supervisión y las alertas para las funciones de Lambda de AWS. Para obtener más información, consulte Supervisión y solución de problemas de funciones de Lambda. Para obtener más información sobre las prácticas recomendadas generales en el uso de funciones de Lambda, consulte la documentación de AWS.

Epics

Configuración de las credenciales de AWS en su máquina local

Tarea	Descripción	Habilidades requeridas
Exporte las variables de la cuenta y región de AWS en	Para proporcionar las credenciales de AWS para	DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
las que se implementará la pila.	AWS CDK mediante variables de entorno, ejecute los siguientes comandos. `export CDK_DEFAU LT_ACCOUNT=<12 Digit AWS Account Number> export CDK_DEFAU LT_REGION=<region>`	
Configure el perfil de AWS CLI.	Para configurar el perfil de AWS CLI para la cuenta, siga las instrucciones de la documentación de AWS.	DevOps ingeniero, AWS DevOps

Configure su entorno

Tarea	Descripción	Habilidades requeridas
Clone el repositorio en su máquina local.	Para clonar el repositorio, ejecute el siguiente comando en el terminal. `git clone https://g ithub.com/awslabs/ genai-bedrock-chat bot.git`	DevOps ingeniero, AWS DevOps
Configure el entorno virtual de Python e instale las dependencias necesarias.	Para configurar y activar el entorno virtual de Python, ejecute el siguiente comando. `cd genai-bedrock-chat bot python3 -m venv .venv`	DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`source .venv/bin/activate`
	
	Para configurar las dependencias necesarias, ejecute el siguiente comando.
	
	`pip3 install -r requirements.txt`	

Configure el entorno de AWS CDK y sintetice el código de AWS CDK.	1. Para configurar el entorno de AWS CDK en su cuenta de AWS, ejecute el siguiente comando. `cdk bootstrap aws://ACCOUNT-NUMBER/REGION` 2. Para convertir el código en una configuración de CloudFormation pila de AWS, ejecute el comando`cdk synth`.	DevOps ingeniero, AWS DevOps

Configuración e implementación de la aplicación de asistente basado en el chat

Tarea	Descripción	Habilidades requeridas
Proporcione acceso al modelo Claude.	Para activar el acceso al modelo Anthropic Claude en su cuenta de AWS, siga las instrucciones de la documentación de Amazon Bedrock.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Implementar recursos en la cuenta.	Para implementar recursos en la cuenta de AWS mediante AWS CDK, haga lo siguiente: 1. En la raíz del repositorio clonado, en el archivo `cdk.json`, introduzca entradas para los parámetros `logging`: Los valores de ejemplo son `INFO`, `DEBUG`, `WARN` y `ERROR`. Estos valores definen los mensajes de registro para la función de Lambda y la aplicación Streamlit. 2. El `app.py` archivo de la raíz del repositorio clonado contiene el nombre de la CloudFormation pila de AWS utilizada para la implementación. El nombre predeterminado de la pila es `chatbot-stack` . 3. Ejecute el `cdk deploy` comando para implementar los recursos. El comando `cdk deploy` usa constructos de L3 para crear varias funciones de Lambda para copiar documentos y archivos de	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	conjuntos de datos CSV en buckets de S3. 4. Una vez completado el comando, inicie sesión en la consola de administración de AWS, abra la CloudFormation consola y compruebe que la pila se ha implementado correctamente. Tras una implementación correcta, puede acceder a la aplicación de asistente basada en el chat mediante la URL proporcionada en la sección de CloudFormation resultados.	

Tarea	Descripción	Habilidades requeridas
Ejecute el rastreador de AWS Glue y cree la tabla del catálogo de datos.	El rastreador de AWS Glue se usa para mantener el esquema de datos dinámico. La solución crea y actualiza las particiones en la tabla del catálogo de datos de AWS Glue mediante la ejecución del rastreador bajo demanda. Una vez copiados los archivos del conjunto de datos CSV en el bucket de S3, ejecute el rastreador de AWS Glue y cree el esquema de la tabla del catálogo de datos para realizar las pruebas: 1. Vaya la consola de AWS Glue. 2. En el panel de navegació n, en Catálogo de datos, seleccione rastreador. 3. Seleccione el rastreador con el sufijo `sagemaker-pricing-crawler` . 4. Ejecute el rastreador. 5. Una vez que el rastreador se ejecuta correctamente, crea una tabla de Catálogo de datos de AWS Glue. **Note** El código de AWS CDK configura el	DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	rastreador de AWS Glue para que se ejecute bajo demanda, pero también puede programarlo para que se ejecute de forma periódica.	

Tarea	Descripción	Habilidades requeridas
Inicie la indexación de documentos.	Una vez copiados los archivos en el bucket de S3, utilice Amazon Kendra para rastrearl os e indexarlos: 1. Vaya a la consola de Amazon Kendra. 2. Seleccione el índice con el sufijo `chatbot-index` . 3. En el panel de navegació n, elija Orígenes de datos y seleccione el conector de orígenes de datos con el sufijo `chatbot-index` . 4. Seleccione Sincroniz ar ahora para iniciar el proceso de indexación. **Note** El código de AWS CDK configura la sincronización de índices de Amazon Kendra para que se ejecute bajo demanda, pero también puede ejecutarla periódica mente mediante el parámetro de programación.	AWS DevOps, DevOps ingeniero

Limpie todos los recursos de AWS de la solución

Tarea	Descripción	Habilidades requeridas
Elimine los recursos de AWS.	Después de probar la solución, limpie los recursos: 1. Para eliminar los recursos de AWS implementados por la solución, ejecute el comando `cdk destroy`. 2. Elimine todos los objetos de los dos buckets de S3 y, a continuación, elimine los buckets. Para obtener más información, consulte Eliminación de un bucket.	DevOps ingeniero, AWS DevOps

Resolución de problemas

Problema	Solución
AWS CDK devuelve errores.	Para obtener ayuda con los errores de AWS CDK, consulte Solución de problemas comunes de AWS CDK.

Recursos relacionados

- Amazon Bedrock:
  - Acceso a modelos
  - Parámetros de inferencia para modelos básicos
- Creación de funciones de Lambda con Python
- Introducción a AWS CDK

- Utilización de AWS CDK en Python
- Creador de aplicaciones de IA generativa en AWS
- LangChain documentación
- Documentación de Streamlit

Información adicional

Comandos de AWS CDK

Cuando trabaje con AWS CDK, recuerde los siguientes comandos útiles:

- Muestra todas las pilas de la aplicación

```
cdk ls
```

- Emite la plantilla de AWS CloudFormation sintetizada

```
cdk synth
```

- Implementa la pila en la cuenta y región de AWS predeterminadas

```
cdk deploy
```

- Compara la pila implementada con el estado actual

```
cdk diff
```

- Abre la documentación de AWS CDK

```
cdk docs
```

- Elimina la CloudFormation pila y elimina los recursos desplegados por AWS

```
cdk destroy
```

Desarrollo de un asistente basado en el chat totalmente automatizado con los agentes y las bases de conocimiento de Amazon Bedrock

Jundong Qiao, Shuai Cao, Noah Hamilton, Kiowa Jackson, Praveen Kumar Jeyarajan y Kara Yang, Amazon Web Services

Resumen

Muchas organizaciones se enfrentan a desafíos a la hora de crear un asistente basado en el chat que sea capaz de organizar diversos orígenes de datos para ofrecer respuestas integrales. Este patrón presenta una solución para desarrollar un asistente basado en el chat que sea capaz de responder a consultas tanto de la documentación como de las bases de datos, con una implementación sencilla.

Empezando por Amazon Bedrock, este servicio de inteligencia artificial generativa (IA) totalmente gestionado ofrece una amplia gama de modelos básicos avanzados (FMs). Esto facilita la creación eficiente de aplicaciones de IA generativa con un fuerte enfoque en la privacidad y la seguridad. En el contexto de la recuperación de documentación, la generación aumentada por recuperación (RAG) es una característica fundamental. Utiliza bases de conocimiento para complementar las peticiones de FM con información relevante desde el punto de vista contextual procedente de orígenes externos. Un índice de Amazon OpenSearch Serverless sirve como base de datos vectorial detrás de las bases de conocimiento de Amazon Bedrock. Esta integración se mejora mediante una ingeniería de peticiones cuidadosa para minimizar las imprecisiones y garantizar que las respuestas se basen en la documentación fáctica. Para las consultas de bases FMs de datos, Amazon Bedrock transforma las consultas textuales en consultas SQL estructuradas, incorporando parámetros específicos. Esto permite la recuperación precisa de los datos de las bases de datos administradas por las bases de datos.AWS Glue Para estas consultas se utiliza Amazon Athena.

Para gestionar consultas más complejas, lograr respuestas integrales exige información procedente tanto de la documentación como de las bases de datos. Agentes para Amazon Bedrock es una característica de IA generativa que lo ayuda a crear agentes autónomos que puedan entender tareas complejas y dividirlas en tareas más sencillas para su orquestación. La combinación de información obtenida de las tareas simplificadas, facilitada por los agentes autónomos de Amazon Bedrock, mejora la síntesis de la información y permite obtener respuestas más completas y exhaustivas. Este patrón demuestra cómo crear un asistente basado en el chat mediante Amazon Bedrock y los servicios y características de IA generativa relacionados dentro de una solución automatizada.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Docker instalado
- AWS Cloud Development Kit (AWS CDK), instalado y arrancado en el o `us-east-1` `us-west-2` Regiones de AWS
- AWS CDK Kit de herramientas, versión 2.114.1 o posterior, instalado
- AWS Command Line Interface (AWS CLI), instalado y configurado
- La versión 3.11 o posterior de Python instalada
- En Amazon Bedrock, habilite el acceso a Claude 2, Claude 2.1, Claude Instant y Titan Embeddings G1 — Text

Limitaciones

- Esta solución se implementa en una sola unidad Cuenta de AWS.
- Esta solución solo se puede implementar en Regiones de AWS lugares donde Amazon Bedrock y Amazon OpenSearch Serverless sean compatibles. Para obtener más información, consulte la documentación de Amazon Bedrock y Amazon OpenSearch Serverless.

Versiones de producto

- Llama-index versión 0.10.6 o posterior
- Sqlalchemy versión 2.0.23 o posterior
- Opensearch-py versión 2.4.2 o posterior
- Requests_aws4auth versión 1.2.3 o posterior
- AWS SDK para Python (Boto3) versión 1.34.57 o posterior

Arquitectura

Pila de tecnología de destino

AWS Cloud Development Kit (AWS CDK)Se trata de un marco de desarrollo de software de código abierto para definir la infraestructura de nube en el código y aprovisionarla mediante ella. AWS CloudFormation La AWS CDK pila utilizada en este patrón emplea los siguientes recursos: AWS

- AWS Key Management Service (AWS KMS)
- Amazon Simple Storage Service (Amazon S3)
- AWS Glue Data Catalog, para el componente de AWS Glue base de datos
- AWS Lambda
- AWS Identity and Access Management (IAM)
- Amazon OpenSearch Serverless
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- AWS Fargate
- Amazon Virtual Private Cloud (Amazon VPC)
- Equilibrador de carga de aplicación

Arquitectura de destino

El diagrama muestra una completa configuración AWS nativa de la nube dentro de una sola Región de AWS, usando múltiples. Servicios de AWS La interfaz principal del asistente basado en el chat es una aplicación de Streamlit alojada en un clúster de Amazon ECS. Un equilibrador de carga de aplicación administra la accesibilidad. Las consultas realizadas a través de esta interfaz activan la función de Lambda `Invocation`, que luego interactúa con los agentes para Amazon Bedrock. Este agente responde a las consultas de los usuarios consultando las bases de conocimiento de Amazon Bedrock o invocando una función de Lambda `Agent executor`. Esta función desencadena un conjunto de acciones asociadas al agente, siguiendo un esquema de API predefinido. Las bases de conocimiento de Amazon Bedrock utilizan un índice OpenSearch sin servidor como base de base de datos vectorial. Además, la `Agent executor` función genera consultas SQL que se ejecutan en la AWS Glue base de datos a través de Amazon Athena.

Tools (Herramientas)

Servicios de AWS

- Amazon Athena es un servicio interactivo de consultas que le permite analizar datos directamente en Amazon Simple Storage Service (Amazon S3) usando SQL estándar.
- Amazon Bedrock es un servicio totalmente gestionado que pone a su disposición modelos básicos de alto rendimiento (FMs) de las principales empresas emergentes de IA y Amazon a través de una API unificada.
- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir y aprovisionar AWS la infraestructura de la nube en código.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que te ayuda a interactuar Servicios de AWS mediante comandos en tu shell de línea de comandos.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores escalable y rápido que ayuda a ejecutar, detener y administrar contenedores en un clúster.
- Elastic Load Balancing permite distribuir el tráfico entrante de las aplicaciones o de la red entre varios destinos. Así, por ejemplo, puede distribuir el tráfico a través de instancias de Amazon Elastic Compute Cloud (Amazon EC2), contenedores y direcciones IP de una o varias zonas de disponibilidad.
- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos. Este patrón utiliza un AWS Glue rastreador y una tabla. AWS Glue Data Catalog
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon OpenSearch Serverless es una configuración sin servidor bajo demanda para Amazon OpenSearch Service. En este patrón, un índice OpenSearch sin servidor sirve como base de datos vectorial para las bases de conocimiento de Amazon Bedrock.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

- Streamlit es un marco de Python de código abierto para crear aplicaciones de datos.

Repositorio de código

El código de este patrón está disponible en el GitHub genai-bedrock-agent-chatbotrepositorio. El repositorio de código contiene los siguientes archivos y carpetas:

- Carpeta `assets`: los activos estáticos, como el diagrama de arquitectura y el conjunto de datos público.
- Carpeta `code/lambdas/action-lambda`: el código de Python de la función de Lambda que actúa como una acción para el agente de Amazon Bedrock.
- `code/lambdas/create-index-lambda`folder: el código de Python de la función Lambda que crea el índice OpenSearch Serverless.
- Carpeta `code/lambdas/invoke-lambda`: el código de Python de la función de Lambda que invoca el agente de Amazon Bedrock, al que se llama directamente desde la aplicación Streamlit.
- `code/lambdas/update-lambda`carpeta: el código de Python de la función Lambda que actualiza o elimina los recursos después de desplegarlos a AWS través de. AWS CDK
- `code/layers/boto3_layer`folder: la AWS CDK pila que crea una capa de Boto3 que se comparte entre todas las funciones de Lambda.
- `code/layers/opensearch_layer`carpeta: la AWS CDK pila que crea una capa OpenSearch sin servidor que instala todas las dependencias para crear el índice.
- `code/streamlit-app`folder: el código de Python que se ejecuta como imagen del contenedor en Amazon ECS.
- `code/code_stack.py`— AWS CDK Construyen archivos de Python que crean AWS recursos.
- `app.py`— La AWS CDK pila de archivos Python que despliegan AWS recursos en la AWS cuenta de destino.
- `requirements.txt`— La lista de todas las dependencias de Python que se deben instalar para. AWS CDK
- `cdk.json`: el archivo de entrada que proporciona los valores necesarios para crear los recursos. Además, en los campos `context/config`, puede personalizar la solución en consecuencia. Para más información sobre la personalización, consulte la sección Información adicional.

Prácticas recomendadas

- El ejemplo de código que se proporciona aquí es únicamente para fines proof-of-concept (PoC) o piloto. Si desea llevar el código a producción, asegúrese de seguir las siguientes prácticas recomendadas:

  - Habilitación del registro de acceso a Amazon S3
  - Habilitación de los registros de flujo de VPC
- Configure la supervisión y las alertas para las funciones de Lambda. Para obtener más información, consulte Supervisión y solución de problemas de funciones de Lambda. Para obtener información sobre las prácticas recomendadas, consulte las prácticas recomendadas para trabajar con AWS Lambda funciones.

Epics

Configure AWS las credenciales en su estación de trabajo local

Tarea	Descripción	Habilidades requeridas
Exporte las variables de cuenta y región.	Para proporcionar AWS las credenciales AWS CDK mediante variables de entorno, ejecute los siguientes comandos. `export CDK_DEFAU LT_ACCOUNT=<12-digit AWS account number> export CDK_DEFAU LT_REGION=<Region>`	AWS DevOps, DevOps ingeniero
Configure el AWS CLI perfil indicado.	Para configurar el perfil AWS CLI designado para la cuenta, siga las instrucciones de los ajustes de configuración y del archivo de credenciales.	AWS DevOps, DevOps ingeniero

Configure su entorno

Tarea	Descripción	Habilidades requeridas
Clone el repositorio en su estación de trabajo local.	Para clonar el repositorio, ejecute el siguiente comando en el terminal. `git clone https://github.com/awslabs/genai-bedrock-agent-chatbot.git`	DevOps ingeniero, AWS DevOps

Configure un entorno de Python virtual.	Para configurar y activar el entorno virtual de Python, ejecute el siguiente comando.
	`cd genai-bedrock-agent-chatbot`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	Para configurar las dependencias necesarias, ejecute el siguiente comando.
	`pip3 install -r requirements.txt`
		DevOps ingeniero, AWS DevOps

Configure el AWS CDK entorno.	Para convertir el código en una AWS CloudFormation plantilla, ejecute el comando`cdk synth`.	AWS DevOps, DevOps ingeniero

Configuración e implementación de la aplicación

Tarea	Descripción	Habilidades requeridas
Implementar recursos en la cuenta.	Para implementar recursos en el Cuenta de AWS mediante el AWS CDK, haga lo siguiente: 1. En la raíz del repositor io clonado, en el archivo `cdk.json`, introduzc a entradas para los parámetros de registro: Los valores de ejemplo son `INFO`, `DEBUG`, `WARN` y `ERROR`. Estos valores definen los mensajes de cada registro para las funciones de Lambda y la aplicación Streamlit. 2. El `cdk.json` archivo de la raíz del repositorio clonado contiene el nombre de la AWS CloudForm ation pila utilizada para la implementación. El nombre predeterminado de la pila es `chatbot-stack` . El nombre predeterminado del agente de Amazon Bedrock es `ChatbotBe drockAgent` y el alias predeterminado del agente de Amazon Bedrock es `Chatbot_Agent` .	DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	3. Ejecute el `cdk deploy` comando para implement ar los recursos. El comando `cdk deploy` usa construct os de capa 3 para crear varias funciones de Lambda para copiar documentos y archivos de conjuntos de datos CSV en buckets de S3. También implement a el agente de Amazon Bedrock, las bases de conocimiento y la función de Lambda `Action group` para el agente de Amazon Bedrock. 4. Inicie sesión en la CloudFormation consola y Consola de administración de AWS, a continuación, ábrala. 5. Confirme que se ha implementado correctam ente la pila. Para obtener instrucciones, consulta Cómo revisar tu pila en la AWS CloudFormation consola. Tras una implementación correcta, puede acceder a la aplicación de asistente basada en el chat mediante la URL proporcionada en la pestaña	

Tarea	Descripción	Habilidades requeridas
	Resultados de la CloudFormation consola.	

Limpie todos los AWS recursos de la solución

Tarea	Descripción	Habilidades requeridas
Elimine los AWS recursos.	Después de probar la solución, limpie los recursos y ejecute el comando `cdk destroy`.	AWS DevOps, DevOps ingeniero

Recursos relacionados

AWS documentación

- Recursos de Amazon Bedrock:
  - Acceso a modelos
  - Parámetros de inferencia para modelos básicos
  - Agentes de Amazon Bedrock
  - Bases de conocimiento de Amazon Bedrock
- Creación de funciones de Lambda con Python
- AWS CDK recursos:
  - Comience con el AWS CDK
  - Solución de AWS CDK problemas comunes
  - Trabajando con el AWS CDK en Python
- Creador de aplicaciones de IA generativa en AWS

Otros recursos AWS

- Motor vectorial para Amazon OpenSearch Serverless

Otros recursos

- LlamaIndex documentación
- Documentación de Streamlit

Información adicional

Personalización del asistente basado en el chat con sus propios datos

Para integrar sus datos personalizados para implementar la solución, siga estas pautas estructuradas. Estos pasos están diseñados para garantizar un proceso de integración eficiente y fluido, lo que le permitirá implementar la solución de manera efectiva con sus datos personalizados.

Para la integración de datos de la base de conocimientos

Preparación de datos

1. Localice el directorio `assets/knowledgebase_data_source/`.
2. Coloque el conjunto de datos en esta carpeta.

Ajustes de configuración

1. Abra el archivo `cdk.json`.
2. Navegue hasta el campo `context/configure/paths/knowledgebase_file_name` y, a continuación, actualícelo en consecuencia.
3. Navegue hasta el campo `bedrock_instructions/knowledgebase_instruction` y, a continuación, actualícelo para que refleje con precisión los matices y el contexto de su nuevo conjunto de datos.

Para la integración de datos estructurales

Organización de datos

1. En el directorio `assets/data_query_data_source/`, cree un subdirectorio, como `tabular_data`.
2. Coloque su conjunto de datos estructurado (los formatos aceptables incluyen CSV, JSON, ORC y Parquet) en esta subcarpeta recién creada.

3. Si se está conectando a una base de datos existente, actualice la función `create_sql_engine()` en `code/lambda/action-lambda/build_query_engine.py` para conectarse a su base de datos.

Actualizaciones de configuración y código

1. En el archivo `cdk.json`, actualice el campo `context/configure/paths/athena_table_data_prefix` para alinearlo con la nueva ruta de datos.
2. Realice `code/lambda/action-lambda/dynamic_examples.csv` la revisión incorporando nuevos text-to-SQL ejemplos que se correspondan con su conjunto de datos.
3. Revise `code/lambda/action-lambda/prompt_templates.py` para reflejar los atributos de su conjunto de datos estructurado.
4. En el archivo `cdk.json`, actualice el campo `context/configure/bedrock_instructions/action_group_description` para explicar el propósito y la funcionalidad de la función de Lambda `Action group`.
5. En el archivo `assets/agent_api_schema/artifacts_schema.json`, explique las nuevas funcionalidades de la función de Lambda `Action group`.

Actualización general

En el archivo `cdk.json`, en la sección `context/configure/bedrock_instructions/agent_instruction`, proporcione una descripción completa de la funcionalidad y el propósito de diseño previstos por el agente de Amazon Bedrock, teniendo en cuenta los datos recién integrados.

Documentación del conocimiento institucional a partir de las entradas de voz mediante Amazon Bedrock y Amazon Transcribe

Praveen Kumar Jeyarajan, Jundong Qiao, Rajiv Upadhyay y Megan Wu, Amazon Web Services

Resumen

Capturar el conocimiento institucional es fundamental para garantizar el éxito y la resiliencia de la organización. El conocimiento institucional representa la sabiduría, los conocimientos y las experiencias colectivos acumulados por los empleados a lo largo del tiempo, a menudo de naturaleza tácita y transmitidos de manera informal. Esta gran cantidad de información abarca enfoques únicos, prácticas recomendadas y soluciones para problemas complejos que tal vez no estén documentados en otros lugares. Al formalizar y documentar este conocimiento, las empresas pueden preservar la memoria institucional, fomentar la innovación, mejorar los procesos de toma de decisiones y acelerar las curvas de aprendizaje de los nuevos empleados. Además, promueve la colaboración, empodera a las personas y cultiva una cultura de mejora continua. En última instancia, el aprovechamiento del conocimiento institucional ayuda a las empresas a utilizar su activo más valioso, la inteligencia colectiva de su fuerza laboral, para superar los desafíos, impulsar el crecimiento y mantener una ventaja competitiva en entornos empresariales dinámicos.

Este patrón explica cómo captar el conocimiento institucional a través de grabaciones de voz de los empleados sénior. Utiliza Amazon Transcribe y Amazon Bedrock para la documentación y verificación sistemáticas. Al documentar este conocimiento informal, puede conservarlo y compartirlo con otros grupos de empleados. Este esfuerzo apoya la excelencia operativa y mejora la eficacia de los programas de formación mediante la incorporación de los conocimientos prácticos adquiridos a través de la experiencia directa.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Docker instalado
- La versión 2.114.1 o posterior de AWS Cloud Development Kit (AWS CDK) instalada y arrancada en las regiones de AWS `us-east-1` o `us-west-2`
- La versión 2.114.1 o posterior del Kit de herramientas de AWS CDK instalada
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada

- La versión 3.12 o posterior de Python instalada
- Permisos para crear recursos de Amazon Transcribe, Amazon Bedrock, Amazon Simple Storage Service (Amazon S3) y AWS Lambda

Limitaciones

- Esta solución se implementa en una única cuenta de AWS.
- Esta solución solo se puede implementar en las regiones de AWS en las que estén disponibles Amazon Bedrock y Amazon Transcribe. Para obtener información sobre la disponibilidad, consulte la documentación de Amazon Bedrock y Amazon Transcribe.
- Los archivos de audio deben estar en un formato compatible con Amazon Transcribe. Para obtener una lista de los formatos compatibles, consulte Formatos multimedia en la documentación de Transcribe.

Versiones de producto

- AWS SDK para Python (Boto3) versión 1.34.57 o posterior
- LangChain versión 0.1.12 o posterior

Arquitectura

La arquitectura representa un flujo de trabajo sin servidor en AWS. AWS Step Functions organiza las funciones de Lambda para el procesamiento de audio, el análisis de texto y la generación de documentos. En el siguiente diagrama se muestra el flujo de trabajo de Step Functions, también conocido como máquina de estado.

Cada paso de la máquina de estado lo gestiona una función de Lambda distinta. Los siguientes son los pasos del proceso de generación de documentos:

1. La función de Lambda `preprocess` valida la entrada pasada a Step Functions y muestra todos los archivos de audio presentes en la ruta de la carpeta URI de Amazon S3 proporcionada. Las funciones de Lambda posteriores del flujo de trabajo utilizan la lista de archivos para validar, resumir y generar el documento.
2. La función de Lambda `transcribe` usa Amazon Transcribe para convertir archivos de audio en transcripciones de texto. Esta función de Lambda es responsable de iniciar el proceso de

transcripción y transformar con precisión la voz en texto, que luego se almacena para su posterior procesamiento.

3. La función de Lambda `validate` analiza las transcripciones del texto y determina la relevancia de las respuestas a las preguntas iniciales. Al utilizar un modelo de lenguaje de gran tamaño (LLM) a través de Amazon Bedrock, identifica y separa las respuestas relacionadas con el tema de las respuestas no relacionadas con el tema.
4. La función de Lambda `summarize` utiliza Amazon Bedrock para generar un resumen coherente y conciso de las respuestas relacionadas con el tema.
5. La función de Lambda `generate` agrupa los resúmenes en un documento bien estructurado. Puede formatear el documento de acuerdo con plantillas predefinidas e incluir cualquier contenido o dato adicional necesario.
6. Si se produce un error en alguna de las funciones de Lambda, recibirá una notificación por correo electrónico a través de Amazon Simple Notification Service (Amazon SNS).

A lo largo de este proceso, AWS Step Functions se asegura de que cada función de Lambda se inicie en la secuencia correcta. Esta máquina de estado tiene la capacidad de procesamiento en paralelo para mejorar la eficiencia. Un bucket de Amazon S3 actúa como repositorio de almacenamiento central y respalda el flujo de trabajo mediante la administración de los distintos formatos multimedia y de documentos involucrados.

Tools (Herramientas)

Servicios de AWS

- Amazon Bedrock es un servicio totalmente gestionado que pone a su disposición modelos básicos de alto rendimiento (FMs) de las principales empresas emergentes de IA y Amazon a través de una API unificada.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de Lambda AWS y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial.
- Amazon Transcribe es un servicio de reconocimiento de voz automático que utiliza modelos de machine learning para convertir audio en texto.

Otras herramientas

- LangChaines un marco para desarrollar aplicaciones que funcionan con modelos de lenguaje de gran tamaño ()LLMs.

Repositorio de código

El código de este patrón está disponible en el GitHub genai-knowledge-capturerepositorio.

El repositorio de código contiene los siguientes archivos y carpetas:

- Carpeta `assets`: los activos estáticos de la solución, como el diagrama de arquitectura y el conjunto de datos público.
- Carpeta `code/lambdas`: el código de Python para todas las funciones de Lambda.
  - Carpeta `code/lambdas/generate`: el código Python que genera un documento a partir de los datos resumidos en el bucket de S3.
  - Carpeta `code/lambdas/preprocess`: el código de Python que procesa las entradas de la máquina de estado de Step Functions.
  - Carpeta `code/lambdas/summarize`: el código de Python que resume los datos transcritos mediante el servicio de Amazon Bedrock.
  - Carpeta `code/lambdas/transcribe`: el código Python que convierte los datos de voz (archivo de audio) en texto mediante Amazon Transcribe.
  - Carpeta `code/lambdas/validate`: el código de Python que valida si todas las respuestas pertenecen al mismo tema.
- `code/code_stack.py`: los archivos de Python de constructo de AWS CDK usados para crear los recursos de AWS.
- `app.py`: los archivos de Python de la aplicación de AWS CDK que se utilizan para implementar los recursos de AWS en la cuenta de AWS de destino.

- `requirements.txt`: la lista de todas las dependencias de Python que se deben instalar para AWS CDK.
- `cdk.json`: el archivo de entrada que proporciona los valores necesarios para crear los recursos.

Prácticas recomendadas

El ejemplo de código proporcionado es únicamente para fines proof-of-concept (PoC) o piloto. Si desea llevar el código a producción, siga las siguientes prácticas recomendadas:

- Habilitación del registro de acceso a Amazon S3
- Habilitación de los registros de flujo de VPC

Epics

Configuración de las credenciales de AWS en su estación de trabajo

Tarea	Descripción	Habilidades requeridas

Exporte las variables de cuenta y región de AWS.	Para proporcionar las credenciales de AWS para AWS CDK mediante variables de entorno, ejecute los siguientes comandos.
	`export CDK_DEFAU LT_ACCOUNT=<12-digit AWS account number>`
	`export CDK_DEFAU LT_REGION=<Region>`
		AWS DevOps, DevOps ingeniero

Configure el perfil con nombre de AWS CLI.	Para configurar el perfil de la AWS CLI para la cuenta, siga las instrucciones de Opciones de los archivos de configuración y credenciales.	AWS DevOps, DevOps ingeniero

Configure su entorno

Tarea	Descripción	Habilidades requeridas
Clone el repositorio en su estación de trabajo local.	Para clonar el genai-knowledge-capturerepositorio, ejecuta el siguiente comando en tu terminal. `git clone https://github.com/aws-samples/genai-knowledge-capture`	AWS DevOps, DevOps ingeniero
(Opcional) Sustituya los archivos de audio.	Para personalizar la aplicación de muestra para que incorpore sus propios datos, haga lo siguiente: 1. Navegue hasta la carpeta `assets/audio_samples` del repositorio clonado. 2. Elimine las carpetas que contienen los archivos de audio de muestra. 3. Cree una carpeta para cada tema que desee analizar. 4. Transfiera sus archivos de audio a sus carpetas respectivas.	AWS DevOps, DevOps ingeniero

Configure un entorno de Python virtual.	Para configurar y activar el entorno virtual de Python, ejecute el siguiente comando.
	`cd genai-knowledge-capture`
	`python3 -m venv .venv`
		AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`source .venv/bin/activate` `pip install -r requirements.txt`	
Sintetice el código de AWS CDK.	Para convertir el código en una configuración de CloudFormation pila de AWS, ejecute el siguiente comando. `cdk synth`	AWS DevOps, DevOps ingeniero

Configuración e implementación de la solución

Tarea	Descripción	Habilidades requeridas
Aprovisione el acceso al modelo fundacional.	Habilite el acceso al modelo Anthropic Claude 3 Sonnet para su cuenta de AWS. Para obtener instrucciones, consulte Adición de un modelo de acceso en la documentación de Bedrock.	AWS DevOps
Implementar recursos en la cuenta.	Para implementar recursos en la cuenta de AWS mediante AWS CDK, haga lo siguiente: 1. (Opcional) En la raíz del repositorio clonado, en el `app.py` archivo, actualiza el nombre de la CloudFormation pila de AWS. El nombre predeterminado de la pila es `genai-kno`	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`wledge-capture-sta ck .` 2. Ejecute el `cdk deploy` comando para implementar los recursos. El comando `cdk deploy` usa constructos de capa 3 para crear un conjunto de funciones de Lambda, un bucket de S3, un tema de Amazon SNS y una máquina de estado de Step Functions. Los archivos de audio de la carpeta `assets/audio_sampl es` se copian en el bucket de S3 durante la implement ación. 3. Inicie sesión en la consola de administración de AWS y, a continuación, abra la CloudFormation consola en https://console.aw s.amazon.com/cloud formation/. 4. Confirme que se ha implementado correctam ente la pila. Para obtener instrucciones, consulte Revisar la pila en la CloudFormation consola de AWS.	

Tarea	Descripción	Habilidades requeridas
Suscríbase al tema de Amazon SNS.	Para suscribirse al tema de Amazon SNS para recibir notificaciones, haga lo siguiente: 1. En la CloudFormation consola, en el panel de navegación, selecciona Stacks. 2. Elija la pila `genai-knowledge-capture-stack` . 3. Elija la pestaña Salidas. 4. Busque el nombre del tema de Amazon SNS con la clave `SNSTopicName` . 5. Para configurar una dirección de correo electrónico para recibir notificaciones, siga las instrucciones de Suscripción de una dirección de correo electrónico a un tema de Amazon SNS.	AWS general

Pruebe la solución

Tarea	Descripción	Habilidades requeridas
Ejecuta la máquina de estado.	1. Abra la consola de Step Functions. 2. En la página State machines, selecciona	Desarrollador de aplicaciones, AWS general

Tarea	Descripción	Habilidades requeridas
	genai-knowledge-capture-stack-state-machine. 3. Seleccione Iniciar ejecución. 4. (Opcional) En el cuadro Nombre, escriba un nombre para la ejecución. 5. En el área de entrada, introduzca el siguiente objeto JSON mediante la sustitución del texto del marcador de posición, donde: • <Name> es el nombre que desea asignar al documento. • <S3 bucket name> es el nombre del bucket de Amazon S3 que contiene los archivos de audio. • <Folder path> es el nombre del directorio que contiene los archivos de audio. `{ "documentName": "<Name>", "audioFileFolderUri": "s3://<S3 bucket name>/<Folder path>" }` 6. Seleccione Iniciar ejecución.	

Tarea	Descripción	Habilidades requeridas
	7. En la página de detalles de la ejecución, revise los resultados y espere a que se complete la ejecución.	

Limpie todos los recursos de AWS de la solución

Tarea	Descripción	Habilidades requeridas
Elimine los recursos de AWS.	Después de probar la solución, limpie los recursos: 1. Elimine todos los objetos del bucket de S3 y, a continuación, elimine el bucket. Para obtener más información, consulte Eliminación de un bucket. 2. Para clonar el repositorio, ejecute el comando `cdk destroy`.	AWS DevOps, DevOps ingeniero

Recursos relacionados

Documentación de AWS

- Recursos de Amazon Bedrock:
  - Acceso a modelos
  - Parámetros de inferencia para modelos básicos
- Recursos de AWS CDK:
  - Introducción a AWS CDK
  - Utilización de AWS CDK en Python
  - Solución de problemas comunes de AWS CDK

  - Comandos del kit de herramientas
- Recursos de AWS Step Functions:
  - Introducción a AWS Step Functions
  - Solución de problemas
- Creación de funciones de Lambda con Python
- Creador de aplicaciones de IA generativa en AWS

Otros recursos

- LangChain documentación

Genere recomendaciones personalizadas y reclasificadas con Amazon Personalize

Mason Cahill, Matthew Chasse y Tayo Olajide, Amazon Web Services

Resumen

Este patrón le muestra cómo usar Amazon Personalize para generar recomendaciones personalizadas, incluidas las recomendaciones reclasificadas, para sus usuarios en función de la ingesta de datos de interacción de los usuarios en tiempo real por parte de esos usuarios. El escenario de ejemplo utilizado en este patrón se basa en un sitio web de adopción de mascotas que genera recomendaciones para sus usuarios en función de sus interacciones (por ejemplo, qué mascotas visita un usuario). Siguiendo el escenario de ejemplo, aprenderá a utilizar Amazon Kinesis Data Streams para ingerir datos de interacción, AWS Lambda para generar recomendaciones y reordenar las recomendaciones, y Amazon Data Firehose para almacenar los datos en un bucket de Amazon Simple Storage Service (Amazon S3). También aprenderá a usar AWS Step Functions para crear una máquina de estados que administre la versión de la solución (es decir, un modelo entrenado) que genera sus recomendaciones.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa con un AWS Cloud Development Kit (AWS CDK) arrancado.
- Interfaz de la línea de comandos de AWS (AWS CLI) con credenciales configuradas
- Python 3.9

Versiones de producto

- Python 3.9
- CDK de AWS 2.23.0 o posterior
- AWS SDK: 2.7.27 o posterior

Arquitectura

Pila de tecnología

- Amazon Data Firehose
- Amazon Kinesis Data Streams
- Amazon Personalize
- Amazon Simple Storage Service (Amazon S3)
- AWS Cloud Development Kit (AWS CDK)
- Interfaz de la línea de comandos de AWS (AWS CLI)
- AWS Lambda
- AWS Step Functions

Arquitectura de destino

El siguiente diagrama ilustra una canalización para incorporar datos en tiempo real a Amazon Personalize. Luego, la canalización utiliza esos datos para generar recomendaciones personalizadas y reclasificadas para los usuarios.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El flujo de datos de Kinesis ingiere datos de usuarios en tiempo real (por ejemplo, eventos como visitas de mascotas) para que Lambda y Firehose los procesen.
2. Una función de Lambda procesa los registros de flujo de datos de Kinesis y realiza una llamada a la API para añadir la interacción del usuario en el registro a un rastreador de eventos de Amazon Personalize.
3. Una regla basada en el tiempo invoca un equipo de estados de Step Functions y genera nuevas versiones de soluciones para los modelos de recomendación y reclasificación mediante los eventos del rastreador de eventos de Amazon Personalize.
4. El equipo de estados actualiza las campañas de Amazon Personalize para usar la nueva versión de la solución.
5. Lambda cambia el orden de la lista de artículos recomendados mediante la campaña Amazon Personalize de reclasificación.
6. Lambda devuelve la lista de artículos recomendados mediante la campaña de recomendaciones de Amazon Personalize.
7. Firehose guarda los eventos en un bucket de S3 donde se puede acceder a ellos como datos históricos.

Tools (Herramientas)

Herramientas de AWS

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- La Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de la línea de comandos.
- Amazon Data Firehose lo ayuda a entregar datos de streaming en tiempo real a otros servicios de AWS, puntos de conexión HTTP personalizados y puntos de conexión HTTP propiedad de proveedores de servicios externos compatibles.
- Amazon Kinesis Data Streams le ayuda a recopilar y procesar grandes secuencias de registros de datos en tiempo real.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Personalize es un servicio de machine learning (ML) totalmente gestionado que le ayuda a generar recomendaciones de artículos para sus usuarios en función de sus datos.
- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de Lambda y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial.

Otras herramientas

- pytest es un marco de Python para escribir pruebas pequeñas y legibles.
- Python es un lenguaje de programación informático de uso general.

Código

El código de este patrón está disponible en el repositorio GitHub Animal Recommender. Puede usar la CloudFormation plantilla de AWS de este repositorio para implementar los recursos de la solución de ejemplo.

> **Note**
>
> Las versiones de la solución Amazon Personalize, el rastreador de eventos y las campañas están respaldadas por recursos personalizados (dentro de la infraestructura) que amplían CloudFormation los recursos nativos.

Epics

Creación de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree un entorno Python aislado.	Configuración de Mac/Linux 1. Para crear manualmente un entorno virtual, ejecute el comando `$ python3 -m venv .venv` desde su terminal. 2. Una vez finalizado el proceso de inicio, ejecute el comando `$ source .venv/bin/activate` para activar el entorno virtual. Configuración en Windows Para crear manualmente un entorno virtual, ejecute el comando `% .venv\Scripts\activate.bat` desde su terminal.	DevOps ingeniero
Sintetiza la CloudFormation plantilla.	1. Ejecute el comando `$ pip install -r requireme`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`nts.txt` desde su terminal para asegurarse de que dispone de todas las dependencias necesarias. 2. En el shell de la CLI de AWS, configure las siguientes variables de entorno: • `export ACCOUNT_ID=123456789` • `export CDK_DEPLOY_REGION=us-east-1` • `export CDK_ENVIRONMENT=dev` 3. En el archivo `config/{env}.yml` , actualice `vpcId` para que coincida con su ID de nube privada virtual (VPC). 4. Para sintetizar la CloudFormation plantilla de este código, ejecute el `$ cdk synth` comando. **Note** En el paso 2, `CDK_ENVIRONMENT` hace referencia al archivo `config/{env}.yml` .	

Tarea	Descripción	Habilidades requeridas
Implemente recursos y cree infraestructura.	Desde su terminal, ejecute el comando `./deploy.sh` para implementar todos los recursos. Este script instala las dependencias requerida s de Python. Un script de Python crea un bucket de S3 y una clave de AWS Key Management Service (AWS KMS) y, a continuación, agrega los datos de base para las creaciones iniciales del modelo. Por último, el script se ejecuta `cdk deploy` para crear la infraestructura restante. **Note** El entrenamiento del modelo inicial se lleva a cabo durante la creación de la pila. La pila puede tardar hasta dos horas en terminar de crearse.	DevOps ingeniero

Recursos relacionados

- Recomendador de animales () GitHub
- Documentación de referencia de AWS SDK

- Documentación de Boto3
- Optimice las recomendaciones personalizadas para una métrica empresarial de su elección con Amazon Personalize (blog de AWS Machine Learning)

Información adicional

Ejemplos de cargas útiles y respuestas

Función de Lambda de recomendación

Para recuperar las recomendaciones, envíe una solicitud a la función de Lambda de recomendaciones con una carga útil en el siguiente formato:

```
{
  "userId": "3578196281679609099",
  "limit": 6
}
```

El siguiente ejemplo de respuesta contiene una lista de grupos de animales:

```
[{"id": "1-domestic short hair-1-1"},
{"id": "1-domestic short hair-3-3"},
{"id": "1-domestic short hair-3-2"},
{"id": "1-domestic short hair-1-2"},
{"id": "1-domestic short hair-3-1"},
{"id": "2-beagle-3-3"},
```

Si omite el campo `userId`, la función devuelve recomendaciones generales.

Reordenación de la función de Lambda

Para utilizar la reclasificación, envíe una solicitud a la función de Lambda de reclasificación. La carga útil contiene todos `userId` los elementos que se van IDs a reclasificar y sus metadatos. Los siguientes datos de ejemplo utilizan las clases de Oxford Pets para `animal_species_id` (1=gato, 2=perro) y los números enteros del 1 al 5 para `animal_age_id` y `animal_size_id`:

```
{
   "userId":"12345",
   "itemMetadataList":[
      {
```

```
         "itemId":"1",
         "animalMetadata":{
            "animal_species_id":"2",
            "animal_primary_breed_id":"Saint_Bernard",
            "animal_size_id":"3",
            "animal_age_id":"2"
         }
      },
      {
         "itemId":"2",
         "animalMetadata":{
            "animal_species_id":"1",
            "animal_primary_breed_id":"Egyptian_Mau",
            "animal_size_id":"1",
            "animal_age_id":"1"
         }
      },
      {
         "itemId":"3",
         "animalMetadata":{
            "animal_species_id":"2",
            "animal_primary_breed_id":"Saint_Bernard",
            "animal_size_id":"3",
            "animal_age_id":"2"
         }
      }
   ]
}
```

La función Lambda vuelve a clasificar estos artículos y, a continuación, devuelve una lista ordenada que incluye el artículo IDs y la respuesta directa de Amazon Personalize. Esta es una lista ordenada de los grupos de animales en los que se encuentran los artículos y su puntuación. Amazon Personalize utiliza recetas de Personalización por usuario y Clasificación personalizada para incluir una puntuación para cada artículo en las recomendaciones. Estas puntuaciones representan la certeza relativa que tiene Amazon Personalize respecto a qué elemento va a seleccionar el usuario a continuación. Las puntuaciones más altas representan una mayor certeza.

```
{
   "ranking":[
      "1",
      "3",
      "2"
```

```
   ],
   "personalizeResponse":{
      "ResponseMetadata":{
         "RequestId":"a2ec0417-9dcd-4986-8341-a3b3d26cd694",
         "HTTPStatusCode":200,
         "HTTPHeaders":{
            "date":"Thu, 16 Jun 2022 22:23:33 GMT",
            "content-type":"application/json",
            "content-length":"243",
            "connection":"keep-alive",
            "x-amzn-requestid":"a2ec0417-9dcd-4986-8341-a3b3d26cd694"
         },
         "RetryAttempts":0
      },
      "personalizedRanking":[
         {
            "itemId":"2-Saint_Bernard-3-2",
            "score":0.8947961
         },
         {
            "itemId":"1-Siamese-1-1",
            "score":0.105204
         }
      ],
      "recommendationId":"RID-d97c7a87-bd4e-47b5-a89b-ac1d19386aec"
   }
}
```

Carga de Amazon Kinesis

La carga que se va a enviar a Amazon Kinesis tiene el formato siguiente:

```
{
    "Partitionkey": "randomstring",
    "Data": {
        "userId": "12345",
        "sessionId": "sessionId4545454",
        "eventType": "DetailView",
        "animalMetadata": {
            "animal_species_id": "1",
            "animal_primary_breed_id": "Russian_Blue",
            "animal_size_id": "1",
            "animal_age_id": "2"
        },
```

```
        "animal_id": "98765"

    }
}
```

> **Note**
>
> El campo `userId` se elimina para un usuario no autenticado.

Optimice los flujos de trabajo de aprendizaje automático desde el desarrollo local hasta los experimentos escalables mediante el uso de SageMaker IA e Hydra

David Sauerwein, Marco Geiger y Julian Ferdinand Grueber, Amazon Web Services

Resumen

Este patrón proporciona un enfoque unificado para configurar y ejecutar algoritmos de aprendizaje automático (ML) desde las pruebas locales hasta la producción en Amazon SageMaker AI. Este patrón se centra en los algoritmos de ML, pero su enfoque se extiende a la ingeniería de características, la inferencia y canalizaciones completas de ML. Este patrón demuestra la transición del desarrollo de guiones locales a los trabajos de formación en SageMaker IA a través de un ejemplo de caso de uso.

Un flujo de trabajo de ML típico consiste en desarrollar y probar soluciones en una máquina local, ejecutar experimentos a gran escala (por ejemplo, con distintos parámetros) en la nube e implementar la solución aprobada en la nube. A continuación, se debe supervisar y mantener la solución implementada. Sin un enfoque unificado de este flujo de trabajo, los desarrolladores a menudo tienen que refactorizar su código en cada etapa. Si la solución depende de una gran cantidad de parámetros que pueden cambiar en cualquier etapa de este flujo de trabajo, puede resultar cada vez más difícil mantener la organización y la coherencia.

Este patrón resuelve estos desafíos. En primer lugar, elimina la necesidad de refactorizar el código entre entornos al proporcionar un flujo de trabajo unificado que mantiene la coherencia tanto si se ejecuta en máquinas locales, en contenedores o en SageMaker IA. En segundo lugar, simplifica la administración de parámetros mediante el sistema de configuración de Hydra, en el que los parámetros se definen en archivos de configuración independientes que se pueden modificar y combinar fácilmente, con un registro automático de la configuración de cada ejecución. Para más detalles acerca de cómo este patrón resuelve estos desafíos, consulte la sección Información adicional.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS

- Un rol de usuario AWS Identity and Access Management (IAM) para implementar e iniciar los trabajos de formación en SageMaker IA
- AWS Command Line Interface (AWS CLI) versión 2.0 o posterior instalada y configurada
- La versión 1.8 o posterior de Poetry, pero anterior a la versión 2.0, instalada
- Docker instalado
- Python versión 3.10.x

Limitaciones

- Actualmente, el código solo se dirige a los trabajos de formación en SageMaker IA. Extenderlo a los trabajos de procesamiento y a toda la cartera de SageMaker IA es sencillo.
- Para una configuración de SageMaker IA totalmente productiva, es necesario contar con detalles adicionales. Algunos ejemplos podrían ser las claves personalizadas AWS Key Management Service (AWS KMS) para el procesamiento y el almacenamiento, o las configuraciones de red. También puede configurar estas opciones adicionales con Hydra en una subcarpeta específica de la carpeta `config`.
- Algunas Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

En el diagrama siguiente se muestra la arquitectura de la solución.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El científico de datos puede iterar el algoritmo a pequeña escala en un entorno local, ajustar los parámetros y probar el guion de entrenamiento rápidamente sin necesidad de usar Docker o IA. SageMaker (Para más información, consulte la tarea “Run locally for quick testing” en Epics).
2. Una vez satisfecho con el algoritmo, el científico de datos crea y envía la imagen de Docker al repositorio de Amazon Elastic Container Registry (Amazon ECR) denominado `hydra-sm-artifact`. (Para obtener más información, consulta la sección «Ejecutar flujos de trabajo con SageMaker IA» en Epics).

3. El científico de datos inicia trabajos de capacitación en SageMaker IA o trabajos de optimización de hiperparámetros (HPO) mediante scripts de Python. Para los trabajos de entrenamiento habituales, la configuración ajustada se escribe en el bucket de Amazon Simple Storage Service (Amazon S3) denominado `hydra-sample-config`. En el caso de los trabajos de HPO, se aplica el conjunto de configuraciones predeterminadas que se encuentra en la carpeta `config`.
4. El trabajo de entrenamiento de SageMaker IA extrae la imagen de Docker, lee los datos de entrada del bucket `hydra-sample-data` de Amazon S3 y obtiene la configuración del bucket de Amazon S3 `hydra-sample-config` o utiliza la configuración predeterminada. Tras el entrenamiento, el trabajo guarda los datos de salida en el bucket `hydra-sample-data` de Amazon S3.

Automatización y escala

- Para la formación, el reentrenamiento o la inferencia automatizados, puedes integrar el AWS CLI código con servicios como AWS LambdaAWS CodePipeline, o Amazon. EventBridge
- El escalamiento se puede lograr al cambiar las configuraciones (por ejemplo, el tamaño de las instancias) o agregar configuraciones para el entrenamiento distribuido.

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en Cuentas de AWS todo el mundo. Regiones de AWS
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que te ayuda a interactuar Servicios de AWS mediante los comandos de tu consola de línea de comandos. Para este patrón, AWS CLI es útil tanto para la configuración inicial de los recursos como para las pruebas.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon SageMaker AI es un servicio de aprendizaje automático (ML) gestionado que le ayuda a crear y entrenar modelos de aprendizaje automático para luego implementarlos en un entorno hospedado listo para la producción. SageMaker AI Training es un servicio de aprendizaje automático totalmente gestionado dentro de la SageMaker IA que permite el entrenamiento de modelos de aprendizaje automático a escala. La herramienta puede gestionar las demandas

computacionales de los modelos de entrenamiento de manera eficiente, haciendo uso de la escalabilidad incorporada y la integración con otros Servicios de AWS modelos. SageMaker AI Training también es compatible con algoritmos y contenedores personalizados, lo que la hace flexible para una amplia gama de flujos de trabajo de aprendizaje automático.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización del sistema operativo para entregar software en contenedores. Se utilizó en este patrón para garantizar entornos coherentes en varias etapas, desde el desarrollo hasta la implementación, y para empaquetar las dependencias y el código de manera fiable. La contenedorización de Docker permitió un escalado y control de versiones fáciles en el flujo de trabajo.
- Hydra es una herramienta de administración de la configuración que proporciona flexibilidad para gestionar varias configuraciones y una administración dinámica de los recursos. Es fundamental para administrar las configuraciones del entorno, ya que permite una implementación perfecta en entornos distintos. Para más información acerca de Hydra, consulte Información adicional.
- Python es un lenguaje de programación informático de uso general. Se utilizó Python para escribir el código de ML y el flujo de trabajo de implementación.
- Poetry es una herramienta de empaquetado y administración de dependencias de Python.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub configuring-sagemaker-training-jobs-with-hydra.

Prácticas recomendadas

- Elija una función de IAM para implementar e iniciar los trabajos de formación en SageMaker IA que siga el principio de privilegios mínimos y conceda los permisos mínimos necesarios para realizar una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.
- Utilice credenciales temporales para acceder al rol de IAM en la terminal.

Epics

Configuración del entorno

Tarea	Descripción	Habilidades requeridas

Cree y active un entorno virtual.	Para crear y activar el entorno virtual, ejecute los comandos siguientes en la raíz del repositorio:
	`poetry install`
	`poetry shell`
		AWS general

Implemente la infraestructura.	Para implementar la infraestructura mediante CloudFormation, ejecute el siguiente comando: `aws cloudformation deploy --template-file infra/hydra-sagemaker-setup.yaml --stack-name hydra-sagemaker-setup --capabilities CAPABILITY_NAMED_IAM`	General AWS, DevOps ingeniero
Descargue de los datos de muestra.	Para descargar los datos de entrada de openml a su equipo local, ejecute el comando siguiente: `python scripts/download_data.py`	AWS general
Ejecute localmente para hacer pruebas rápidas.	Para ejecutar el código de entrenamiento de manera	Científico de datos

Tarea	Descripción	Habilidades requeridas
	local para la prueba, ejecute el comando siguiente: `python mypackage/train.py data.train_data_path=data/train.csv evaluation.base_dir_path=data` Los registros de todas las ejecuciones se almacenan por tiempo de ejecución en una carpeta llamada `outputs`. Para obtener más información, consulte la sección «Resultados» del GitHub repositorio. También puede hacer varios entrenamientos en paralelo, con parámetros distintos, mediante la funcionalidad `--multirun` . Para más detalles, consulte la documentación de Hydra.	

Ejecute flujos de trabajo en SageMaker IA

Tarea	Descripción	Habilidades requeridas
Establezca las variables de entorno.	Para ejecutar tu trabajo con SageMaker IA, establece las siguientes variables de entorno, proporcionando tu ID Región de AWS y tu Cuenta de AWS ID:	AWS general

Tarea	Descripción	Habilidades requeridas

	`export ECR_REPO_NAME=hydra-sm-artifact`
	`export image_tag=latest`
	`export AWS_REGION="<your_aws_region>" # for instance, us-east-1`
	`export ACCOUNT_ID="<your_account_id>"`
	`export BUCKET_NAME_DATA=hydra-sample-data-$ACCOUNT_ID`
	`export BUCKET_NAME_CONFIG=hydra-sample-config-$ACCOUNT_ID`
	`export AWS_DEFAULT_REGION=$AWS_REGION`
	`export ROLE_ARN=arn:aws:iam::${ACCOUNT_ID}:role/hydra-sample-sagemaker`
	`export INPUT_DATA_S3_PATH=s3://$BUCKET_NAME_DATA/hydra-on-sm/input/`
	`export OUTPUT_DATA_S3_PATH=s3://$BUCKET_NAME_DATA/hydra-on-sm/output/`	

Tarea	Descripción	Habilidades requeridas

Cree y envíe la imagen de Docker.	Para crear la imagen de Docker y enviarla al repositorio de Amazon ECR, ejecute los comandos siguientes:
	`chmod +x scripts/create_and_push_image.sh`
	`scripts/create_and_push_image.sh $ECR_REPO_NAME $image_tag $AWS_REGION $ACCOUNT_ID`
	Esta tarea supone que tiene credenciales válidas en su entorno. La imagen de Docker se envía al repositorio de Amazon ECR especificado en la variable de entorno de la tarea anterior y se utiliza para activar el contenedor de SageMaker IA en el que se ejecutará el trabajo de formación.
		Ingeniero de ML, AWS general

Tarea	Descripción	Habilidades requeridas
Copie los datos de entrada en Amazon S3.	El trabajo de formación en SageMaker IA debe recoger los datos de entrada. Para copiar los datos de entrada al bucket de Amazon S3 para datos, ejecute el comando siguiente: `aws s3 cp data/train.csv "${INPUT_DATA_S3_PATH}train.csv"`	Ingeniero de datos, AWS general

Tarea	Descripción	Habilidades requeridas
Envíe trabajos de formación en SageMaker IA.	Para simplificar la ejecución de sus scripts, especifique los parámetros de configuración predeterminados en el archivo `default.yaml` . Además de garantizar la coherenci a en las ejecuciones, este enfoque también ofrece la flexibilidad de anular fácilment e la configuración predeterm inada según sea necesario. Vea el siguiente ejemplo: `python scripts/s tart_sagemaker_tra ining_job.py sagemaker .role_arn=$ROLE_AR N sagemaker.config_s 3_bucket=$BUCKET_N AME_CONFIG sagemaker .input_data_s3_path= $INPUT_DATA_S3_PATH sagemaker.output_d ata_s3_path=$OUTPU T_DATA_S3_PATH`	AWS general, ingeniero de ML, científico de datos

Tarea	Descripción	Habilidades requeridas
Ejecute el ajuste de hiperpará metros de la SageMaker IA.	Ejecutar el ajuste de los hiperparámetros de la SageMaker IA es similar a enviar un trabajo de entrenami ento SageMaker de IA. Sin embargo, el script de ejecución difiere en algunos aspectos importantes, como puede ver en el archivo start_sagemaker_hpo_job.py. Los hiperparámetros que se van a ajustar deben pasar por la carga útil del boto3, no por un canal hacia el trabajo de entrenamiento. Para iniciar el trabajo de optimización de hiperpará metros (HPO), ejecute los comandos siguientes: `python scripts/s tart_sagemaker_hpo _job.py sagemaker .role_arn=$ROLE_AR N sagemaker.config_s 3_bucket=$BUCKET_N AME_CONFIG sagemaker .input_data_s3_path= $INPUT_DATA_S3_PATH sagemaker.output_d ata_s3_path=$OUTPU T_DATA_S3_PATH`	Científico de datos

Resolución de problemas

Problema	Solución
Token vencido	Exporte AWS credenciales nuevas.
Falta de permisos de IAM	Asegúrese de exportar las credenciales de un rol de IAM que tenga todos los permisos de IAM necesarios para implementar la CloudFormation plantilla e iniciar los trabajos de formación en SageMaker IA.

Recursos relacionados

- Entrena un modelo con Amazon SageMaker AI (AWS documentación)
- What is Hyperparameter Tuning?

Información adicional

Este patrón resuelve los desafíos siguientes:

Coherencia desde el desarrollo local hasta la implementación a escala: con este patrón, los desarrolladores pueden usar el mismo flujo de trabajo, independientemente de si utilizan scripts de Python locales, ejecutan contenedores Docker locales, realizan grandes experimentos con SageMaker IA o despliegan en SageMaker producción con IA. Esta coherencia es importante por los motivos siguientes:

- Iteración más rápida: permite una experimentación local rápida sin necesidad de hacer ajustes importantes al escalar verticalmente.
- Sin necesidad de refactorizar: la transición a experimentos de SageMaker IA de mayor envergadura es sencilla y no requiere una revisión de la configuración existente.
- Mejora continua: desarrollar características nuevas y mejorar de manera continua el algoritmo es sencillo, ya que el código sigue siendo el mismo en todos los entornos.

Administración de la configuración: este patrón utiliza Hydra, una herramienta de administración de la configuración, para ofrecer las ventajas siguientes:

- Los parámetros se definen en los archivos de configuración, independientes del código.
- Los conjuntos de parámetros distintos se pueden intercambiar o combinar con facilidad.
- El seguimiento de los experimentos se simplifica porque la configuración de cada ejecución se registra de manera automática.
- Los experimentos en la nube pueden utilizar la misma estructura de configuración que las ejecuciones locales, lo que garantiza la coherencia.

Con Hydra, puede administrar la configuración de manera eficaz; para ello, habilite las características siguientes:

- Divida las configuraciones: divida las configuraciones de su proyecto en partes más pequeñas y manejables que se puedan modificar de manera independiente. Este enfoque facilita la gestión de proyectos complejos.
- Ajuste los valores predeterminados con facilidad: cambie de manera rápida las configuraciones de referencia para que sea más fácil probar nuevas ideas.
- Alinee las entradas de la CLI y los archivos de configuración: combine las entradas de la línea de comandos con sus archivos de configuración sin problemas. Este enfoque reduce el desorden y la confusión, lo que hace que el proyecto sea más manejable con el tiempo.

Traduce el lenguaje natural a consultas (DSL) para consultas de Elasticsearch OpenSearch y consultas de Elasticsearch

Tabby Ward, Nicholas Switzer y Breanne Warner, Amazon Web Services

Resumen

Este patrón demuestra cómo utilizar modelos de lenguaje grandes (LLMs) para convertir las consultas en lenguaje natural en un lenguaje específico del dominio de consulta (consulta DSL), lo que facilita a los usuarios la interacción con los servicios de búsqueda, como OpenSearch Elasticsearch, sin un conocimiento exhaustivo del lenguaje de consulta. Este recurso es especialmente valioso para los desarrolladores y científicos de datos que quieren mejorar las aplicaciones basadas en búsquedas con funcionalidades de consulta en lenguaje natural y, en última instancia, mejorar la experiencia del usuario y la funcionalidad de búsqueda.

El patrón ilustra las técnicas de ingeniería de peticiones, el perfeccionamiento iterativo y la incorporación de conocimientos especializados, todas fundamentales en la generación de datos sintéticos. Si bien este enfoque se centra principalmente en la conversión de consultas, demuestra de manera implícita el potencial del aumento de datos y la producción escalable de datos sintéticos. Esta base podría ampliarse a tareas de generación de datos sintéticos más exhaustivas, a fin de resaltar el poder de unir las entradas de lenguaje natural no LLMs estructuradas con las salidas estructuradas y específicas de la aplicación.

Esta solución no implica herramientas de migración ni implementación en el sentido tradicional. En cambio, se centra en demostrar una prueba de concepto (PoC) para convertir consultas en lenguaje natural en consultas de DSL mediante el uso de. LLMs

- El patrón utiliza un cuaderno de Jupyter como step-by-step guía para configurar el entorno e implementar la conversión. text-to-query
- Utiliza Amazon Bedrock para acceder LLMs, que es crucial para interpretar el lenguaje natural y generar las consultas adecuadas.
- La solución está diseñada para funcionar con Amazon OpenSearch Service. Puede seguir un proceso similar para Elasticsearch y las consultas generadas podrían adaptarse a los motores de búsqueda similares.

Query DSL es un lenguaje de búsqueda flexible basado en JSON que se utiliza para crear consultas complejas tanto en Elasticsearch como en. OpenSearch Permite especificar consultas en el

parámetro de consulta de las operaciones de búsqueda y admite varios tipos de consultas. Una consulta de DSL incluye consultas hojas y consultas compuestas. Las consultas hoja buscan valores específicos en campos determinados y abarcan consultas de texto completo, por términos, geográficas, de unión, de alcance y especializadas. Las consultas compuestas actúan como contenedores para cláusulas compuestas o de varias hojas y combinan sus resultados o modifican su comportamiento. Query DSL permite la creación de búsquedas sofisticadas, que van desde consultas sencillas que coinciden con todos los requisitos hasta consultas complejas con varias cláusulas que producen resultados muy específicos. Query DSL es especialmente útil para proyectos que requieren funcionalidades de búsqueda avanzadas, una construcción de consultas flexible y estructuras de consulta basadas en JSON.

Para la conversión de DSL, este patrón utiliza técnicas como la generación de mensajes en pocos pasos, las solicitudes del sistema, la salida estructurada, el encadenamiento de solicitudes, el suministro de contexto y las solicitudes específicas para tareas específicas. text-to-query Para definiciones y ejemplos de estas técnicas, consulte la sección Información adicional.

Requisitos previos y limitaciones

Requisitos previos

Para utilizar de manera eficaz el cuaderno de Jupyter para convertir consultas en lenguaje natural en DSL de consultas, necesita lo siguiente:

- Conocimientos de los cuadernos de Jupyter. Comprensión básica de cómo navegar y ejecutar código en un entorno de cuadernos de Jupyter.
- Entorno de Python. Un entorno de Python que funcione, de preferencia Python 3.x, con las bibliotecas necesarias instaladas.
- OpenSearch Elasticsearch o conocimiento. Conocimientos básicos de Elasticsearch o OpenSearch, incluida su arquitectura y cómo realizar consultas.
- Cuenta de AWS. Un activo Cuenta de AWS para acceder a Amazon Bedrock y otros servicios relacionados.
- Bibliotecas y dependencias. Instalación de bibliotecas específicas mencionadas en el cuaderno, por ejemplo, `boto3` para la AWS interacción, y cualquier otra dependencia necesaria para la integración con LLM.
- Acceso a modelos en Amazon Bedrock. Este patrón usa tres Claude LLMs de Anthropic. Abra la consola de Amazon Bedrock y elija Acceso a modelos. En la pantalla siguiente, elija Activar modelos específicos y seleccione estos tres modelos:

  - Claude 3 Sonnet
  - Claude 3.5 Sonnet
  - Claude 3 Haiku
- Políticas de IAM y rol de IAM adecuados. Para ejecutar el cuaderno en una función AWS Identity and Access Management (de IAM) Cuenta de AWS, es necesaria la `SagemakerFullAccess` política, así como la política que se proporciona en la sección de información adicional, a la que puede dar un nombre. `APGtext2querydslpolicy` Esta política incluye la suscripción a los tres modelos de Claude que se indican.

Contar con estos requisitos previos garantiza una experiencia fluida a la hora de trabajar con el portátil e implementar la text-to-query funcionalidad.

Limitaciones

- Estado de la prueba de concepto. Este proyecto pretende principalmente ser una prueba de concepto (PoC). Demuestra el potencial de su uso LLMs para convertir consultas en lenguaje natural en consultas DSL, pero es posible que no esté completamente optimizado o preparado para la producción.
- Limitaciones del modelo:

  Restricciones de la ventana de contexto. Cuando utilice las LLMs que están disponibles en Amazon Bedrock, tenga en cuenta las limitaciones de la ventana de contexto:

  Modelos de Claude (a partir de septiembre de 2024):

  - Claude 3 Opus: 200.000 tokens
  - Claude 3 Sonnet: 200.000 tokens
  - Claude 3 Haiku: 200.000 tokens

  Es posible que otros modelos de Amazon Bedrock tengan tamaños de ventana de contexto distintos. Consulte siempre la documentación más reciente para obtener la información más actualizada.

  Disponibilidad de modelos. La disponibilidad de modelos específicos en Amazon Bedrock puede variar. Asegúrese de tener acceso a los modelos necesarios antes de implementar esta solución.
- Limitaciones adicionales

- Complejidad de la consulta. La eficacia de la conversión del lenguaje natural a DSL de consulta puede variar según la complejidad de la consulta introducida.
- Compatibilidad de versiones. Es posible que el DSL de consulta generado necesite ajustes en función de la versión específica de Elasticsearch o OpenSearch de la que utilice.
- Rendimiento. Este patrón proporciona una implementación de PoC, por lo que la velocidad y precisión de la generación de consultas podrían no ser óptimas la producción a gran escala.
- Costo. Su uso LLMs en Amazon Bedrock conlleva costes. Tenga en cuenta la estructura de precios del modelo que elija. Para obtener más información, consulte Precios de Amazon Bedrock.
- Mantenimiento. Es posible que sea necesario actualizar de manera periódica las peticiones y la selección de modelos para mantenerse al día con los avances de la tecnología de los LLM y los cambios en la sintaxis del DSL de consultas.

Versiones de producto

Esta solución se probó en Amazon OpenSearch Service. Si quiere utilizar Elasticsearch, es posible que tenga que hacer algunos cambios para replicar la funcionalidad exacta de este patrón.

- OpenSearch compatibilidad de versiones. OpenSearch mantiene la compatibilidad con versiones anteriores en las principales versiones. Por ejemplo:
  - OpenSearch Los clientes 1.x son generalmente compatibles con los clústeres OpenSearch 1.x.
  - OpenSearch Los clientes 2.x son generalmente compatibles con OpenSearch los clústeres 2.x.

  Sin embargo, siempre que sea posible, es mejor utilizar la misma versión secundaria para el cliente y para el clúster.
- OpenSearch Compatibilidad con las API. OpenSearch mantiene la compatibilidad de la API con Elasticsearch OSS 7.10.2 para la mayoría de las operaciones. Sin embargo, existen algunas diferencias, sobre todo en las versiones más recientes.
- OpenSearch consideraciones sobre la actualización:
  - No se admiten las versiones de nivel inferior directas. Utilice instantáneas para la reversión si es necesario.
  - Cuando actualice, consulte la matriz de compatibilidad y notas de la versión para ver si hay cambios importantes.

Consideraciones sobre Elasticsearch

- Versión de Elasticsearch. La versión principal de Elasticsearch que utilice es crucial, ya que la sintaxis y las características de las consultas pueden cambiar entre las versiones principales. Actualmente, la última versión estable es Elasticsearch 8.x. Asegúrese de que las consultas sean compatibles con la versión específica de Elasticsearch.
- Versión de la biblioteca de DSL de consultas de Elasticsearch. Si utiliza la biblioteca de Python de DSL de consultas de Elasticsearch, asegúrese de que la versión coincida con la versión de Elasticsearch. Por ejemplo:
  - Para Elasticsearch 8.x, utilice una versión de `elasticsearch-dsl` superior o igual a la versión 8.0.0, pero inferior a la versión 9.0.0.
  - Para Elasticsearch 7.x, utilice una versión de `elasticsearch-dsl` superior o igual a la versión 7.0.0, pero inferior a la versión 8.0.0.
- Versión de la biblioteca del cliente. Ya sea que utilice el cliente oficial de Elasticsearch o un cliente para un lenguaje específico, asegúrese de que sea compatible con la versión de Elasticsearch.
- Versión de Query DSL. Query DSL evoluciona con las versiones de Elasticsearch. Es posible que algunos tipos o parámetros de consulta estén en desuso o se hayan introducido en versiones diferentes.
- Asignación de versión. La manera en que define las asignaciones de los índices y cambia de una versión a otra. Consulte siempre la documentación de asignación de la versión específica de Elasticsearch.
- Versiones de herramientas de análisis. Si utiliza analizadores, tokenizadores u otras herramientas de análisis de texto, su comportamiento o disponibilidad podrían cambiar de una versión a otra.

Arquitectura

Arquitectura de destino

El siguiente diagrama ilustra la arquitectura de este patrón.

donde:

1. Entrada de usuario y petición del sistema con algunos ejemplos de solicitudes de pocos pasos. El proceso comienza con un usuario que proporciona una consulta en lenguaje natural o una solicitud de generación de esquemas.
2. Amazon Bedrock La entrada se envía a Amazon Bedrock, que sirve como interfaz para acceder al LLM de Claude.

3. LLM de Claude 3 Sonnet. Amazon Bedrock utiliza el soneto Claude 3 de la familia Claude 3 LLMs para procesar la entrada. Interpreta y genera el DSL de Elasticsearch o consulta adecuado. OpenSearch Para las solicitudes de esquemas, genera Elasticsearch o mapeos sintéticos. OpenSearch
4. Generación de DSL de consultas. En el caso de las consultas en lenguaje natural, la aplicación toma el resultado del LLM y lo formatea en un DSL válido para consultas de Elasticsearch o Service. OpenSearch
5. Generación de datos sintéticos. La aplicación también utiliza esquemas para crear Elasticsearch sintético o OpenSearch datos para cargarlos en una colección Serverless con fines de prueba. OpenSearch
6. OpenSearch o Elasticsearch. La consulta DSL generada se consulta con una colección OpenSearch Serverless en todos los índices. La salida de JSON contiene los datos relevantes y el número de visitas de los datos que residen en la colección Serverless. OpenSearch

Automatización y escala

El código que se proporciona con este patrón está diseñado estrictamente para fines de PoC. En la lista siguiente se proporcionan algunas sugerencias para automatizar y escalar aún más la solución y pasar el código a producción. Estas mejoras quedan fuera del alcance de este patrón.

- Creación de contenedores:
  - Utilice Docker para la aplicación a fin de garantizar la coherencia entre los diversos entornos.
  - Utilice plataformas de orquestación de contenedores como Amazon Elastic Container Service (Amazon ECS) o Kubernetes para las implementaciones escalables.
- Arquitectura sin servidor:
  - Convierta la funcionalidad principal en AWS Lambda funciones.
  - Utilice Amazon API Gateway para crear RESTful puntos de enlace para la entrada de consultas en lenguaje natural.
- Proceso asíncrono:
  - Implemente Amazon Simple Queue Service (Amazon SQS) para poner en cola las consultas entrantes.
  - Úselo AWS Step Functions para organizar el flujo de trabajo de procesamiento de consultas y generación del DSL de consultas.
- Almacenamiento en caché:

    - Implemente un mecanismo para almacenar las peticiones en la memoria caché.
- Supervisión y registro:
    - Usa Amazon CloudWatch para monitorizar y emitir alertas.
    - Implemente el registro centralizado con Amazon CloudWatch Logs o Amazon OpenSearch Service para el análisis de registros.
- Mejoras de seguridad:
    - Implemente los roles de IAM para el control de acceso específico.
    - Úselo AWS Secrets Manager para almacenar y administrar de forma segura las claves y credenciales de la API.
- Implementación multirregional
    - Considere la posibilidad de implementar la solución en varios Regiones de AWS para mejorar la latencia y la recuperación ante desastres.
    - Utilice Amazon Route 53 para el enrutamiento de solicitudes inteligente.

Al implementar estas sugerencias, puede transformar esta PoC en una solución sólida, escalable y lista para la producción. Recomendamos que pruebe exhaustivamente cada componente y todo el sistema antes de la implementación completa.

Tools (Herramientas)

Herramientas

- Los cuadernos Amazon SageMaker AI son cuadernos Jupyter totalmente gestionados para el desarrollo del aprendizaje automático. Este patrón utiliza las libretas como un entorno interactivo para la exploración de datos, el desarrollo de modelos y la experimentación en Amazon SageMaker AI. Los cuadernos proporcionan una integración perfecta con otras funciones de SageMaker IA y. Servicios de AWS
- Python es un lenguaje de programación informático de uso general. Este patrón utiliza Python como lenguaje principal para implementar la solución.
- Amazon Bedrock es un servicio totalmente gestionado que pone a su disposición modelos básicos de alto rendimiento (FMs) de las principales empresas emergentes de IA y Amazon a través de una API unificada. Amazon Bedrock proporciona acceso al procesamiento LLMs del lenguaje natural. Este patrón utiliza modelos Anthropic Claude 3.

- AWS SDK para Python (Boto3)es un kit de desarrollo de software que le ayuda a integrar su aplicación, biblioteca o script de Python con Servicios de AWS, incluido Amazon Bedrock.
- Amazon OpenSearch Service es un servicio gestionado que le ayuda a implementar, operar y escalar clústeres de OpenSearch servicios en la nube de AWS. Este patrón utiliza OpenSearch Service como sistema de destino para generar el DSL de consultas.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub Prompt Engineering Text-to-QueryDSL Using Claude 3 Models. En el ejemplo se utiliza una aplicación de redes sociales de salud que crea publicaciones para los usuarios y los perfiles de usuario asociados a la aplicación de salud.

Prácticas recomendadas

Al trabajar con esta solución, tenga en cuenta lo siguiente:

- La necesidad de contar con AWS las credenciales y los permisos adecuados para acceder a Amazon Bedrock
- Los posibles costos asociados con el uso Servicios de AWS y LLMs
- La importancia de comprender el DSL de consultas para validar y, posiblemente, modificar las consultas generadas

Epics

Configuración del entorno y preparación de los datos

Tarea	Descripción	Habilidades requeridas
Configure el entorno de desarrollo.	**Note** Para obtener instrucciones detalladas y el código para este y los demás pasos de este patrón, consulte el	Python, pip, AWS SDK

Tarea	Descripción	Habilidades requeridas
	tutorial completo en el GitHub repositorio. 1. Instale los paquetes de Python necesarios, entre estos `boto3`, `numpy`, `awscli`, `opensearch-py` y `requests-aws4auth` mediante pip. 2. Importe los módulos necesarios, tales como `boto3`, `json`, `os`, `opensearch` de `opensearchpy`, `RequestsHttpConnection` de `Opensearchpy`, `bulk` de `opensearchpy.helpers`, `sagemaker`, `time`, `random`, `re` y `AWS4Auth` de `requests_aws4auth`.	
Configura el AWS acceso.	Configure el cliente de Amazon Bedrock y la sesión de SageMaker IA. Recupera el nombre del recurso de Amazon (ARN) del rol de ejecución de SageMaker IA para usarlo más adelante en la creación de la colección OpenSearch Serverless.	IAM, AWS CLI, Amazon Bedrock, Amazon SageMaker

Tarea	Descripción	Habilidades requeridas
Cargue esquemas de aplicaciones de salud.	Lea y analice los esquemas JSON de las publicaciones de salud y perfiles de usuario a partir de archivos predefinidos. Convierta los esquemas en cadenas para utilizarlos más adelante en las peticiones.	DevOps ingeniero, AWS general, Python, JSON

Generación de datos sintéticos

Tarea	Descripción	Habilidades requeridas

Cree un generador de datos basado en LLM.	Implemente la función generate_data() para llamar a la API de Converse de Amazon Bedrock con los modelos Claude 3. Modelo de configuración IDs para Sonnet, Sonnet 3.5 y Haiku:
	`model_id_sonnet3_5 = "anthropic.claude-3-5-sonnet-20240620-v1:0"`
	`model_id_sonnet = "anthropic.claude-3-sonnet-20240229-v1:0"`
	`model_id_haiku = "anthropic.claude-3-haiku-20240307-v1:0"`
		Python, API de Amazon Bedrock, peticiones de LLM

Cree publicaciones de salud sintéticas.	Utilice la función generate_ data() con una petición específica para crear entradas sintéticas de publicaciones de	Python, JSON

Tarea	Descripción	Habilidades requeridas
	salud basadas en el esquema proporcionado. Una llamada a la función tiene un aspecto similar al siguiente: `health_post_data = generate_data(bedrock_rt, model_id_sonnet, system_prompt, message_healthpost, inference_config)`	
Cree perfiles de usuario sintéticos.	Utilice la función generate_data() con una petición específica para crear entradas sintéticas de perfiles de usuario basadas en el esquema proporcionado. Esto es similar a la generación de publicaciones de salud, pero utiliza una petición distinta.	Python, JSON

Configure e ingiera datos OpenSearch

Tarea	Descripción	Habilidades requeridas
Configure una colección OpenSearch sin servidor.	Utilice Boto3 para crear una colección OpenSearch sin servidor con las políticas de cifrado, red y acceso adecuadas. La creación de la colección tiene un aspecto como el siguiente:	OpenSearch Sin servidor, IAM

Tarea	Descripción	Habilidades requeridas
	`collection = aoss_client.create_collection(name=es_name, type='SEARCH')` Para obtener más información sobre OpenSearch Serverless, consulte la documentación.AWS	
Defina los índices OpenSearch .	Cree índices para publicaciones de salud y perfiles de usuario mediante el OpenSearch cliente, en función de las asignaciones de esquemas predefinidas. La creación del índice tiene un aspecto como este: `response_health = oss_client.indices.create(healthpost_index, body=healthpost_body)`	OpenSearch, JSON

Tarea	Descripción	Habilidades requeridas
Cargue datos en OpenSearch.	Ejecuta la función ingest_da ta () para insertar de forma masiva las publicaciones sintéticas sobre salud y los perfiles de usuario en sus índices respectivos. OpenSearch La función utiliza el asistente masivo de `opensearch-py` : `success, failed = bulk(oss_client, actions)`	Python, OpenSearch API, operaciones de datos masivos

Creación y ejecución de consultas

Tarea	Descripción	Habilidades requeridas
Diseñe ejemplos de peticiones con pocos pasos.	Genere consultas de ejemplo y las preguntas correspon dientes en lenguaje natural con los modelos de Claude 3 como ejemplos con pocos pasos para la generación de consultas. La petición del sistema incluye los ejemplos siguientes: `system_prompt_quer y_generation = [{"text": f"""You are an expert query dsl generator. ...`	Petición de LLM, DSL de consultas

Tarea	Descripción	Habilidades requeridas
	`Examples: {example_prompt} ..."""}]`	
Crea un conversor text-to-query DSL.	Implemente la petición del sistema, que incluye esquemas, datos y ejemplos con pocos pasos, para la generación de consultas. Utilice la petición del sistema para convertir las consultas en lenguaje natural en DSL de consultas. Una llamada a la función tiene un aspecto similar al siguiente: `query_response = generate_data(bedrock_rt, model_id, system_prompt_query_generation, query, inference_config)`	Python, API de Amazon Bedrock, peticiones de LLM
Pruebe la consulta DSL activada. OpenSearch	Ejecute la función query_oss () para ejecutar la consulta DSL generada en la colección OpenSearch Serverless y obtener resultados. La función utiliza el método de búsqueda del cliente OpenSearch : `response = oss_client.search(index="_all", body=temp)`	Python, OpenSearch API, consulta DSL

Prueba y evaluación

Tarea	Descripción	Habilidades requeridas
Cree un conjunto de consultas de prueba.	Utilice Claude 3 para generar un conjunto diverso de preguntas de prueba basadas en los datos y esquemas sintéticos: `test_queries = generate_data(bedrock_rt, model_id_sonnet, query_system_prompt, query_prompt, inference_config)`	Peticiones de LLM
Evalúe la precisión de la conversión de DSL de consultas.	Pruebe la consulta DSL generada mediante la ejecución de consultas OpenSearch y el análisis de los resultados devueltos para comprobar su relevancia y precisión. Esto implica ejecutar la consulta e inspeccionar los resultados: `output = query_oss(response1) print("Response after running query against Opensearch") print(output)`	Python, análisis de datos, DSL de consultas
Modelos Claude 3 de referencia.	Compare el rendimiento de los distintos modelos de Claude 3 (Haiku, Sonnet, Sonnet 3.5) para la generación de consultas en términos	Python, análisis comparativo de rendimiento

Tarea	Descripción	Habilidades requeridas
	de precisión y latencia. Para comparar, cambie `model_id` cuando llame a generate_data() y mide el tiempo de ejecución.	

Limpieza y documentación

Tarea	Descripción	Habilidades requeridas
Desarrolle un proceso de limpieza.	Elimine todos los índices de la colección OpenSearch Serverless después de usarlos.	Python, SDK de AWS, OpenSearch API

Recursos relacionados

- Consulta DSL (OpenSearch documentación)
- Documentación OpenSearch de Amazon Service
- OpenSearch Colecciones sin servidor
- Documentación de Amazon Bedrock
- Documentación de Amazon SageMaker AI
- AWS SDK para Python (Boto3) documentación

Información adicional

Política de IAM

Esta es la política `APGtext2querydslpolicy` para el rol de IAM que se utiliza en este patrón:

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Effect": "Allow",
```

```
      "Action": [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::sagemaker-*",
        "arn:aws:s3:::sagemaker-*/*"
      ]
    },
    { "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    { "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": [
        "aoss:*"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": [
        "iam:PassRole",
        "sagemaker:*"
      ],
```

```
      "Resource": [
        "arn:aws:iam::*:role/*", "*"
      ],
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "sagemaker.amazonaws.com"
          }
      }
    },
    { "Effect": "Allow",
      "Action": [
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "codecommit:ListRepositories"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": [
        "aws-marketplace:Subscribe"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws-marketplace:ProductId": [
            "prod-6dw3qvchef7zy",
            "prod-m5ilt4siql27k",
            "prod-ozonys2hmmpeu"
          ]
        }
      }
    },
    { "Effect": "Allow",
      "Action": [
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": "iam:*",
      "Resource": "*"
```

```
    }
  ]
}
```

Técnicas de peticiones con modelos Anthropic Claude 3

Este patrón muestra las siguientes técnicas de solicitud para la conversión text-to-query DSL utilizando los modelos Claude 3.

- Petición con pocos pasos: las peticiones con pocos pasos es una técnica eficiente para mejorar el rendimiento de los modelos de Claude 3 en Amazon Bedrock. Este enfoque implica proporcionar al modelo un pequeño número de ejemplos que demuestren el input/output comportamiento deseado antes de pedirle que realice una tarea similar. Al utilizar los modelos de Claude 3 en Amazon Bedrock, las peticiones con pocos pasos pueden resultar muy eficaces para las tareas que requieren un formato específico, patrones de razonamiento o conocimientos del dominio. Para implementar esta técnica, en general, se estructura la petición con dos componentes principales: la sección de ejemplos y la consulta propiamente dicha. La sección de ejemplos contiene uno o más input/output pares que ilustran la tarea y la sección de consultas presenta la nueva entrada para la que desea obtener una respuesta. Este método ayuda a Claude 3 a entender el contexto y el formato de salida esperado y, a menudo, da como resultado una respuesta más precisa y coherente.

  Ejemplo:

  ```
  "query": {
    "bool": {
      "must": [
        {"match": {"post_type": "recipe"}},
        {"range": {"likes_count": {"gte": 100}}},
        {"exists": {"field": "media_urls"}}
      ]
    }
  }
  Question: Find all recipe posts that have at least 100 likes and include media URLs.
  ```

- Peticiones del sistema: además de las peticiones con pocos pasos, los modelos de Claude 3 de Amazon Bedrock también admiten el uso de peticiones del sistema. Las peticiones del sistema son una manera de proporcionar un contexto general, instrucciones o directrices al modelo antes de presentarlo con entradas específicas del usuario. Son muy útiles para definir el tono,

establecer el papel del modelo o establecer las limitaciones de toda la conversación. Para utilizar una petición del sistema con Claude 3 en Amazon Bedrock, debe incluirlo en el parámetro `system` de su solicitud de API. Esto es independiente de los mensajes de usuario y se aplica a toda la interacción. Las peticiones detalladas del sistema se utilizan para establecer el contexto y proporcionar pautas para el modelo.

Ejemplo:

```
You are an expert query dsl generator. Your task is to take an input question and
 generate a query dsl to answer the question. Use the schemas and data below to
 generate the query.

Schemas: [schema details]
Data: [sample data]
Guidelines:
- Ensure the generated query adheres to DSL query syntax
- Do not create new mappings or other items that aren't included in the provided
 schemas.
```

- Salida estructurada: puede indicar al modelo que proporcione la salida en formatos específicos, como JSON o en etiquetas XML.

  Ejemplo:

  ```
  Put the query in json tags
  ```

- Encadenamiento de peticiones: el cuaderno utiliza el resultado de una llamada al LLM como entrada para otra, por ejemplo, utiliza los datos sintéticos generados para crear preguntas de ejemplo.
- Aprovisionamiento de contexto: en las peticiones se proporciona el contexto correspondiente, como los esquemas y los datos de muestra.

  Ejemplo:

  ```
  Schemas: [schema details]
  Data: [sample data]
  ```

- Peticiones específicas para cada tarea: se diseñan peticiones distintas para tareas específicas, como generar datos sintéticos, crear preguntas de ejemplo y convertir consultas en lenguaje natural en DSL de consultas.

Ejemplo de generación de preguntas de prueba:

```
Your task is to generate 5 example questions users can ask the health app based on
 provided schemas and data. Only include the questions generated in the response.
```

Uso de Amazon Q Developer como asistente de codificación para aumentar la productividad

Ram Kandaswamy, Amazon Web Services

Resumen

Este patrón utiliza un tic-tac-toe juego para demostrar cómo puedes aplicar Amazon Q Developer en una variedad de tareas de desarrollo. Genera código para un tic-tac-toe juego como una aplicación de una sola página (SPA), mejora su interfaz de usuario y crea scripts para implementar la AWS aplicación.

Amazon Q Developer funciona como un asistente de codificación para ayudar a acelerar los flujos de trabajo de desarrollo de software y mejorar la productividad para desarrolladores y para no desarrolladores. Independientemente de sus conocimientos técnicos, le permite crear arquitecturas y diseñar soluciones para problemas empresariales, a reforzar su entorno de trabajo, a implementar características nuevas y a generar casos de prueba para su validación. Utiliza instrucciones en lenguaje natural y funcionalidades de IA para garantizar un código coherente y de alta calidad y mitigar los desafíos de codificación, independientemente de sus habilidades de programación.

La ventaja principal de Amazon Q Developer es su capacidad para quitarle de encima las tareas de codificación repetitivas. Cuando utiliza la anotación `@workspace`, Amazon Q Developer ingiere e indexa todos los archivos de código, las configuraciones y la estructura del proyecto en su entorno de desarrollo integrado (IDE) y proporciona respuestas personalizadas para que se centre en la resolución creativa de problemas. Puede dedicar más tiempo a diseñar soluciones innovadoras y a mejorar la experiencia del usuario. Si no tiene conocimientos técnicos, puede utilizar Amazon Q Developer para agilizar los flujos de trabajo y colaborar de manera más eficaz con el equipo de desarrollo. La característica de explicación del código de Amazon Q Developer ofrece instrucciones y resúmenes detallados para que pueda navegar por bases de código complejas.

Además, Amazon Q Developer ofrece un enfoque independiente del lenguaje que ayuda a los desarrolladores de nivel medio y medio a ampliar sus habilidades. Puede concentrarse en los conceptos básicos y la lógica empresarial en lugar de centrarse en la sintaxis específica del lenguaje. Esto reduce la curva de aprendizaje al cambiar de tecnología.

Requisitos previos y limitaciones

Requisitos previos

- IDE (por ejemplo, WebStorm o Visual Studio Code) con el complemento Amazon Q Developer instalado. Para obtener instrucciones, consulte Installing the Amazon Q Developer extension or plugin in your IDE en la documentación de Amazon Q Developer.
- Una Cuenta de AWS configuración activa con Amazon Q Developer. Para obtener instrucciones, consulte Getting started en la documentación de Amazon Q Developer.
- npm instalado. Para obtener instrucciones, consulte la documentación de npm. Este patrón se probó con la versión 10.8 de npm.
- AWS Command Line Interface (AWS CLI) instalado. Para obtener instrucciones, consulte la documentación de AWS CLI.

Limitaciones

- Amazon Q Developer solo puede hacer una tarea de desarrollo a la vez.
- Algunas Servicios de AWS no están disponibles en todas Regiones de AWS. Para conocer la disponibilidad de las regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Tools (Herramientas)

- Este patrón requiere un IDE como Visual Studio Code o WebStorm. Para obtener una lista de los compatibles IDEs, consulte la documentación para desarrolladores de Amazon Q.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar Servicios de AWS mediante los comandos de su shell de línea de comandos.

Prácticas recomendadas

Consulte las prácticas recomendadas de codificación con Amazon Q Developer en la Guía AWS prescriptiva. Además:

- Al enviar peticiones a Amazon Q Developer, asegúrese de que las instrucciones sean claras e inequívocas. Agregue fragmentos de código y anotaciones, por ejemplo, `@workspace` a la petición para proporcionar más contexto a las peticiones.
- Incluya las bibliotecas pertinentes e impórtelas para evitar conflictos o conjeturas incorrectas por parte del sistema.

- Si el código generado no es exacto o no es el esperado, utilice la opción Enviar comentarios y regenerar. Intente dividir las peticiones en instrucciones más pequeñas.

Epics

Configuración del entorno de trabajo

Tarea	Descripción	Habilidades requeridas
Cree un nuevo proyecto de .	Para crear un proyecto nuevo en el entorno de trabajo, ejecute el comando siguiente y acepte la configuración predeterminada para todas las preguntas: `npx create-next-app@latest`	Desarrollador de aplicaciones, programador, desarrollador de software
Pruebe la aplicación base.	Ejecute el comando siguiente y confirme que la aplicación base cargó de manera correcta en el navegador: `npm run dev`	Desarrollador de aplicaciones, programador, desarrollador de software
Limpie el código base.	Vaya al archivo `page.tsx` de la carpeta `src/app` y elimine el contenido predeterminado para obtener una página en blanco. Una vez eliminado, el archivo debe tener el aspecto siguiente: `export default function Home() { return (<div></div>`	Desarrollador de aplicaciones, programador, desarrollador de software

Tarea	Descripción	Habilidades requeridas
	`);` `}`	

Usa Amazon Q Developer para diseñar un proyecto de tic-tac-toe juego

Tarea	Descripción	Habilidades requeridas
Obtenga información general de los pasos.	1. En el IDE, abra el proyecto y elija el icono de Amazon Q para abrir el panel de chat. 2. En el panel de chat de Amazon Q Developer, solicite información general sobre cómo crear una aplicación de una sola página (SPA). Por ejemplo: `I would like to create a single-page application involving Next.js React framework for tic-tac-toe game. What are the steps?`	Desarrollador de aplicaciones, programador, desarrollador de software
Genera código para tic-tac-toe.	En el panel de chat, inicie una tarea de desarrollo mediante el comando `/dev` seguido de la descripción de la tarea. Por ejemplo: `/dev Create a React-based single-page application written in TypeScript for a`	Desarrollador de aplicaciones, programador, desarrollador de software

Tarea	Descripción	Habilidades requeridas

	`tic-tac-toe game with the following specifications:`
	`1. Design an aesthetically pleasing interface with the game grid centered vertically and horizontally on the page.`
	`2. Include a heading and clear instructions on how to play the game.`
	`3. Implement color-coding for X and O marks to distinguish them easily.`
	
	Amazon Q Developer genera código según sus instrucciones.	

Inspeccione y acepte el código generado.	Inspeccione visualmente el código y elija Aceptar código para reemplazar automáticamente el archivo `page.tsx`. Si tiene problemas, elija Enviar comentarios y regenerar y describa el problema que encontró.	Desarrollador de aplicaciones, programador, desarrollador de software

Tarea	Descripción	Habilidades requeridas
Corrija los errores de linting.	El tic-tac-toe juego de ejemplo incluye una cuadrícula. El código que genera Amazon Q Developer podría utilizar el tipo predeterminado `any`. Para agregar seguridad tipográfica, haga una petición a Amazon Q Developer de la manera siguiente: `/dev Ensure proper TypeScript typing for the onSquare Click event handler to resolve any 'any' type issues.`	Desarrollador de aplicaciones, programador, desarrollador de software

Tarea	Descripción	Habilidades requeridas

Agregue atractivo visual.	Puede dividir el requisito original en fragmentos más pequeños. Por ejemplo, puede mejorar la IU del juego con las peticiones siguientes en las tareas de desarrollo. Esta petición mejora los estilos de Cascading Style Sheets (CSS) y exporta la aplicación para su implementación.
	
	`/dev Debug and fix any CSS issues to correctly display the game grid and overall layout.`
	
	`Simplify the code by removing game history functionality and related components.`
	
	`Implement static file export to an 'out' directory for easy deployment. The solution should be fully functional, visually appealing, and free of typing errors or layout issues.`
		Desarrollador de aplicaciones, programador, desarrollador de software

Tarea	Descripción	Habilidades requeridas

Vuelva a probar.	1. Ahora que completó el ciclo de vida de desarrollo, pruebe el código para confirmar que funciona según lo previsto. Para ejecutar la aplicación localmente, utilice el comando:
	`npm run dev`
	2. Si la aplicación funciona según lo previsto, utilice el comando `build` para exportar toda la aplicación a la carpeta de salida como preparación para la implementación:
	`npm run build`
		Desarrollador de aplicaciones, programador, desarrollador de software

Implemente la aplicación en el Nube de AWS

Tarea	Descripción	Habilidades requeridas
Cree carpetas y archivos para su implementación.	En el proyecto del entorno de trabajo, cree una carpeta de implementación con dos archivos en su interior: `pushtos3.sh` y `cloudformation.yml` `mkdir deployment && cd deployment`	Desarrollador de aplicaciones, programador, desarrollador de software

Tarea	Descripción	Habilidades requeridas
	`touch pushtos3.sh && chmod +x pushtos3.sh` `touch cloudformation.yml`	

Tarea	Descripción	Habilidades requeridas
Genere código de automatización.	1. En el panel de chat de Amazon Q Developer, proporcione la petición siguiente: `/dev Generate a Cloudformation template that creates two resources: tictactoe artifact bucket and CloudFront. CloudFront should be configured with this bucket as origin. Add cache policy appropriate for Amazon S3 and default root object as index.html. Ensure that origin access control is used and no public bucket is created. Output all the resources and their ARNs.`  2. Revise y acepte el código generado. El `cloudformation.yml` archivo que creó anteriormente ahora debería rellenarse con un CloudFormation script que cree los recursos para el Nube de AWS.	Administrador de AWS, AWS DevOps, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Genere el contenido del script.	Para crear un script de implementación, utilice la petición siguiente: `/dev Modify the pushtos3 shell script so that it can use AWS CLI commands to create a CloudFormation stack named tictactoe-stack if it does not exist already, and use cloudformation.yml as the source template. Wait for the stack to complete and sync the contents from the out folder to the S3 bucket. Perform invalidation of the CloudFront origin.`	Desarrollador de aplicaciones, programador, desarrollador de software
Implemente la aplicación en la Nube de AWS.	1. Configure el entorno de trabajo con AWS credencia les válidas. 2. Ejecute el script de shell para implementar el tic-tac-toe juego completamente funcional en Nube de AWS.	Administrador de AWS DevOps, arquitecto de nube, desarrollador de aplicaciones

Resolución de problemas

Problema	Solución

La creación no crea una aplicación de una sola página ni la exporta a la carpeta de salida.	Mire el contenido del archivo `next.config.mjs` :
	
	Si el código tiene la configuración siguiente de manera predeterminada:
	
	`const nextConfig = {};`
	
	modifíquelo de la manera siguiente:
	
	`const nextConfig = {`
	`  output: 'export',`
	`  distDir: 'out',`
	`};`

Recursos relacionados

- Creating a new React project (documetación de React)
- Descripción general para desarrolladores de Amazon Q (AWS documentación)
- Prácticas recomendadas para desarrolladores de Amazon Q (guía AWS prescriptiva)
- Instalación, configuración y uso de Amazon Q Developer con JetBrains IDEs (YouTube vídeo)
- Instalación de Amazon Q para la línea de comandos (AWS documentación)

Utilice el SageMaker procesamiento para la ingeniería de características distribuidas de conjuntos de datos de aprendizaje automático a escala de terabytes

Chris Boomhower, Amazon Web Services

Resumen

Muchos conjuntos de datos a escala de terabytes o más grandes suelen constar de una estructura jerárquica de carpetas y, en ocasiones, los archivos del conjunto de datos comparten interdependencias. Por este motivo, los ingenieros de machine learning (ML) y los científicos de datos deben tomar decisiones de diseño bien pensadas a fin de preparar dichos datos para el entrenamiento y la inferencia de modelos. Este patrón demuestra cómo puede utilizar técnicas manuales de macrofragmentación y microfragmentación en combinación con Amazon SageMaker Processing y la paralelización de CPU virtual (vCPU) para escalar de manera eficiente los procesos de ingeniería de características para conjuntos de datos de aprendizaje automático de big data complicados.

Este patrón define la macrofragmentación como la división de los directorios de datos en varias máquinas para su procesamiento, y la microfragmentación como la división de los datos de cada máquina en varios subprocesos de procesamiento. El patrón demuestra estas técnicas mediante el uso de Amazon SageMaker con ejemplos de registros de formas de onda de series temporales del conjunto de datos PhysioNet MIMIC-III. Al implementar las técnicas en este patrón, puede minimizar el tiempo y los costos de procesamiento de la ingeniería de características y, al mismo tiempo, maximizar la utilización de los recursos y la eficiencia del rendimiento. Estas optimizaciones se basan en el SageMaker procesamiento distribuido en las instancias de Amazon Elastic Compute Cloud (Amazon EC2) y en v CPUs para conjuntos de datos grandes y similares, independientemente del tipo de datos.

Requisitos previos y limitaciones

Requisitos previos

- Acceda a instancias de SageMaker notebook o a SageMaker Studio, si desea implementar este patrón en su propio conjunto de datos. Si es la primera vez que utiliza Amazon SageMaker , consulte Comenzar con Amazon SageMaker en la documentación de AWS.

- SageMaker Studio, si quiere implementar este patrón con los datos de muestra del PhysioNet MIMIC-III.
- El patrón usa SageMaker Processing, pero no requiere experiencia en la ejecución SageMaker de trabajos de Processing.

Limitaciones

- Este patrón se adapta bien a los conjuntos de datos de machine learning que incluyen archivos interdependientes. Estas interdependencias son las que más se benefician de la fragmentación manual de macros y de la ejecución en paralelo de varios trabajos de procesamiento de una sola instancia SageMaker . Para los conjuntos de datos en los que no existen dichas interdependencias, la `ShardedByS3Key` función de SageMaker procesamiento podría ser una mejor alternativa a la macrofragmentación, ya que envía los datos fragmentados a varias instancias administradas por el mismo trabajo de procesamiento. Sin embargo, puede implementar la estrategia de microfragmentación de este patrón en ambos escenarios para aprovechar al máximo la instancia v. CPUs

Versiones de producto

- Amazon SageMaker Python SDK versión 2

Arquitectura

Pila de tecnología de destino

- Amazon Simple Storage Service (Amazon S3)
- Amazon SageMaker

Arquitectura de destino

Macrofragmentación e instancias distribuidas EC2

Los 10 procesos paralelos representados en esta arquitectura reflejan la estructura del conjunto de datos MIMIC-III. (Los procesos se representan mediante elipses para simplificar el diagrama). Cuando se utiliza la macrofragmentación manual, se aplica una arquitectura similar a cualquier conjunto de datos. En el caso de MIMIC-III, puede aprovechar la estructura sin procesar del conjunto de datos procesando la carpeta de cada grupo de pacientes por separado, con un esfuerzo mínimo.

En el siguiente diagrama, el bloque de grupos de registros aparece a la izquierda (1). Dada la naturaleza distribuida de los datos, tiene sentido dividirlos por grupo de pacientes.

Sin embargo, la fragmentación manual por grupo de pacientes significa que se requiere un trabajo de procesamiento independiente para cada carpeta del grupo de pacientes, como puede ver en la sección central del diagrama (2), en lugar de un solo trabajo de procesamiento con varias instancias. EC2 Como los datos de MIMIC-III incluyen tanto archivos de forma de onda binarios como archivos de encabezados basados en texto coincidentes, y existe una dependencia obligatoria de la biblioteca wfdb para la extracción de datos binarios, todos los registros de un paciente específico deben estar disponibles en la misma instancia. La única forma de asegurarse de que el archivo de cabecera asociado a cada archivo de forma de onda binaria también esté presente es implementar la fragmentación manual para ejecutar cada fragmento dentro de su propio trabajo de procesamiento y especificar `s3_data_distribution_type='FullyReplicated'` cuándo se define la entrada del trabajo de procesamiento. Como alternativa, si todos los datos estuvieran disponibles en un único directorio y no existieran dependencias entre los archivos, una opción más adecuada sería lanzar un único trabajo de procesamiento con varias EC2 instancias especificadass3_data_distribution_type='ShardedByS3Key'. Si `ShardedByS3Key` se especifica el tipo de distribución de datos de Amazon S3, se SageMaker gestionará automáticamente la fragmentación de datos en todas las instancias.

Lanzar un trabajo de procesamiento para cada carpeta es una forma rentable de preprocesar los datos, ya que la ejecución simultánea de varias instancias ahorra tiempo. Para ahorrar costos y tiempo adicionales, puede utilizar la microfragmentación en cada trabajo de procesamiento.

Microsharding y parallel v CPUs

Dentro de cada trabajo de procesamiento, los datos agrupados se dividen aún más para maximizar el uso de todos los v disponibles CPUs en la instancia SageMaker totalmente administrada EC2 . Los bloques de la sección central del diagrama (2) muestran lo que ocurre en cada trabajo de procesamiento principal. El contenido de las carpetas de registros de pacientes se aplana y se divide en partes iguales en función del número de v disponibles CPUs en la instancia. Una vez dividido el contenido de la carpeta, el conjunto de archivos de tamaño uniforme se distribuye por todos los archivos v CPUs para su procesamiento. Cuando se completa el procesamiento, los resultados de cada vCPU se combinan en un único archivo de datos para cada trabajo de procesamiento.

En el código adjunto, estos conceptos se representan en la siguiente sección del archivo `src/feature-engineering-pass1/preprocessing.py`.

```
def chunks(lst, n):
    """
    Yield successive n-sized chunks from lst.

    :param lst: list of elements to be divided
    :param n: number of elements per chunk
    :type lst: list
    :type n: int
    :return: generator comprising evenly sized chunks
    :rtype: class 'generator'
    """
    for i in range(0, len(lst), n):
        yield lst[i:i + n]


# Generate list of data files on machine
data_dir = input_dir
d_subs = next(os.walk(os.path.join(data_dir, '.')))[1]
file_list = []
for ds in d_subs:
    file_list.extend(os.listdir(os.path.join(data_dir, ds, '.')))
dat_list = [os.path.join(re.split('_|\.', f)[0].replace('n', ''), f[:-4]) for f in
 file_list if f[-4:] == '.dat']

# Split list of files into sub-lists
cpu_count = multiprocessing.cpu_count()
splits = int(len(dat_list) / cpu_count)
if splits == 0: splits = 1
dat_chunks = list(chunks(dat_list, splits))

# Parallelize processing of sub-lists across CPUs
ws_df_list = Parallel(n_jobs=-1, verbose=0)(delayed(run_process)(dc) for dc in
 dat_chunks)

# Compile and pickle patient group dataframe
ws_df_group = pd.concat(ws_df_list)
ws_df_group = ws_df_group.reset_index().rename(columns={'index': 'signal'})
ws_df_group.to_json(os.path.join(output_dir, group_data_out))
```

Una función, `chunks`, se define primero para consumir una lista dada dividiéndola en trozos de longitud de tamaño uniforme `n` y devolviendo estos resultados como un generador. A continuación, los datos se agrupan en las carpetas de los pacientes mediante la compilación de una lista de todos

los archivos de forma de onda binaria presentes. Una vez hecho esto, se obtiene el número de v CPUs disponible en la EC2 instancia. La lista de archivos de formas de onda binarias se divide uniformemente entre estas v CPUs mediante una llamada `ychunks`, a continuación, cada sublista de formas de onda se procesa en su propia vCPU mediante la clase Parallel de joblib. El trabajo de procesamiento combina automáticamente los resultados en una sola lista de marcos de datos, que SageMaker luego los procesa más antes de escribirlos en Amazon S3 al finalizar el trabajo. En este ejemplo, los trabajos de procesamiento escriben 10 archivos en Amazon S3 (uno para cada trabajo).

Cuando se hayan completado todos los trabajos de procesamiento iniciales, un trabajo de procesamiento secundario, que se muestra en el bloque a la derecha del diagrama (3), combina los archivos de salida generados por cada trabajo de procesamiento principal y escribe el resultado combinado en Amazon S3 (4).

Tools (Herramientas)

Herramientas

- Python: el código de ejemplo utilizado para este patrón es Python (versión 3).
- SageMaker Studio: Amazon SageMaker Studio es un entorno de desarrollo integrado (IDE) basado en la web para el aprendizaje automático que le permite crear, entrenar, depurar, implementar y supervisar sus modelos de aprendizaje automático. Los trabajos de SageMaker procesamiento se ejecutan con los cuadernos de Jupyter incluidos en Studio. SageMaker
- SageMaker Procesamiento: Amazon SageMaker Processing proporciona una forma simplificada de ejecutar sus cargas de trabajo de procesamiento de datos. En este patrón, el código de ingeniería de funciones se implementa a escala mediante tareas SageMaker de procesamiento.

Código

El archivo .zip adjunto proporciona el código completo de este patrón. En la siguiente sección se describen los pasos para crear la arquitectura para este patrón. Cada paso se ilustra con un ejemplo de código del archivo adjunto.

Epics

Configura tu entorno de SageMaker estudio

Tarea	Descripción	Habilidades requeridas
Accede a Amazon SageMaker Studio.	Inscríbase en SageMaker Studio en su cuenta de AWS siguiendo las instrucciones que se proporcionan en la SageMaker documentación de Amazon.	Científico de datos, ingeniero de machine learning
Instale la utilidad wget.	Instala wget si has incorpora do una nueva configuración de SageMaker Studio o si nunca has utilizado estas utilidades en SageMaker Studio. Para instalarlo, abre una ventana de terminal en la consola de SageMaker Studio y ejecuta el siguiente comando: `sudo yum install wget`	Científico de datos, ingeniero de machine learning
Descargue y descomprima el código de muestra.	Descargue el archivo `attachments.zip` en la sección Adjuntos. En una ventana de terminal, navegue hasta la carpeta en la que descargó el archivo y extraiga su contenido: `unzip attachment.zip`	Científico de datos, ingeniero de machine learning

Tarea	Descripción	Habilidades requeridas
	Desplácese hasta la ubicación donde descargó el archivo .zip y extraiga el contenido del archivo `Scaled-Processing.zip` . `unzip Scaled-Processing.zip`	
Descargue el conjunto de datos de muestra de physionet.org y cárguelo en Amazon S3.	Ejecute el cuaderno de Jupyter `get_data.ipynb` dentro de la carpeta que contiene los archivos `Scaled-Processing` . Este bloc de notas descarga un conjunto de datos MIMIC-III de muestra de physionet.org y lo carga en el bucket de sesión SageMaker de Studio en Amazon S3.	Científico de datos, ingeniero de machine learning

Configuración del primer script de preprocesamiento

Tarea	Descripción	Habilidades requeridas
Aplane la jerarquía de archivos en todos los subdirectorios.	En conjuntos de datos grandes, como MIMIC-III, los archivos suelen distribuirse en varios subdirectorios, incluso dentro de un grupo principal lógico. El script debe estar configurado para aplanar todos los archivos del grupo en todos los subdirect	Científico de datos, ingeniero de machine learning

Tarea	Descripción	Habilidades requeridas

	orios, como se muestra en el siguiente código.
	
	`# Generate list of .dat files on machine`
	`data_dir = input_dir`
	`d_subs = next(os.walk(os.path.join(data_dir, '.')))[1]`
	`file_list = []`
	`for ds in d_subs:`
	`  file_list.extend(os.listdir(os.path.join(data_dir, ds, '.')))`
	`dat_list = [os.path.join(re.split('_|\.', f)[0].replace('n', ''), f[:-4]) for f in file_list if f[-4:] == '.dat']`
	
	Note
	Los fragmentos de código de ejemplo de esta epic provienen del archivo `src/feature-engineering-pass1/preprocessing.py` que se proporciona en el archivo adjunto.	

Tarea	Descripción	Habilidades requeridas

Divida los archivos en subgrupos según el recuento de vCPU.	Los archivos deben dividirse en subgrupos o fragmentos de tamaño uniforme, según el número de v CPUs presentes en la instancia que ejecuta el script. Para este paso, puede implementar código similar al siguiente.
	`# Split list of files into sub-lists`
	`cpu_count = multiprocessing.cpu_count()`
	`splits = int(len(dat_list) / cpu_count)`
	`if splits == 0: splits = 1`
	`dat_chunks = list(chunks(dat_list, splits))`
		Científico de datos, ingeniero de machine learning

Paralelice el procesamiento de los subgrupos entre v. CPUs	La lógica del script debe configurarse para procesar todos los subgrupos en paralelo. Para ello, utilice la clase `Parallel` y el método `delayed` de la biblioteca Joblib de la siguiente manera.
	`# Parallelize processing of sub-lists across CPUs`
	`ws_df_list = Parallel(n_jobs=-1, verbose=0)(delayed(run_process)(dc) for dc in dat_chunks)`
		Científico de datos, ingeniero de machine learning

Tarea	Descripción	Habilidades requeridas

Guarde la salida de un solo grupo de archivos en Amazon S3.	Cuando se complete el procesamiento de la vCPU paralela, los resultados de cada vCPU deben combinarse y cargarse en la ruta del bucket de S3 del grupo de archivos. Para este paso, puede utilizar código similar al siguiente.
	`# Compile and pickle patient group dataframe`
	`ws_df_group = pd.concat(ws_df_list)`
	`ws_df_group = ws_df_group.reset_index().rename(columns={'index': 'signal'})`
	`ws_df_group.to_json(os.path.join(output_dir, group_data_out))`
		Científico de datos, ingeniero de machine learning

Configuración del segundo script de preprocesamiento

Tarea	Descripción	Habilidades requeridas
Combine los archivos de datos generados en todos los trabajos de procesamiento en los que se ejecutó el primer script.	El script anterior genera un único archivo para cada trabajo de SageMaker procesamiento que procesa un grupo de archivos del conjunto de datos. A continuación, debe combinar estos archivos de salida en	Científico de datos, ingeniero de machine learning

Tarea	Descripción	Habilidades requeridas

	un único objeto y escribir un único conjunto de datos de salida en Amazon S3. Esto se demuestra en el archivo `src/feature-engineering-pass1p5/preprocessing.py` , que se proporciona en el archivo adjunto, de la siguiente manera.
	
	`def write_parquet(wavs_df, path):`
	`"""`
	`Write waveform summary dataframe to S3 in parquet format.`
	
	`:param wavs_df: waveform summary dataframe`
	`:param path: S3 directory prefix`
	`:type wavs_df: pandas dataframe`
	`:type path: str`
	`:return: None`
	`"""`
	`extra_args = {"ServerSideEncryption": "aws:kms"}`
	`wr.s3.to_parquet(`
	`df=wavs_df,`
	`path=path,`
	`compression='snappy',`
	`s3_additional_kwargs=extra_args)`	

Tarea	Descripción	Habilidades requeridas

	`def combine_data():`
	`    """`
	`    Get combined data and write to parquet.`
	
	`    :return: waveform summary dataframe`
	`    :rtype: pandas dataframe`
	`    """`
	`    wavs_df = get_data()`
	`    wavs_df = normalize_signal_names(wavs_df)`
	`    write_parquet(wavs_df, "s3://{}/{}/{}".format(buck et_xform, dataset_p refix, pass1p5ou t_data))`
	
	`    return wavs_df`
	
	`wavs_df = combine_d ata()`	

Ejecutar trabajos de procesamiento

Tarea	Descripción	Habilidades requeridas
Ejecute el primer trabajo de procesamiento.	Para realizar la fragmenta ción de macros, ejecute un trabajo de procesami ento independiente para cada grupo de archivos.	Científico de datos, ingeniero de machine learning

Tarea	Descripción	Habilidades requeridas

	La microfragmentación se realiza dentro de cada trabajo de procesamiento, ya que cada trabajo ejecuta el primer script. El código siguiente muestra cómo iniciar un trabajo de procesami ento para cada directorio de grupos de archivos en el siguiente fragmento (incluido en `notebooks/FeatExtr act_Pass1.ipynb`).
	
	`pat_groups = list(rang e(30,40))`
	`ts = str(int(time.time( )))`
	
	`for group in pat_group s:`
	`sklearn_processor = SKLearnProcessor(f ramework_version=' 0.20.0',`
	
	`role=role,`
	
	`instance_ type='ml.m5.4xlarge',`
	
	`instance_ count=1,`
	
	`volume_si ze_in_gb=5)`
	`sklearn_processor. run(`
	`code='../src/ feature-engineering-`	

Tarea	Descripción	Habilidades requeridas
	pass1/preprocessing.py', job_name='-'.join(['scaled-processing-p1', str(group), ts]), arguments=["input_path", "/opt/ml/processing/input", "output_path", "/opt/ml/processing/output", "group_data_out", "ws_df_group.json"], inputs= [ProcessingInput(source=f's3://{sess.default_bucket()}/data_inputs/{group}', destination='/opt/ml/processing/input', s3_data_distribution_type='FullyReplicated')], outputs= [ProcessingOutput(source='/opt/ml/processing/output',	

Tarea	Descripción	Habilidades requeridas

	<pre>destination=f's3://{sess.default_bucket()}/data_outputs/{group}'
	            )
	        ],
	        wait=False
	    )</pre>	

Tarea	Descripción	Habilidades requeridas

Ejecute el segundo trabajo de procesamiento.	Para combinar los resultados generados por el primer conjunto de trabajos de procesamiento y realizar cualquier cálculo adicional para el preprocesamiento, ejecute el segundo script mediante un único trabajo de SageMaker procesamiento. El siguiente código lo demuestra (incluido en `notebooks/FeatExtract_Pass1p5.ipynb`).
	
	`ts = str(int(time.time()))`
	`bucket = sess.default_bucket()`
	
	`sklearn_processor = SKLearnProcessor(framework_version='0.20.0',`
	
	`role=role,`
	
	`instance_type='ml.t3.2xlarge',`
	
	`instance_count=1,`
	
	`volume_size_in_gb=5)`
	`sklearn_processor.run(`
	`code='../src/feature-engineering-pass1p5/preprocessing.py',`
		Científico de datos, ingeniero de machine learning

Tarea	Descripción	Habilidades requeridas

	<pre>job_name='-'.join(
	['scaled-processing',
	'p1p5', ts]),
	arguments=['bucket
	', bucket,
	'pass1out
	_prefix', 'data_out
	puts',
	'pass1out
	_data', 'ws_df_gr
	oup.json',
	'pass1p5o
	ut_data', 'waveform
	_summary.parquet',
	'statsdat
	a_name', 'signal_s
	tats.csv'],
	wait=True
	)</pre>	

Recursos relacionados

- Incorporarse a Amazon SageMaker Studio mediante Quick Start (SageMaker documentación)
- Datos del proceso (SageMaker documentación)
- Procesamiento de datos con scikit-learn (documentación) SageMaker
- Documentación de JobLib.Parallel
- Moody, B., Moody, G., Villarroel, M., Clifford, G. D., & Silva, I. (2020). Base de datos de formas de onda MIMIC-III (versión 1.0). PhysioNet.
- Johnson, A. E. W., Pollard, T. J., Shen, L., Lehman, L. H., Feng, M., Ghassemi, M., Moody, B., Szolovits, P., Celi, L. A., & Mark, R. G. (2016). MIMIC-III, una base de datos de cuidados intensivos de acceso gratuito. Scientific Data, 3, 160035.
- Licencia de MIMIC-III Waveform Database

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Visualice los resultados del AI/ML modelo con Flask y AWS Elastic Beanstalk

Chris Caudill y Durga Sury, Amazon Web Services

Resumen

La visualización de los resultados de los servicios de inteligencia artificial y machine learning (IA/ML) suele requerir llamadas complejas a la API, que los desarrolladores e ingenieros deben personalizar. Esto puede ser un inconveniente si sus analistas desean explorar rápidamente un nuevo conjunto de datos.

Para mejorar la accesibilidad de sus servicios y ofrecer una forma de análisis de datos más interactiva puede utilizar una interfaz de usuario (UI) basada en la web que permite a los usuarios cargar sus propios datos y visualizar los resultados del modelo en un panel de control.

Este patrón utiliza Flask y Plotly para integrar Amazon Comprehend en una aplicación web personalizada y visualizar opiniones y entidades a partir de los datos proporcionados por los usuarios. El patrón también proporciona los pasos para implementar una aplicación mediante el uso AWS Elastic Beanstalk. Puede adaptar la aplicación mediante servicios de AWS IA o con un modelo entrenado personalizado alojado en un punto final (por ejemplo, un SageMaker punto final de Amazon).

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.
- AWS Command Line Interface (AWS CLI), instalado y configurado en su máquina local. Para obtener más información al respecto, consulte Conceptos básicos de configuración en la AWS CLI documentación. También puede usar un entorno de desarrollo AWS Cloud9 integrado (IDE); para obtener más información al respecto, consulte el tutorial de Python para AWS Cloud9 obtener una vista previa de las aplicaciones en ejecución en el AWS Cloud9 IDE en la AWS Cloud9 documentación.

  Aviso: ya no AWS Cloud9 está disponible para nuevos clientes. Los clientes actuales de AWS Cloud9 pueden seguir utilizando el servicio con normalidad. Más información

- Comprensión de la estructura de aplicaciones web de Flask. Para obtener más información acerca de Flask, consulte Quickstart en la documentación de Flask.
- Python 3.6 o una versión posterior, instalada y configurada. Puede instalar Python siguiendo las instrucciones de Configuración del entorno de desarrollo de Python en la AWS Elastic Beanstalk documentación.
- Interfaz de la línea de comandos de Elastic Beanstalk (CLI de EB), instalada y configurada. Para obtener más información al respecto, consulte Instalación de la CLI de EB y Configuración de la CLI de EB en la documentación de Elastic Beanstalk.

Limitaciones

- La aplicación Flask de este patrón está diseñada para funcionar con archivos .csv que utilizan una sola columna de texto y están limitados a 200 filas. El código de la aplicación se puede adaptar para gestionar otros tipos de archivos y volúmenes de datos.
- La aplicación no tiene en cuenta la retención de datos y continúa agregando los archivos de usuario cargados hasta que se eliminan manualmente. Puede integrar la aplicación con Amazon Simple Storage Service (Amazon S3) para el almacenamiento persistente de objetos o utilizar una base de datos como Amazon DynamoDB para el almacenamiento de valores clave sin servidor.
- La aplicación solo tiene en cuenta documentos en inglés. Sin embargo, puede utilizar Amazon Comprehend para detectar el idioma principal de un documento. Para obtener más información acerca de los idiomas admitidos para cada acción, consulte la Referencia de la API en la documentación de Amazon Comprehend.

Arquitectura

Arquitectura de aplicaciones Flask

Flask es una estructura ligera para desarrollar aplicaciones web en Python. Está diseñada para combinar el potente procesamiento de datos de Python con una interfaz de usuario web enriquecida. La aplicación Flask del patrón muestra cómo crear una aplicación web que permita a los usuarios cargar datos, enviar los datos a Amazon Comprehend para su inferencia y, a continuación, visualizar los resultados. La aplicación tiene la estructura siguiente:

- `static`— Contiene todos los archivos estáticos que admiten la interfaz de usuario web (por ejemplo JavaScript, CSS e imágenes)
- `templates` – Contiene todas las páginas HTML de la aplicación

- `userData` – Almacena los datos cargados por el usuario
- `application.py` – El archivo de la aplicación Flask
- `comprehend_helper.py` – Funciones para realizar llamadas de API a Amazon Comprehend
- `config.py` – Archivo de configuración de la aplicación
- `requirements.txt` – Las dependencias de Python que requiere la aplicación

El script `application.py` contiene la funcionalidad principal de la aplicación web, que consta de cuatro rutas de Flask. En el diagrama siguiente se muestran estas rutas de Flask.

- `/` es la raíz de la aplicación y dirige a los usuarios a la página `upload.html` (almacenada en el directorio `templates`).
- `/saveFile` es una ruta que se invoca después de que un usuario cargue un archivo. Esta ruta recibe una solicitud `POST` a través de un formulario HTML, que contiene el archivo cargado por el usuario. El archivo se guarda en el directorio `userData` y la ruta redirige a los usuarios a la ruta `/dashboard`.
- `/dashboard` envía a los usuarios a la página `dashboard.html`. En el HTML de esta página, ejecuta el JavaScript código `static/js/core.js` que lee los datos de la `/data` ruta y, a continuación, crea visualizaciones para la página.
- `/data` es una API de JSON que presenta los datos que se van a visualizar en el panel de control. Esta ruta lee los datos proporcionados por el usuario y utiliza las funciones en `comprehend_helper.py` para enviar los datos del usuario a Amazon Comprehend para el análisis de opiniones y el reconocimiento de entidades nombradas (NER). La respuesta de Amazon Comprehend se formatea y se devuelve como un objeto JSON.

Arquitectura de implementación

Consideraciones sobre el diseño

Para obtener más información sobre las consideraciones de diseño de las aplicaciones implementadas con Elastic Beanstalk Nube de AWS en el, consulte la documentación. AWS Elastic Beanstalk

Pila de tecnología

- Amazon Comprehend
- Elastic Beanstalk
- Flask

Automatización y escala

Las implementaciones de Elastic Beanstalk se configuran automáticamente con equilibradores de carga y grupos de escalado automático. Para obtener más opciones de configuración, consulte Configuración de entornos de Elastic Beanstalk en la documentación de Elastic Beanstalk.

Tools (Herramientas)

- AWS Command Line Interface (AWS CLI) es una herramienta unificada que proporciona una interfaz coherente para interactuar con todas las partes de AWS.
- Amazon Comprehend: utiliza el procesamiento de lenguaje natural (NLP) para extraer información sobre el contenido de los documentos, sin necesitar procesamiento especial.
- AWS Elastic Beanstalkle ayuda a implementar y administrar aplicaciones rápidamente Nube de AWS sin tener que conocer la infraestructura en la que se ejecutan esas aplicaciones.
- La CLI de Elastic Beanstalk (EB CLI) es una AWS Elastic Beanstalk interfaz de línea de comandos que proporciona comandos interactivos para simplificar la creación, la actualización y la supervisión de los entornos desde un repositorio local.
- El marco de Flask hace el procesamiento de datos y las llamadas a la API mediante Python y ofrece una visualización web interactiva con Plotly.

Repositorio de código

El código de este patrón está disponible en los resultados del AI/ML modelo de GitHub Visualize mediante Flask y el repositorio. AWS Elastic Beanstalk

Epics

Configurar la aplicación Flask

Tarea	Descripción	Habilidades requeridas
Clona el GitHub repositorio.	Extraiga el código de la aplicación de los resultados	Desarrollador

Tarea	Descripción	Habilidades requeridas
	del AI/ML modelo de GitHub Visualize mediante Flask y el AWS Elastic Beanstalk repositorio ejecutando el siguiente comando: `git clone git@github.com:aws-samples/aws-comprehend-elasticbeanstalk-for-flask.git` **Note** Asegúrese de configurar sus claves SSH con. GitHub	

Tarea	Descripción	Habilidades requeridas

Instale los módulos de Python.	Una vez clonado el repositorio, se crea un nuevo directorio `aws-comprehend-elasticbeanstalk-for-flask` local. En ese directorio, el archivo `requirements.txt` contiene los módulos y las versiones de Python que ejecutan la aplicación. Utilice los comandos siguientes para instalar los módulos:
	
	`cd aws-comprehend-elasticbeanstalk-for-flask`
	
	`pip install -r requirements.txt`
		Python developer

Tarea	Descripción	Habilidades requeridas

Pruebe la aplicación localmente.	Ejecute el siguiente comando para iniciar el servidor de Flask:
	
	`python application.py`
	
	Esto devuelve información sobre el servidor en ejecución. Debería poder acceder a la aplicación si abre un navegador y visita http://localhost:5000
	
	Note
	Si ejecutas la aplicación en un AWS Cloud9 IDE, debes reemplazar el `application.run()` comando del `application.py` archivo por la siguiente línea:
	
	`application.run(host=os.getenv('IP', '0.0.0.0'),port=int(os.getenv('PORT', 8080)))`
	
	Debe revertir este cambio antes de la implementación.
		Python developer

Implementar la aplicación en Elastic Beanstalk

Tarea	Descripción	Habilidades requeridas
Inicie la aplicación Elastic Beanstalk.	Para lanzar el proyecto como una aplicación de Elastic Beanstalk, ejecute el comando siguiente desde el directorio raíz de la aplicación: `eb init -p python-3.6 comprehend_flask --region us-east-1` ⚠ Important • `comprehend_flask` es el nombre de la aplicación de Elastic Beanstalk y se puede cambiar según las necesidades. • Puede sustituirla por Región de AWS una región de su elección. Si no especificas una región, AWS CLI se utiliza la opción de región predeterminada. • La aplicación se creó con la versión de Python 3.6. Es posible que se produzcan errores si utiliza otras versiones de Python.	Arquitecto, desarrollador

Tarea	Descripción	Habilidades requeridas
	Ejecute el comando `eb init -i` para obtener más opciones de configuración de implementación.	
Implemente el entorno de Elastic Beanstalk.	Ejecute el comando siguiente desde el directorio raíz de la aplicación: `eb create comprehend-flask-env` **Note** `comprehend-flask-env` es el nombre del entorno de Elastic Beanstalk y se puede cambiar según las necesidades. El nombre solo puede contener letras, números y guiones.	Arquitecto, desarrollador

Tarea	Descripción	Habilidades requeridas
Autorice su implementación para usar Amazon Comprehend.	Si bien es posible que su aplicación se haya implementado correctamente, también debe proporcionar a su implementación acceso a Amazon Comprehend. `ComprehendFullAccess` es una política AWS gestionada que proporciona a la aplicación implementada permisos para realizar llamadas de API a Amazon Comprehend. Adjunte la política `ComprehendFullAccess` a `aws-elasticbeanstalk-ec2-role` (esta función se crea automáticamente para las instancias de Amazon Elastic Compute Cloud (Amazon EC2) de la implementación) al ejecutar el comando siguiente: `aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/ComprehendFullAccess --role-name aws-elasticbeanstalk-ec2-role`	Desarrollador, arquitecto de seguridad

Tarea	Descripción	Habilidades requeridas
	Important `aws-elasticbeanstalk-ec2-role` se crea cuando se implementa la aplicación. Debe completar el proceso de implementación antes de poder adjuntar la política AWS Identity and Access Management (IAM).	
Visite su aplicación implementada.	Una vez que la aplicación se haya implementado correctamente, puede visitarla mediante la ejecución del comando `eb open`. También puede ejecutar el comando `eb status` para recibir detalles sobre su implementación. La URL de la implementación aparece en `CNAME`.	Arquitecto, desarrollador

(Opcional) Personalizar la aplicación según su modelo de ML

Tarea	Descripción	Habilidades requeridas
Autorice que Elastic Beanstalk acceda al nuevo modelo.	Asegúrese de que Elastic Beanstalk tenga los permisos	Desarrollador, arquitecto de seguridad

Tarea	Descripción	Habilidades requeridas
	de acceso necesarios para el nuevo modelo de punto de conexión. Por ejemplo, si utilizas un punto de conexión de Amazon SageMaker AI, tu implementación debe tener permiso para invocar el punto de conexión. Para obtener más informaci ón al respecto, consulte InvokeEndpointla documenta ción de Amazon SageMaker AI.	

Tarea	Descripción	Habilidades requeridas
Envíe los datos del usuario a un nuevo modelo.	Para cambiar el modelo de ML subyacente en esta aplicación, debe cambiar los archivos siguientes: • `comprehend_helper.py` : Este es el script de Python que se conecta con Amazon Comprehend, procesa la respuesta y devuelve el resultado final a la aplicación. En este script, puede enrutar los datos a otro servicio de IA del Nube de AWS servidor o enviar los datos a un punto final de modelo personalizado. Es recomendable formatear también los resultados de este script para separarlos lógicamente y poder reutilizar este patrón. • `application.py` : Si cambia el nombre del script `comprehend_helper.py` o de las funciones, debe actualizar el script `application.py` de la aplicación para que refleje esos cambios.	Científico de datos

Tarea	Descripción	Habilidades requeridas
Actualice las visualizaciones del panel de control.	Por lo general, la incorporación de un nuevo modelo de ML significa que las visualizaciones deben actualizarse para reflejar los nuevos resultados. Se han realizado estos cambios en los archivos siguientes: • `templates/dashboard.html` : La aplicación prediseñada solo tiene en cuenta dos visualizaciones básicas. El diseño completo de la página se puede ajustar en este archivo. • `static/js/core.js` : Este script captura la salida formateada de la ruta `/data` del servidor Flask y usa Plotly para crear visualizaciones. Puede añadir o actualizar los gráficos de la página.	Desarrollador web

(Opcional) Implementar la aplicación actualizada

Tarea	Descripción	Habilidades requeridas
Actualice el archivo de requisitos de su solicitud.	Antes de enviar los cambios a Elastic Beanstalk, actualice el archivo `requirements.txt` para que refleje los nuevos módulos de Python. Para ello,	Python developer

Tarea	Descripción	Habilidades requeridas
	ejecute el siguiente comando en el directorio raíz de la aplicación: `pip freeze > requirements.txt`	
Vuelva a implementar el entorno de Elastic Beanstalk.	Para asegurarse de que los cambios en la aplicación se reflejen en la implementación de Elastic Beanstalk, navegue hasta el directorio raíz de la aplicación y ejecute el comando siguiente: `eb deploy` Esto envía la versión más reciente del código de la aplicación a la implementación de Elastic Beanstalk existente.	Administrador de sistemas, arquitecto

Resolución de problemas

Problema	Solución
`Unable to assume role "arn:aws:iam::xxxxxxxxxx:role/aws-elasticbeanstalk-ec2-role". Verify that the role exists and is configured correctly.`	Si este error se produce al ejecutar`eb create`, cree una aplicación de muestra en la consola de Elastic Beanstalk para crear el perfil de instancia predeterminado. Para obtener más información al respecto, consulte Creación de un entorno de Elastic Beanstalk en la documentación. AWS Elastic Beanstalk

Problema	Solución

`Your WSGIPath refers to a file that does not exist.`	Este error se produce en los registros de implementación porque Elastic Beanstalk espera que se nombre el código de Flask. `application.py` Si eligió un nombre diferente, ejecútelo `eb config` y edítelo WSGIPath como se muestra en el siguiente ejemplo de código:
	
	`aws:elasticbeanstalk:container:python:`
	`  NumProcesses: '1'`
	`  NumThreads: '15'`
	`  StaticFiles: /static/=static/`
	`  WSGIPath: application.py`
	
	Asegúrese de reemplazar `application.py` con el nombre de su archivo.
	
	También puede aprovechar Gunicorn y un Procfile. Para obtener más información sobre este enfoque, consulte Configurar el servidor WSGI con un Procfile en la AWS Elastic Beanstalk documentación.

`Target WSGI script '/opt/python/current/app/application.py' does not contain WSGI application 'application'.`	Elastic Beanstalk espera que se nombre la variable que representa la aplicación Flask. `application` Asegúrese de que el archivo `application.py` utilice `application` como nombre de la variable: `application = Flask(__name__)`

Problema	Solución
`The EB CLI cannot find your SSH key file for keyname`	Utilice la CLI de EB para especificar qué par de claves usar o para crear un par de claves para las instancias Amazon EC2 de la implementación. Para resolver el error, ejecute `eb init -i` y una de las opciones le solicitar á lo siguiente: `Do you want to set up SSH for your instances?` Responda Y para crear un par de claves o especificar un par de claves existente.
He actualizado mi código y lo he vuelto a implementar, pero mi implementación no refleja mis cambios.	Si utilizas un repositorio de Git con tu implementación, asegúrate de añadir y confirmar los cambios antes de volver a implementarlos.
Estás previsualizando la aplicación Flask desde un AWS Cloud9 IDE y te encuentras con errores.	Para obtener más información al respecto, consulte la documentación sobre cómo obtener una vista previa de las aplicaciones en ejecución en el AWS Cloud9 IDE. AWS Cloud9

Recursos relacionados

- Llame a un punto final modelo Amazon SageMaker AI mediante Amazon API Gateway y AWS Lambda
- Implementación de una aplicación Flask en Elastic Beanstalk
- Referencia de los comandos de EB CLI
- Configuración del entorno de desarrollo de Python

Información adicional

Uso de Amazon Comprehend para el procesamiento de lenguaje natural

Al elegir Amazon Comprehend, puede detectar entidades personalizadas en documentos de texto individuales mediante la ejecución de análisis en tiempo real o trabajos por lotes asíncronos. Amazon Comprehend también le permite entrenar modelos personalizados de reconocimiento de entidades y clasificación de texto que se pueden utilizar en tiempo real mediante la creación de un punto de conexión.

Este patrón utiliza trabajos por lotes asíncronos para detectar opiniones y entidades en un archivo de entrada que contiene varios documentos. La aplicación de ejemplo que proporciona este patrón está diseñada para que los usuarios carguen un archivo .csv que contenga una sola columna con un documento de texto por fila. El `comprehend_helper.py` archivo del AI/ML modelo GitHub Visualize muestra los resultados con Flask y el AWS Elastic Beanstalk repositorio lee el archivo de entrada y envía la entrada a Amazon Comprehend para su procesamiento.

BatchDetectEntities

Amazon Comprehend inspecciona el texto de un lote de documentos en busca de entidades nombradas y devuelve la entidad detectada, la ubicación, el tipo de entidad y una puntuación que indica el nivel de confianza de Amazon Comprehend. Se puede enviar un máximo de 25 documentos en una llamada de API, y cada documento tiene un tamaño inferior a 5000 bytes. Puede filtrar los resultados para mostrar solo determinadas entidades en función del caso de uso. Así, por ejemplo, puede omitir el tipo de entidad `'quantity'` y establecer una puntuación límite para la entidad detectada (por ejemplo, 0,75). Le recomendamos que explore los resultados para su caso de uso específico antes de elegir un valor umbral. Para obtener más información al respecto, consulte BatchDetectEntitiesla documentación de Amazon Comprehend.

BatchDetectSentiment

Amazon Comprehend inspecciona un lote de documentos entrantes y devuelve la opinión predominante para cada documento (`POSITIVE`, `NEUTRAL`, `MIXED` o `NEGATIVE`). Se puede enviar un máximo de 25 documentos en una llamada de API, y cada documento tiene un tamaño inferior a 5000 bytes. Analizar la opinión es sencillo y se puede elegir aquella que tiene la puntuación más alta para que aparezca en los resultados finales. Para obtener más información al respecto, consulte BatchDetectSentimentla documentación de Amazon Comprehend.

Manejo de la configuración de Flask

Los servidores Flask utilizan una serie de variables de configuración para controlar el funcionamiento del servidor. Estas variables pueden contener el resultado de la depuración, tokens de sesión u otros ajustes de la aplicación. También puede definir variables personalizadas a las que se puede acceder

mientras la aplicación se está ejecutando. Existen varios enfoques para establecer las variables de configuración.

En este patrón, la configuración se define `config.py` y se hereda dentro de `application.py`.

- `config.py` contiene las variables de configuración que se configuran al iniciar la aplicación. En esta aplicación, se define una variable `DEBUG` para indicar a la aplicación que ejecute el servidor en modo de depuración.

  > **Note**
  >
  > El modo de depuración no debe utilizarse cuando se ejecuta una aplicación en un entorno de producción. `UPLOAD_FOLDER`es una variable personalizada que se define para hacer referencia a ella más adelante en la aplicación e indicarle dónde deben almacenarse los datos de usuario cargados.

- `application.py` inicia la aplicación Flask y hereda los ajustes de configuración definidos en `config.py`. Esto se lleva a cabo mediante el código siguiente:

```
application = Flask(__name__)
application.config.from_pyfile('config.py')
```

Más patrones

- Acelere MLOps con las plantillas Backstage y de autoservicio de Amazon AI SageMaker
- Automatice las operaciones de AWS infraestructura con Amazon Bedrock
- Automatice la configuración del emparejamiento entre regiones con AWS Transit Gateway
- Implementación de sistemas de agentes en Amazon Bedrock con el marco CrewAI mediante Terraform
- Implemente una ChatOps solución para gestionar los resultados de los escaneos SAST mediante Amazon Q Developer en aplicaciones de chat, acciones personalizadas y CloudFormation
- Genere información de datos mediante AWS Mainframe Modernization Amazon Q en Quick Sight
- Genere información sobre z/OS datos de Db2 mediante AWS Mainframe Modernization Amazon Q en Quick Sight
- Otorgue a las instancias de SageMaker notebook acceso temporal a un CodeCommit repositorio de otra cuenta de AWS
- Gestione AWS Organizations las políticas como código mediante AWS CodePipeline Amazon Bedrock
- Modernice la aplicación de CardDemo mainframe mediante AWS Transform
- Modernice e implemente aplicaciones de mainframe con Terraform AWS Transform
- Realizar análisis avanzados mediante Amazon Redshift ML
- Optimice la gestión EC2 del cumplimiento de Amazon con los agentes de Amazon Bedrock y AWS Config
- Simplificación del desarrollo y la implementación de los bots de Amazon Lex mediante un flujo de trabajo automatizado
- Transforma Easytrieve a lenguajes modernos usando AWS Transform personalizado
- Solucione problemas de estados AWS Step Functions mediante Amazon Bedrock

Análisis

Temas

- Analizar los datos de Amazon Redshift en Microsoft SQL Server Analysis Services
- Analice y visualice datos JSON anidados con Amazon Athena y Amazon Quick Sight
- Automatice la ingesta de datos desde AWS Data Exchange Amazon S3
- Automatice la aplicación del cifrado en AWS Glue mediante una CloudFormation plantilla de AWS
- Cree una canalización de datos para incorporar, transformar y analizar los datos de Google Analytics con el kit de AWS DataOps desarrollo
- Cree una canalización de procesamiento de video con Amazon Kinesis Video Streams y AWS Fargate
- Cree una canalización de servicios de ETL para cargar datos de forma incremental desde Amazon S3 a Amazon Redshift mediante AWS Glue
- Cree una malla de datos empresarial con Amazon DataZone y AWS CDK AWS CloudFormation
- Calcule el valor en riesgo (VaR) mediante los servicios de AWS
- Configurar el acceso entre cuentas a un catálogo de datos de AWS Glue compartido con Amazon Athena
- Convierta la característica temporal NORMALIZE de Teradata en Amazon Redshift SQL
- Convierta la característica RESET WHEN de Teradata en Amazon Redshift SQL
- Implementar y administrar un lago de datos sin servidor en la nube de AWS mediante el uso de la infraestructura como código
- Imponga el etiquetado de los clústeres de Amazon EMR en el lanzamiento
- Asegúrese de que el registro de Amazon EMR en Amazon S3 esté habilitado en el lanzamiento
- Genere datos de prueba con un trabajo de AWS Glue y Python
- Capturar datos de IoT directamente en Amazon S3 de forma rentable con AWS IoT Greengrass
- Lanzar un trabajo de Spark en un clúster EMR transitorio mediante una función de Lambda
- Migración de cargas de trabajo de Apache Cassandra a Amazon Keyspaces mediante AWS Glue
- Migración de Oracle Business Intelligence 12c a la nube de AWS desde servidores en las instalaciones
- Migración de ELK Stack a Elastic Cloud en AWS
- Migre datos al Nube de AWS mediante Starburst

- Optimice la incorporación ETL del tamaño del archivo de entrada en AWS
- Organice una canalización de ETL con validación, transformación y particionamiento mediante AWS Step Functions
- Realizar análisis avanzados mediante Amazon Redshift ML
- Consulta de las tablas de Amazon DynamoDB con SQL mediante Amazon Athena
- Acceder, consultar y unirse a las tablas de Amazon DynamoDB con Athena
- Configure la clasificación por idioma para los resultados de las consultas de Amazon Redshift mediante una UDF escalar de Python
- Suscripción de una función de Lambda a las notificaciones de eventos de buckets de S3 en diferentes regiones de AWS
- Tres tipos de trabajos de AWS Glue ETL para convertir datos a Apache Parquet
- Visualice los registros de auditoría de Amazon Redshift con Amazon Athena y Amazon QuickSight
- Visualice los informes de credenciales de IAM para todas las cuentas de AWS mediante Amazon Quick Sight
- Más patrones

Analizar los datos de Amazon Redshift en Microsoft SQL Server Analysis Services

Sunil Vora, Amazon Web Services

Resumen

Este patrón describe cómo conectar y analizar los datos de Amazon Redshift en Microsoft SQL Server Analysis Services, mediante el proveedor OLE DB de Intellisoft o el proveedor de CData ADO.NET para el acceso a la base de datos.

Amazon Redshift es un servicio de almacenamiento de datos administrado de varios petabytes en la nube. SQL Server Analysis Services es una herramienta de procesamiento analítico en línea (OLAP) que se puede utilizar para analizar datos de data mart y almacenamiento de datos como Amazon Redshift. Puede usar SQL Server Analysis Services para crear cubos OLAP a partir de sus datos para un análisis de datos rápido y avanzado.

Requisitos previos y limitaciones

Supuestos

- Este patrón describe cómo configurar SQL Server Analysis Services e Intellisoft OLE DB Provider o CData ADO.NET Provider para Amazon Redshift en una instancia de Amazon Elastic Compute Cloud (Amazon). EC2 Como alternativa, puede instalar ambas opciones en un host del centro de datos corporativo.

Requisitos previos

- Una cuenta de AWS activa
- Un clúster de Amazon Redshift con credenciales

Arquitectura

Pila de tecnología de origen

- Un clúster de Amazon Redshift

Pila de tecnología de destino

- Microsoft SQL Server Analysis Services

Arquitectura de origen y destino

Tools (Herramientas)

- Microsoft Visual Studio 2019 (Community Edition)
- Intellisoft OLE DB Provider para Amazon Redshift (versión de prueba) CData o ADO.NET Provider para Amazon Redshift (versión de prueba)

Epics

Analizar tablas

Tarea	Descripción	Habilidades requeridas
Analice las tablas y los datos que se van a importar.	Identifique las tablas de Amazon Redshift que se van a importar y sus tamaños.	Administrador de base de datos

Configure la instancia y las herramientas de instalación EC2

Tarea	Descripción	Habilidades requeridas
Configura una EC2 instancia.	En su cuenta de AWS, cree una EC2 instancia en una subred pública o privada.	Administrador de sistemas
Instale herramientas para acceder a la base de datos.	Descargue e instale el proveedor OLE DB de Intellisoft para Amazon Redshift (CData o el proveedor de ADO.NET para Amazon Redshift).	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Instale Visual Studio.	Descargue e instale Visual Studio 2019 (Community Edition).	Administrador de sistemas
Instalar extensiones.	Instale la extensión de Microsoft Analysis Services Projects en Visual Studio.	Administrador de sistemas
Cree un proyecto.	Cree un nuevo proyecto de modelo tabular en Visual Studio para almacenar los datos de Amazon Redshift. En Visual Studio, seleccione la opción Analysis Services Tabular Project (Proyecto tabular de Analysis Services) al crear el proyecto.	Administrador de base de datos

Cree un origen de datos y tablas de importación

Tarea	Descripción	Habilidades requeridas
Cree un origen de datos de Amazon Redshift.	Cree una fuente de datos de Amazon Redshift con el proveedor OLE DB de Intelliso ft para Amazon Redshift (o el CData proveedor de ADO.NET para Amazon Redshift) y sus credenciales de Amazon Redshift.	Amazon Redshift, administr ador de base de datos
Importar tablas.	Seleccione e importe tablas y vistas de Amazon Redshift	Amazon Redshift, administr ador de base de datos

Tarea	Descripción	Habilidades requeridas
	a su proyecto de SQL Server Analysis Services.	

Limpiar después de la migración

Tarea	Descripción	Habilidades requeridas
EC2 Elimine la instancia.	Elimina la EC2 instancia que lanzaste anteriormente.	Administrador de sistemas

Recursos relacionados

- Amazon Redshift (Documentación de AWS)
- Install SQL Server Analysis Services (Instalar SQL Server Analysis Services) (documentación de Microsoft)
- Tabular Model Designer (Diseñador de modelos tabulares) (documentación de Microsoft)
- Overview of OLAP cubes for advanced analytics (Descripción general de los cubos OLAP para análisis avanzados) (documentación de Microsoft)
- Microsoft Visual Studio 2019 (Community Edition)
- Intellisoft OLE DB Provider for Amazon Redshift (Trial)
- CData Proveedor de ADO.NET para Amazon Redshift (versión de prueba)

Analice y visualice datos JSON anidados con Amazon Athena y Amazon Quick Sight

Anoop Singh, Amazon Web Services

Resumen

Este patrón explica cómo convertir una estructura de datos anidada con formato JSON en una vista tabular mediante Amazon Athena y, a continuación, visualizar los datos en Amazon Quick Sight.

Puede usar datos con formato JSON en fuentes de datos de sistemas operativos basadas en API para crear productos de datos. Estos datos también pueden ayudarle a comprender mejor a sus clientes y sus interacciones con sus productos, de forma que pueda personalizar las experiencias de los usuarios y predecir los resultados.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Un archivo JSON que representa una estructura de datos anidada (este patrón proporciona un archivo de ejemplo)

Limitaciones:

- Las características de JSON se integran bien con las funciones orientadas a SQL existentes en Athena. Sin embargo, no son compatibles con ANSI SQL y se espera que el archivo JSON contenga cada registro en una línea separada. Puede que tenga que usar la propiedad `ignore.malformed.json` de Athena para indicar si los registros JSON con formato incorrecto deben convertirse en caracteres nulos o generar errores. Para más información, consulte Prácticas recomendadas para leer datos JSON en la documentación de Athena.
- Este patrón considera solo cantidades pequeñas y simples de datos con formato JSON. Si desea utilizar estos conceptos a escala, considere la posibilidad de aplicar la partición de datos y consolidar los datos en archivos más grandes.

Arquitectura

En el siguiente diagrama se muestran los componentes de la arquitectura y el flujo de trabajo de este patrón. Las estructuras de datos anidadas se almacenan en Amazon Simple Storage Service (Amazon S3) en formato JSON. En Athena, los datos JSON se asignan a una estructura de datos de Athena. A continuación, se crea una vista para analizar los datos y visualizar la estructura de los datos en Quick Sight.

Tools (Herramientas)

Servicios de AWS

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos. Este patrón utiliza Amazon S3 para almacenar el archivo JSON.
- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar. Este patrón utiliza Athena para consultar y transformar los datos de JSON. Con unas cuantas acciones en el Consola de administración de AWS, puede dirigir Athena a sus datos en Amazon S3 y usar SQL estándar para ejecutar consultas únicas. Athena no requiere un servidor, por lo que no hay que configurar ni administrar ninguna infraestructura y solo pagará por las consultas que ejecute. Athena se escala automáticamente y ejecuta las consultas en paralelo, de modo que los resultados se obtienen rápidamente, incluso con conjuntos de datos de gran tamaño y consultas complejas.
- Amazon Quick Sight es un servicio de inteligencia empresarial (BI) a escala de nube que le ayuda a visualizar, analizar y elaborar informes sobre sus datos en un único panel. Quick Sight le permite crear y publicar fácilmente paneles interactivos que incluyen información sobre el aprendizaje automático (ML). Puede acceder a los paneles desde cualquier dispositivo e integrarlos en sus aplicaciones, portales y sitios web.

Código de ejemplo

El siguiente archivo JSON proporciona una estructura de datos anidada que puede utilizar en este patrón.

```
{
  "symbol": "AAPL",
```

```
  "financials": [
    {
      "reportDate": "2017-03-31",
      "grossProfit": 20591000000,
      "costOfRevenue": 32305000000,
      "operatingRevenue": 52896000000,
      "totalRevenue": 52896000000,
      "operatingIncome": 14097000000,
      "netIncome": 11029000000,
      "researchAndDevelopment": 2776000000,
      "operatingExpense": 6494000000,
      "currentAssets": 101990000000,
      "totalAssets": 334532000000,
      "totalLiabilities": 200450000000,
      "currentCash": 15157000000,
      "currentDebt": 13991000000,
      "totalCash": 67101000000,
      "totalDebt": 98522000000,
      "shareholderEquity": 134082000000,
      "cashChange": -1214000000,
      "cashFlow": 12523000000,
      "operatingGainsLosses": null
    }
  ]
}
```

Epics

Configuración de un bucket de S3

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Para crear un bucket para almacenar el archivo JSON, inicie sesión en Consola de administración de AWS, abra la consola Amazon S3 y, a continuación, seleccione Create bucket. Para obtener más información, consulte Crear un bucket en la	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	documentación de Amazon S3.	
Añada los datos JSON anidados.	Cargue el archivo JSON en un bucket de S3. Para ver un archivo JSON de muestra, consulte la sección anterior. Para más instrucciones, consulte Cargar objetos en la documentación de Amazon S3.	Administrador de sistemas

Análisis de datos en Athena

Tarea	Descripción	Habilidades requeridas
Cree una tabla para asignar los datos de JSON.	1. Abra la consola de Athena. 2. Cree una base de datos siguiendo las instrucciones de la documentación de Athena. 3. En el menú Base de datos, elija la base de datos que creó. 4. En el Editor de consultas, introduzca una instrucción `CREATE TABLE` como la siguiente: `CREATE EXTERNAL TABLE financials_json ( symbol string, financials array< struct<re portdate: string,`	Desarrollador

Tarea	Descripción	Habilidades requeridas

	<pre>grossprof
	it: bigint,
	totalreve
	nue: bigint,
	totalcash
	: bigint,
	totaldebt
	: bigint,
	researcha
	nddevelopment:
	bigint>>
	)
	ROW FORMAT SERDE
	'org.openx.data.js
	onserde.JsonSerDe'
	LOCATION 's3://s3b
	ucket-for-athena/'</pre> LOCATION especifica la ubicación del bucket de S3 que contiene el archivo JSON.
	5. Elija Run (Ejecutar) para crear la tabla.
	
	Para más información acerca de la creación de tablas, consulte la documentación de Athena.	

Tarea	Descripción	Habilidades requeridas
Cree una vista para el análisis de datos.	1. Abra la consola de Athena. 2. Cree una base de datos siguiendo las instrucciones de la documentación de Athena. 3. En el menú Base de datos, elija la base de datos que creó. 4. En el Editor de consultas, introduzca una instrucción `CREATE VIEW` como la siguiente: `CREATE OR REPLACE VIEW financial_json_view AS SELECT symbol, financials[1].reportdate one_report_date, -- indexes start with 1 financials[1].totalrevenue one_total_revenue, financials[1].reportdate another_report_date, financials[1].totalrevenue another_total_revenue FROM financials_json where symbol='AAPL' ORDER BY 1` 5. Elija Ejecutar para crear la vista.	Desarrollador

Tarea	Descripción	Habilidades requeridas
	Para más información acerca de la creación de vistas, consulte la documentación de Athena.	
Análisis y validación de los datos.	1. Abra la consola de Athena. 2. En el editor de consultas , ejecute las consultas mediante la vista que creó en el paso anterior. 3. Valide los datos con el archivo JSON para confirmar que los nombres de las columnas y los tipos de datos están asignados correctamente.	Desarrollador

Visualice los datos en Quick Sight

Tarea	Descripción	Habilidades requeridas
Configure Athena como fuente de datos en Quick Sight.	1. Abre la consola Quick. 2. Elija Conjuntos de datos, Nuevo conjunto de datos. 3. Elija Athena como origen de datos. 4. Elija la base de datos que incluye la vista que ha creado. 5. Elija la vista en la que quiere crear el conjunto de datos.	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	6. En la página Finalizar la creación del conjunto de datos, elija Directly query your data (Consultar directamente los datos). 7. Elija Visualize.	
Visualice los datos en Quick Sight.	1. Después de visualizar el conjunto de datos, elija las imágenes del panel izquierdo y elija los campos para el conjunto de datos. Para obtener más información, consulte el tutorial en la documentación rápida. 2. Guarde los cambios aplicados al análisis. 3. Elija Publish dashboard (Publicar el panel de control) para publicar las imágenes que ha creado.	Analista de datos

Recursos relacionados

- Documentación de Amazon Athena
- Tutoriales de Amazon Quick Sight
- Cómo trabajar con JSON anidado (entrada en el blog)

Automatice la ingesta de datos desde AWS Data Exchange Amazon S3

Adnan Alvee y Manikanta Gona, Amazon Web Services

Resumen

Este patrón proporciona una CloudFormation plantilla que le permite incorporar automáticamente datos de su lago de AWS Data Exchange datos en Amazon Simple Storage Service (Amazon S3).

AWS Data Exchange es un servicio que facilita el intercambio seguro de conjuntos de datos basados en archivos en la nube de AWS. AWS Data Exchange los conjuntos de datos se basan en suscripciones. Como suscriptor, también puede acceder a las revisiones de los conjuntos de datos a medida que los proveedores publican nuevos datos.

La CloudFormation plantilla crea un evento en Amazon CloudWatch Events y una AWS Lambda función. El evento está pendiente de cualquier actualización del conjunto de datos del suscriptor. Si hay una actualización, CloudWatch inicia una función Lambda, que copia los datos en el bucket de S3 que especifique. Cuando los datos se han copiado correctamente, Lambda le envía una notificación de Amazon Simple Notification Service (Amazon SNS).

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Suscripción a un conjunto de datos en AWS Data Exchange

Limitaciones

- La CloudFormation plantilla debe implementarse por separado para cada conjunto de datos suscrito en AWS Data Exchange.

Arquitectura

Pila de tecnología de destino

- AWS Lambda

- Amazon S3
- AWS Data Exchange
- Amazon CloudWatch
- Amazon SNS

Arquitectura de destino

Automatización y escala

Puede usar la CloudFormation plantilla varias veces para los conjuntos de datos que desee incorporar al lago de datos.

Tools (Herramientas)

- AWS Data Exchangefacilita a AWS los clientes el intercambio seguro de conjuntos de datos basados en archivos en el. Nube de AWS Como suscriptor, puede encontrar y suscribirse a cientos de productos de proveedores de datos cualificados. Luego, puede descargar rápidamente el conjunto de datos o copiarlo en Amazon S3 para usarlo en una variedad de servicios de AWS análisis y aprendizaje automático. Cualquier persona que tenga una Cuenta de AWS puede AWS Data Exchange suscribirse.
- AWS Lambda le permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo se paga por el tiempo de computación que se consume, sin ningún cargo mientras el código no se ejecuta. Con Lambda puede ejecutar código para prácticamente cualquier tipo de aplicación o servicio de backend, sin ningún esfuerzo de administración. Lambda ejecuta el código en una infraestructura informática de alta disponibilidad y realiza todas las tareas de administración de los recursos informáticos, incluidos el mantenimiento del servidor y del sistema operativo, el aprovisionamiento de capacidad y el escalado automático, así como la supervisión del código y las funciones de registro.
- Amazon S3 proporciona almacenamiento para Internet. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web.
- Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en AWS los recursos. Con reglas sencillas que puede configurar rápidamente, puede hacer coincidir los eventos y dirigirlos a una o más funciones o transmisiones de destino. CloudWatch Los eventos se dan cuenta de los cambios operativos a medida que

se producen. Responde a estos cambios operativos y toma medidas correctoras según sea necesario, enviando mensajes para responder al entorno, activando funciones, realizando cambios y captando información de estado. También puedes usar CloudWatch Events para programar acciones automatizadas que se inicien automáticamente en determinados momentos mediante expresiones cron o rate.

- Amazon Simple Notification Service (Amazon SNS) permite a las aplicaciones, los usuarios finales y los dispositivos enviar y recibir al instante notificaciones desde la nube. Amazon SNS proporciona temas (canales de comunicación) para mensajes push de alto rendimiento. many-to-many AI utilizar los temas de Amazon SNS, los editores pueden distribuir mensajes a un gran número de suscriptores para su procesamiento en paralelo, incluidas las colas de Amazon Simple Queue Service (Amazon SQS), las funciones de Lambda y los webhooks. HTTP/S También puede utilizar Amazon SNS para enviar notificaciones a usuarios finales mediante notificaciones push para móvil, SMS y correo electrónico.

Epics

Suscribirse a un conjunto de datos

Tarea	Descripción	Habilidades requeridas
Suscríbase a un conjunto de datos.	En la AWS Data Exchange consola, suscríbase a un conjunto de datos. Para obtener instrucciones, consulte Suscribirse a productos de datos AWS Data Exchange en la AWS documentación.	AWS general
Tenga en cuenta los atributos del conjunto de datos.	Anote Región de AWS el ID y el ID de revisión del conjunto de datos. Lo necesitará para la CloudFormation plantilla en el siguiente paso.	AWS general

Implemente la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3 y una carpeta.	Si ya tiene un lago de datos en Amazon S3, cree una carpeta para almacenar los datos desde AWS Data Exchange los que se van a ingerir. Si va a implementar la plantilla con fines de prueba, cree un nuevo bucket de S3 y anote el nombre del bucket y el prefijo de la carpeta para el paso siguiente.	AWS general
Implemente la CloudFormation plantilla.	Implemente la CloudFormation plantilla que se proporciona como adjunto a este patrón. Para obtener instrucciones, consulte la documentación de CloudFormation. Configure los siguiente s parámetros para que se correspondan con su configuración Cuenta de AWS, su conjunto de datos y su bucket de S3: conjunto de datos Región de AWS, ID de conjunto de datos, ID de revisión, nombre del bucket de S3 (por ejemplo`DOC-EXAMPLE-BUCKET`), prefijo de carpeta (por ejemplo,`myfolder/`) y correo electrónico para	AWS general

Tarea	Descripción	Habilidades requeridas
	notificaciones de SNS. Puede establecer el parámetro Nombre del conjunto de datos con cualquier nombre. Al implementar la plantilla , ejecuta una función de Lambda para incorporar automáticamente el primer conjunto de datos disponibl e en el conjunto de datos. En adelante, la ingesta posterior se lleva a cabo automátic amente, a medida que llegan nuevos datos al conjunto de datos.	

Recursos relacionados

- Suscribirse a productos de datos el AWS Data Exchange (documentación)AWS Data Exchange

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Automatice la aplicación del cifrado en AWS Glue mediante una CloudFormation plantilla de AWS

Diogo Guedes, Amazon Web Services

Resumen

Este patrón muestra cómo configurar y automatizar la aplicación del cifrado en AWS Glue mediante una CloudFormation plantilla de AWS. La plantilla crea todas las configuraciones y los recursos necesarios para aplicar el cifrado. Estos recursos incluyen una configuración inicial, un control preventivo creado por una EventBridge regla de Amazon y una función de AWS Lambda.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Permisos para implementar la CloudFormation plantilla y sus recursos

Limitaciones

Este control de seguridad es regional. Debe implementar el control de seguridad en cada región de AWS en la que desee configurar la aplicación del cifrado en AWS Glue.

Arquitectura

Pila de tecnología de destino

- Amazon CloudWatch Logs (de AWS Lambda)
- EventBridge Regla de Amazon
- CloudFormation Pila de AWS
- AWS CloudTrail
- Rol y política gestionados de AWS Identity and Access Management (IAM)
- AWS Key Management Service (AWS KMS)
- Alias de AWS KMS
- Función de AWS Lambda
- Almacén de parámetros de AWS Systems Manager

Arquitectura de destino

En el siguiente diagrama, se muestra cómo automatizar la aplicación del cifrado en AWS Glue.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Una CloudFormation plantilla crea todos los recursos, incluida la configuración inicial y el control de detección para la aplicación del cifrado en AWS Glue.
2. Una EventBridge regla detecta un cambio de estado en la configuración de cifrado.
3. Se invoca una función Lambda para la evaluación y el registro a través CloudWatch de los registros. En caso de detección de incumplimiento, se recupera el almacén de parámetros con un nombre de recurso de Amazon (ARN) como clave de AWS KMS. Se corrige el estado de cumplimiento del servicio con el cifrado activado.

Automatización y escala

Si utiliza AWS Organizations, puede utilizar AWS CloudFormation StackSets para implementar esta plantilla en varias cuentas en las que desee habilitar la aplicación del cifrado en AWS Glue.

Tools (Herramientas)

- Amazon le CloudWatch ayuda a monitorizar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, funciones de Lambda, puntos de conexión de invocación HTTP que utilizan destinos API o buses de eventos en otras cuentas de AWS.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS le CloudTrail ayuda a habilitar la auditoría operativa y de riesgos, la gobernanza y el cumplimiento de su cuenta de AWS.
- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.

- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Systems Manager le permite administrar las aplicaciones y la infraestructura que se ejecutan en la nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo requerido para detectar y resolver problemas operativos y ayuda a utilizar y administrar los recursos de AWS a escala de manera segura.

Código

El código de este patrón está disponible en el repositorio GitHub aws-custom-guardrail-eventcontrolado por componentes.

Prácticas recomendadas

AWS Glue admite el cifrado de datos en reposo para la creación de trabajos en AWS Glue y el desarrollo de scripts mediante puntos de conexión de desarrollo.

Tenga en cuenta las siguientes prácticas recomendadas:

- Configure trabajos ETL y puntos de conexión de desarrollo para utilizar claves de AWS KMS para escribir datos cifrados en reposo.
- Cifre los metadatos almacenados en el catálogo de datos de AWS Glue mediante claves que administra a través de KMS de AWS.
- Además, puede usar las claves KMS de AWS para cifrar marcadores de trabajo y los registros que generan los rastreadores y los trabajos de ETL.

Epics

Lanza la plantilla CloudFormation

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla.	Descargue la `aws-custo m-guardrail-event-`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	`driven.yaml` plantilla del GitHub repositorio y, a continuación, impleméntela. El estado `CREATE_COMPLETE` indica que su plantilla se implementó correctamente. **Note** La plantilla no requiere parámetros de entrada.	

Compruebe la configuración de cifrado en AWS Glue

Tarea	Descripción	Habilidades requeridas
Compruebe las configuraciones clave de AWS KMS.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la consola de AWS Glue. 2. En el panel de navegación, en Data Catalog (Catálogo de datos), elija Catalog settings (Configuración de catálogo). 3. Compruebe que los ajustes de cifrado de metadatos y cifrado de contraseñas de conexión estén marcados y configurados para usar `KMSKeyGlue` .	Arquitecto de la nube

Pruebe la aplicación del cifrado

Tarea	Descripción	Habilidades requeridas
Identifique la configuración de cifrado en CloudFormation.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la CloudFormation consola. 2. En el panel de navegación, elija Stacks (Pilas) y, a continuación, elija la pila que desee. 3. Elija la pestaña Recursos. 4. En la tabla de Resources (Recursos), busque la configuración de cifrado por Logical ID (ID lógico).	Arquitecto de la nube
Cambie la infraestructura aprovisionada a un estado que no cumpla con las normas.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la consola de AWS Glue. 2. En el panel de navegación, en Data Catalog (Catálogo de datos), elija Catalog settings (Configuración de catálogo). 3. Desactive la casilla de verificación Metadata encryption (Cifrado de metadatos). 4. Desactive la casilla de verificación Encrypt connection passwords (Cifrar contraseñas de conexión).	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	5. Seleccione Save (Guardar). 6. Actualice la consola de AWS Glue. La barrera de protección detecta el estado no conforme en AWS Glue después de desactivar las casillas y, a continuación, aplica el cumplimiento corrigiendo automáticamente el error de configuración del cifrado. Como resultado, las casillas de verificación de cifrado deberían volver a seleccion arse después de actualizar la página.	

Recursos relacionados

- Creación de una pila en la CloudFormation consola de AWS (CloudFormation documentación de AWS)
- Creación de una regla de CloudWatch eventos que se active en una llamada a la API de AWS mediante AWS CloudTrail (CloudWatch documentación de Amazon)
- Configuración del cifrado en AWS Glue (documentación de AWS Glue)

Cree una canalización de datos para incorporar, transformar y analizar los datos de Google Analytics con el kit de AWS DataOps desarrollo

Anton Kukushkin y Rudy Puig, Amazon Web Services

Resumen

Este patrón describe cómo crear una canalización de datos para incorporar, transformar y analizar los datos de Google Analytics mediante el kit de AWS DataOps desarrollo (AWS DDK) y otros. Servicios de AWS El AWS DDK es un marco de desarrollo de código abierto que te ayuda a crear flujos de trabajo de datos y una arquitectura de datos moderna. AWS Uno de los principales objetivos del AWS DDK es ahorrarle el tiempo y el esfuerzo que normalmente se dedican a tareas de canalización de datos que requieren mucha mano de obra, como la organización de las canalizaciones, la construcción de infraestructuras y la creación de las bases de esa infraestructura. DevOps Puede delegar estas tareas, que requieren mucha mano de obra, a AWS DDK para que pueda centrarse en escribir código y en otras actividades de gran valor.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Un AppFlow conector de Amazon para Google Analytics, configurado
- Python y pip (administrador de paquetes de Python)
- Git, instalado y configurado
- AWS Command Line Interface (AWS CLI), instalado y configurado
- AWS Cloud Development Kit (AWS CDK)instalado

Versiones de producto

- Python 3.7 o posterior
- pip 9.0.3 o posterior

Arquitectura

Pila de tecnología

- Amazon AppFlow
- Amazon Athena
- Amazon CloudWatch
- Amazon EventBridge
- Amazon Simple Storage Service (Amazon S3)
- Amazon Simple Queue Service (Amazon SQS)
- AWS DataOps Kit de desarrollo (AWS DDK)
- AWS Lambda

Arquitectura de destino

El siguiente diagrama muestra el proceso basado en eventos que incorpora, transforma y analiza los datos de Google Analytics.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Una regla de eventos CloudWatch programados de Amazon invoca a Amazon AppFlow.
2. Amazon AppFlow ingiere los datos de Google Analytics en un bucket de S3.
3. Una vez que el bucket de S3 ingiere los datos, EventBridge se generan las notificaciones de eventos, que se capturan mediante una regla de CloudWatch eventos y, a continuación, se colocan en una cola de Amazon SQS.
4. Una función Lambda consume los eventos de la cola de Amazon SQS, lee los objetos S3 correspondientes, transforma los objetos al formato Apache Parquet, escribe los objetos transformados en el bucket de S3 y, a continuación, crea o actualiza la definición de la tabla. AWS Glue Data Catalog
5. Una consulta de Athena realiza comparaciones con la tabla.

Tools (Herramientas)

AWS herramientas

- Amazon AppFlow es un servicio de integración totalmente gestionado que le permite intercambiar datos de forma segura entre aplicaciones de software como servicio (SaaS).
- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.
- Amazon le CloudWatch ayuda a supervisar las métricas de sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, AWS Lambda funciones, puntos finales de invocación HTTP que utilizan destinos de API o buses de eventos en otros. Cuentas de AWS
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Cloud Development Kit (AWS CDK)es un marco para definir la infraestructura de nube en el código y aprovisionarla mediante ella. CloudFormation
- AWS DataOps El kit de desarrollo (AWS DDK) es un marco de desarrollo de código abierto que le ayuda a crear flujos de trabajo de datos y una arquitectura de datos moderna. AWS

Código

El código de este patrón está disponible en los repositorios GitHub AWS DataOps Development Kit (AWS DDK) y Analyzing Google Analytics data with Amazon AppFlow, Amazon Athena AWS DataOps y Development Kit.

Epics

Prepare el entorno

Tarea	Descripción	Habilidades requeridas
Clone el código fuente.	Para clonar el código fuente, ejecute el siguiente comando: `git clone https://github.com/aws-samples/aws-ddk-examples.git`	DevOps ingeniero
Cree un entorno virtual.	Navegue hasta el directorio de código fuente y, a continuación, ejecute el siguiente comando para crear un entorno virtual: `cd google-analytics-data-using-appflow/ python && python3 -m venv .venv`	DevOps ingeniero
Instalar las dependencias.	Para activar el entorno virtual e instalar las dependencias, ejecute el siguiente comando: `source .venv/bin/activate && pip install -r requirements.txt`	DevOps ingeniero

Implemente la aplicación que usa su proceso de datos

Tarea	Descripción	Habilidades requeridas
Inicie el entorno.	1. Confirme que AWS CLI está configurado con credenciales válidas para su Cuenta de AWS. Para obtener más información, consulte Uso de perfiles con nombre en la AWS CLI documentación. 2. Ejecute el comando `cdk bootstrap --profile [AWS_PROFILE] .`	DevOps ingeniero
Implemente los datos.	Para implementar el proceso de datos, ejecute el comando `cdk deploy --profile [AWS_PROFILE] .`	DevOps ingeniero

Cómo probar la implementación

Tarea	Descripción	Habilidades requeridas
Valide el estado de la pila.	1. Abra la consola de CloudFormation. 2. En la página Pilas, confirme que el estado de la pila `DdkAppflowAthenaStack` es `CREATE_COMPLETE` .	DevOps ingeniero

Resolución de problemas

Problema	Solución
La implementación falla durante la creación de un recurso `AWS::AppFlow::Flow` y recibe el siguiente error: `Connector Profile with name ga-connection does not exist`	Confirma que has creado un AppFlow conector de Amazon para Google Analytics y le has dado un nombre`ga-connection` . Para obtener instrucciones, consulta Google Analytics en la AppFlow documentación de Amazon.

Recursos relacionados

- AWS DataOps Kit de desarrollo (AWS DDK) (GitHub)
- AWS Ejemplos de DDK () GitHub

Información adicional

AWS Las canalizaciones de datos del DDK se componen de una o varias etapas. Los siguientes ejemplos de código emplean `AppFlowIngestionStage` para incorporar datos de Google Analytics, `SqsToLambdaStage` para gestionar la transformación de datos y `AthenaSQLStage` para ejecutar la consulta de Athena.

En primer lugar, se crean las etapas de transformación e incorporación de datos, como se muestra en el siguiente ejemplo de código:

```
        appflow_stage = AppFlowIngestionStage(
            self,
            id="appflow-stage",
            flow_name=flow.flow_name,
        )
        sqs_lambda_stage = SqsToLambdaStage(
            self,
            id="lambda-stage",
            lambda_function_props={
                "code": Code.from_asset("./ddk_app/lambda_handlers"),
                "handler": "handler.lambda_handler",
```

```
                "layers": [
                    LayerVersion.from_layer_version_arn(
                        self,
                        id="layer",
                        layer_version_arn=f"arn:aws:lambda:
{self.region}:336392948345:layer:AWSDataWrangler-Python39:1",
                    )
                ],
                "runtime": Runtime.PYTHON_3_9,
            },
        )
        # Grant lambda function S3 read & write permissions
        bucket.grant_read_write(sqs_lambda_stage.function)
        # Grant Glue database & table permissions
        sqs_lambda_stage.function.add_to_role_policy(
            self._get_glue_db_iam_policy(database_name=database.database_name)
        )
        athena_stage = AthenaSQLStage(
            self,
            id="athena-sql",
            query_string=[
                (
                    "SELECT year, month, day, device, count(user_count) as cnt "
                    f"FROM {database.database_name}.ga_sample "
                    "GROUP BY year, month, day, device "
                    "ORDER BY cnt DESC "
                    "LIMIT 10; "
                )
            ],
            output_location=Location(
                bucket_name=bucket.bucket_name, object_key="query-results/"
            ),
            additional_role_policy_statements=[
                self._get_glue_db_iam_policy(database_name=database.database_name)
            ],
        )
```

A continuación, la `DataPipeline` construcción se utiliza para «conectar» las etapas mediante EventBridge reglas, como se muestra en el siguiente ejemplo de código:

```
        (
            DataPipeline(self, id="ingestion-pipeline")
            .add_stage(
```

```
                stage=appflow_stage,
                override_rule=Rule(
                    self,
                    "schedule-rule",
                    schedule=Schedule.rate(Duration.hours(1)),
                    targets=appflow_stage.targets,
                ),
            )
            .add_stage(
                stage=sqs_lambda_stage,
                # By default, AppFlowIngestionStage stage emits an event after the flow
run finishes successfully
                # Override rule below changes that behavior to call the the stage when
data lands in the bucket instead
                override_rule=Rule(
                    self,
                    "s3-object-created-rule",
                    event_pattern=EventPattern(
                        source=["aws.s3"],
                        detail={
                            "bucket": {"name": [bucket.bucket_name]},
                            "object": {"key": [{"prefix": "ga-data"}]},
                        },
                        detail_type=["Object Created"],
                    ),
                    targets=sqs_lambda_stage.targets,
                ),
            )
            .add_stage(stage=athena_stage)
        )
```

Para ver más ejemplos de código, consulta el GitHub repositorio Análisis de datos de Google Analytics con Amazon AppFlow, Amazon Athena y AWS DataOps Development Kit.

Cree una canalización de procesamiento de video con Amazon Kinesis Video Streams y AWS Fargate

Piotr Chotkowski y Pushparaju Thangavel, Amazon Web Services

Resumen

Este patrón muestra cómo utilizar Amazon Kinesis Video Streams y AWS Fargate para extraer fotogramas de una transmisión de video y almacenarlos como archivos de imagen en Amazon Simple Storage Service (Amazon S3) para su posterior procesamiento.

El patrón proporciona una aplicación de muestra en forma de proyecto Java Maven. Esta aplicación define la infraestructura de AWS mediante AWS Cloud Development Kit (AWS CDK). Tanto la lógica de procesamiento de fotogramas como las definiciones de infraestructura están escritas en el lenguaje de programación Java. Puede utilizar esta aplicación de muestra como base para desarrollar su propia canalización de procesamiento de video en tiempo real o para crear la etapa de preprocesamiento de video de una canalización con machine learning.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Java SE Development Kit (JDK) 11, instalado
- Apache Maven, instalado
- AWS Cloud Development Kit (AWS CDK), instalado
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2, instalada
- Docker (necesario para compilar imágenes de Docker con el fin de utilizarlas en las definiciones de tareas de AWS Fargate), instalado

Limitaciones

Este patrón está concebido como prueba de concepto o como base para un desarrollo futuro. No se debe utilizar en su forma actual para implementaciones de producción.

Versiones de producto

- Este patrón se ha probado con la versión 1.77.0 de AWS CDK (consulte las versiones de AWS CDK)
- JDK 11
- CLI de AWS versión 2

Arquitectura

Pila de tecnología de destino

- Amazon Kinesis Video Streams
- Tarea de AWS Fargate
- Cola de Amazon Simple Queue Service (Amazon SQS)
- Bucket S3 de Amazon

Arquitectura de destino

El usuario crea una transmisión de video de Kinesis, carga un video y envía un mensaje JSON que contiene detalles sobre la transmisión de video de Kinesis de entrada y el bucket de S3 de salida a una cola de SQS. AWS Fargate, que ejecuta la aplicación principal en un contenedor, extrae el mensaje de la cola de SQS y comienza a extraer los fotogramas. Cada fotograma se guarda en un archivo de imagen y se almacena en el bucket de S3 de destino.

Automatizar y escalar

La aplicación de muestra se puede escalar tanto horizontal como verticalmente dentro de una misma Región de AWS. El escalado horizontal se puede lograr aumentando el número de tareas de AWS Fargate implementadas que leen de la cola de SQS. El escalado vertical se puede lograr aumentando el número de subprocesos de división de fotogramas y publicación de imágenes en la aplicación. Estos ajustes se transfieren como variables de entorno a la aplicación en la definición del QueueProcessingFargateServicerecurso en la CDK de AWS. Gracias al diseño de implementación de la pila de AWS CDK, puede implementar esta aplicación en varias regiones y cuentas de AWS sin ningún esfuerzo adicional.

Tools (Herramientas)

Herramientas

- AWS CDK es un marco de desarrollo de software para definir la infraestructura y los recursos de la nube mediante lenguajes de programación como Python TypeScript JavaScript, Java y C#/.Net.
- Amazon Kinesis Video Streams es un servicio de AWS completamente administrado que puede utilizar para transmitir videos en directo desde dispositivos a la nube de AWS, o bien crear aplicaciones para el procesamiento de video en tiempo real o el análisis de video orientado a lotes.
- AWS Fargate es un motor de cómputo sin servidor para contenedores. Fargate elimina la necesidad de aprovisionar y administrar servidores y le permite centrarse en el desarrollo de sus aplicaciones.
- Amazon S3: es un servicio de almacenamiento de objetos de AWS que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento.
- Amazon SQS es un servicio de colas de mensajes completamente administrado que permite el desacople y el escalado de microservicios, sistemas distribuidos y aplicaciones sin servidor.

Código

- Se adjunta un archivo .zip del proyecto de la aplicación de muestra (`frame-splitter-code.zip`).

Epics

Implementación de la infraestructura

Tarea	Descripción	Habilidades requeridas
Iniciar el daemon de Docker.	Inicie el daemon de Docker en su sistema local. El AWS CDK usa Docker para crear la imagen que se utiliza en la tarea de AWS Fargate. Debe ejecutar Docker antes de continuar con el siguiente paso.	Desarrollador, ingeniero DevOps
Compilar el proyecto.	Descargue la aplicación de muestra `frame-splitter-code` (adjunta) y extraiga su	Desarrollador, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	contenido en una carpeta de su máquina local. Antes de poder implementar la infraestructura, debe crear el proyecto Java Maven. En el símbolo del sistema, navegue hasta el directorio raíz del proyecto y compile el proyecto ejecutando el comando: `mvn clean install`	
Arrancar el AWS CDK.	(Solo para usuarios iniciales de AWS CDK) Si es la primera vez que utiliza AWS CDK, es posible que tenga que que arrancar el entorno mediante la ejecución del comando AWS CLI: `cdk bootstrap --profile "$AWS_PROFILE_NAME"` donde `$AWS_PROFILE_NAME` contiene el nombre del perfil de AWS obtenido de sus credenciales de AWS. O bien, puede eliminar este parámetro para utilizar el perfil predeterminado. Para obtener más información, consulte la documentación de AWS CDK.	Desarrollador, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Implemente la pila de AWS CDK.	En este paso, debe crear los recursos de infraestructura necesarios (cola de SQS, bucket de S3, definición de tareas de AWS Fargate) en su cuenta de AWS, crear la imagen de Docker necesaria para la tarea de AWS Fargate e implementar la aplicación. En el símbolo del sistema, navegue hasta el directorio raíz del proyecto y ejecute el comando: `cdk deploy --profile "$AWS_PROFILE_NAME" --all` donde `$AWS_PROFILE_NAME` contiene el nombre del perfil de AWS obtenido de sus credenciales de AWS. O bien, puede eliminar este parámetro para utilizar el perfil predeterminado. Confirme la implementación. Anote los valores QueueUrly Bucket del resultado de la implementación del CDK; los necesitará en pasos posteriores. El AWS CDK crea los activos, los carga en su cuenta de AWS y crea todos los recursos de infraestructura.	Desarrollador, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	Puede observar el proceso de creación de recursos en la CloudFormation consola de AWS. Para obtener más información, consulte la CloudFormation documentación de AWS y la documentación de AWS CDK.	

Tarea	Descripción	Habilidades requeridas
Cree una transmisión de video.	En este paso, creará una transmisión de video de Kinesis que servirá como transmisión de entrada para el procesamiento de video. Asegúrese de que ha instalado y configurado la AWS CLI. En la AWS CLI, ejecute: `aws kinesisvideo --profile "$AWS_PROFILE_NAME" create-stream --stream-name "$STREAM_NAME" --data-retention-in-hours "24"` donde `$AWS_PROFILE_NAME` contiene el nombre del perfil de AWS obtenido de sus credenciales de AWS (o elimine este parámetro para utilizar el perfil predeterminado) y `$STREAM_NAME` es cualquier nombre de transmisión válido. Como alternativa, puede crear una transmisión de video mediante la consola de Kinesis siguiendo los pasos indicados en la documentación de Kinesis Video Streams. Anote el nombre de recurso de AWS (ARN)	Desarrollador, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	de la transmisión creada; lo necesitará más adelante.	

Ejecute un ejemplo

Tarea	Descripción	Habilidades requeridas
Subir el video a la transmisión.	En la carpeta del proyecto de la aplicación de muestra `frame-splitter-code`, abra el archivo `ProcessingTaskTest.java` en la carpeta `src/test/java/amazon/awscdk/examples/splitter`. Sustituya las variables `profileName` y `streamName` por los valores que utilizó en los pasos anteriores. Para cargar el video de muestra en la transmisión de video de Kinesis que ha creado en el paso anterior, ejecute: `amazon.awscdk.examples.splitter.ProcessingTaskTest#testExample test` Como alternativa, puede cargar el video mediante uno de los métodos descritos en la documentación de Kinesis Video Streams.	Desarrollador, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Iniciar el procesamiento de video.	Ahora que ha cargado un video a la transmisión de video de Kinesis, puede empezar a procesarlo. Para iniciar la lógica de procesamiento, debe enviar un mensaje con detalles a la cola de SQS que el AWS CDK creó durante la implementación. Para enviar un mensaje utilizando la AWS CLI, ejecute:
	`aws sqs --profile "$AWS_PROFILE_NAME" send-message --queue-url QUEUE_URL --message-body MESSAGE`
	where `$AWS_PROFILE_NAME` contiene el nombre del perfil de AWS de sus credenciales de AWS (elimine este parámetro para usar el perfil predeterminado), `QUEUE_URL` es el `QueueUrl`valor de la salida de la CDK de AWS y `MESSAGE` es una cadena JSON con el siguiente formato:
	`{ "streamARN": "STREAM_ARN", "bucket": "BUCKET_NAME", "s3Directory": "test-output" }`
		Desarrollador, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	donde `STREAM_ARN` es el ARN de la transmisión de video que ha creado en un paso anterior y `BUCKET_NAME` es el valor de Bucket obtenido de la salida de AWS CDK. Al enviar este mensaje, se inicia el procesamiento del video. Como alternativa, puede enviar un mensaje mediante la consola de Amazon SQS, tal y como se describe en la documentación de Amazon SQS.	
Ver imágenes de los fotogramas de video.	Puede ver las imágenes resultantes en el bucket de salida de S3 `s3://BUCKET_NAME/test-output` donde `BUCKET_NAME` es el valor del Bucket obtenido de la salida de AWS CDK.	Desarrollador, DevOps ingeniero

Recursos relacionados

- Documentación de AWS SDK
- Referencia de la API de AWS CDK
- Taller introductorio sobre AWS CDK
- Documentación de Amazon Kinesis Video Streams
- Ejemplo: identificación de objetos en transmisiones de vídeo mediante SageMaker
- Ejemplo: Análisis y renderización de fragmentos de Kinesis Video Streams

- Analice vídeos en directo a escala y en tiempo real con Amazon Kinesis Video Streams y SageMaker Amazon (entrada del blog AWS Machine Learning)
- Introducción de AWS Fargate

Información adicional

Cómo elegir un IDE

Le recomendamos que utilice su IDE de Java favorito para crear y explorar este proyecto.

Limpieza

Cuando termine de ejecutar este ejemplo, elimine todos los recursos implementados para evitar incurrir en costos de infraestructura de AWS adicionales.

Para eliminar la infraestructura y la transmisión de video, utilice estos dos comandos en la AWS CLI:

```
cdk destroy --profile "$AWS_PROFILE_NAME" --all
```

```
aws kinesisvideo --profile "$AWS_PROFILE_NAME" delete-stream --stream-arn "$STREAM_ARN"
```

Como alternativa, puede eliminar los recursos manualmente mediante la CloudFormation consola de AWS para eliminar la CloudFormation pila de AWS y la consola Kinesis para eliminar la transmisión de vídeo de Kinesis. Tenga en cuenta que `cdk destroy` no elimina el bucket de S3 de salida ni las imágenes de los repositorios de Amazon Elastic Container Registry (Amazon ECR) (`aws-cdk/assets`). Debe eliminarlos manualmente.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Cree una canalización de servicios de ETL para cargar datos de forma incremental desde Amazon S3 a Amazon Redshift mediante AWS Glue

Rohan Jamadagni y Arunabha Datta, Amazon Web Services

Resumen

Este patrón proporciona orientación sobre cómo configurar Amazon Simple Storage Service (Amazon S3) para obtener un rendimiento óptimo del lago de datos y, a continuación, cargar los cambios incrementales de datos de Amazon S3 en Amazon Redshift mediante AWS Glue, realizando operaciones de extracción, transformación y carga (ETL).

Los archivos de origen de Amazon S3 pueden tener distintos formatos, incluidos valores separados por comas (CSV), archivos XML y JSON. Este patrón describe cómo puede utilizar AWS Glue para convertir los archivos de origen en un formato optimizado para los costos y el rendimiento, como Apache Parquet. Puede consultar los archivos de Parquet directamente desde Amazon Athena y Amazon Redshift Spectrum. También puede cargar archivos Parquet en Amazon Redshift, agregarlos y compartir los datos agregados con los consumidores, o bien visualizar los datos mediante Amazon Quick Sight.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un bucket de origen de S3 que tenga los privilegios adecuados y que contenga archivos CSV, XML o JSON.

Supuestos

- Los archivos de origen CSV, XML o JSON ya están cargados en Amazon S3 y se puede acceder a ellos desde la cuenta en la que están configurados AWS Glue y Amazon Redshift.
- Se siguen las prácticas recomendadas para cargar los archivos, dividirlos, comprimirlos y utilizar un manifiesto, tal como se describe en la documentación de Amazon Redshift.
- La estructura de los archivos de origen permanece inalterada.

- El sistema de origen puede incorporar datos en Amazon S3 siguiendo la estructura de carpetas definida en Amazon S3.
- El clúster de Amazon Redshift abarca una sola zona de disponibilidad. (Esta arquitectura es adecuada porque AWS Lambda, AWS Glue y Amazon Athena están sin servidor). Para una alta disponibilidad, se toman instantáneas de los clústeres con una frecuencia regular.

Limitaciones

- Los formatos de archivo se limitan a los que actualmente admite AWS Glue.
- No se admite la generación de informes posteriores en tiempo real.

Arquitectura

Pila de tecnología de origen

- Bucket de S3 con archivos CSV, XML o JSON

Pila de tecnología de destino

- Lago de datos de S3 (con almacenamiento de archivos Parquet particionado)
- Amazon Redshift

Arquitectura de destino

Flujo de datos

Tools (Herramientas)

- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable. Amazon S3 puede utilizarse para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- AWS Lambda: AWS Lambda le permite ejecutar código sin aprovisionar ni administrar servidores. AWS Lambda es un servicio basado en eventos; puede configurar el código para que se inicie automáticamente desde otros servicios de AWS.

- Amazon Redshift: Amazon Redshift es un servicio de almacenamiento de datos totalmente administrado de varios petabytes. Con Amazon Redshift, puede consultar petabytes de datos estructurados y semiestructurados en su almacenamiento de datos y su lago de datos mediante SQL estándar.
- AWS Glue: AWS Glue es un servicio ETL totalmente gestionado que facilita la preparación y la carga de datos para su análisis. AWS Glue descubre sus datos y almacena los metadatos asociados (por ejemplo, definiciones de tablas y esquemas) en el catálogo de datos de AWS Glue. Sus datos catalogados se pueden buscar, consultar y están disponibles para ETL inmediatamente.
- AWS Secrets Manager: AWS Secrets Manager facilita la protección y la administración centralizada de los secretos necesarios para el acceso a aplicaciones o servicios. El servicio almacena credenciales de bases de datos, claves de API y otros datos confidenciales y elimina la necesidad de codificar de forma rígida la información confidencial en formato de texto sin formato. Secrets Manager también ofrece rotación de claves para satisfacer las necesidades de seguridad y cumplimiento. Incorpora una integración para Amazon Redshift, Amazon Relational Database Service (Amazon RDS) y Amazon DocumentDB. Puede almacenar y gestionar los secretos de forma centralizada mediante la consola Secrets Manager, la interfaz de línea de comandos (CLI) o la API Secrets Manager y. SDKs
- Amazon Athena : Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos que están almacenados en Amazon S3. Athena no tiene servidor y está integrada con AWS Glue, por lo que puede consultar directamente los datos catalogados con AWS Glue. Athena se escala con elasticidad para ofrecer un rendimiento de consultas interactivas.

Epics

Cree los buckets y la estructura de carpetas de S3

Tarea	Descripción	Habilidades requeridas
Analice los sistemas de origen para determinar la estructura y los atributos de los datos.	Realice esta tarea para cada origen de datos que contribuy a al lago de datos de Amazon S3.	Ingeniero de datos
Defina la estrategia de partición y acceso.	Esta estrategia debe basarse en la frecuencia de las capturas de datos, el	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	procesamiento delta y las necesidades de consumo. Asegúrese de que los buckets de S3 no estén abiertos al público y de que el acceso esté controlado únicament e por políticas específicas basadas en los roles de servicio. Para obtener más información, consulte la documentación de Amazon S3.	
Cree buckets de S3 independi entes para cada tipo de origen de datos y un bucket de S3 independiente por origen para los datos procesados (Parquet).	Cree un bucket independi ente para cada origen y, a continuación, cree una estructura de carpetas que se base en la frecuencia de ingesta de datos del sistema de origen; por ejemplo, `s3://source-system-name/date/hour` . Para los archivos procesados (converti dos al formato Parquet), cree una estructura similar; por ejemplo, `s3://source-processed-bucket/date/hour` . Para más información sobre cómo crear buckets de S3, consulte la documentación de Amazon S3.	Ingeniero de datos

Creación de un almacenamiento de datos en Amazon Redshift

Tarea	Descripción	Habilidades requeridas
Lance el clúster de Amazon Redshift con los grupos de parámetros y la estrategia de mantenimiento y copia de seguridad adecuados.	Utilice el secreto de la base de datos de Secrets Manager como credenciales de usuario administrador al crear el clúster de Amazon Redshift. Para obtener informaci ón sobre la creación y el tamaño de un clúster de Amazon Redshift, consulte la documentación de Amazon Redshift y el documento técnico sobre el tamaño del almacenamiento de datos en la nube.	Ingeniero de datos
Cree y asocie un rol de servicio de IAM al clúster de Amazon Redshift.	El rol de servicio AWS Identity and Access Management (IAM) garantiza el acceso a Secrets Manager y a los buckets de S3 de origen. Para obtener más información, consulte la documentación de AWS sobre la autorización y la adición de un rol.	Ingeniero de datos
Crear el esquema de la base de datos.	Siga las prácticas recomenda das de Amazon Redshift para el diseño de tablas. Según el caso de uso, elija las claves de clasificación y distribución adecuadas y la mejor codificac ión de compresión posible. Para conocer las prácticas	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	recomendadas, consulte la documentación de AWS.	
Configure la administración de cargas de trabajo.	Configure las colas de administración de la carga de trabajo (WLM), la aceleración de consultas cortas (SQA) o el escalado simultáneo, según sus necesidades. Para obtener más información, consulte Implementación de la administración de la carga de trabajo en la documentación de Amazon Redshift.	Ingeniero de datos

Cree un secreto en Secrets Manager

Tarea	Descripción	Habilidades requeridas
Cree un nuevo secreto para almacenar las credenciales de inicio de sesión de Amazon Redshift en Secrets Manager.	Este secreto almacena las credenciales del usuario administrador y de los usuarios individuales del servicio de base de datos. Para obtener instrucciones, consulte la documentación de Secretes Manager. Elija Amazon Redshift Cluster como tipo de secreto. Además, en la página de rotación secreta, active la rotación. Esto creará el usuario adecuado en el clúster de Amazon Redshift y	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	cambiará las claves secretas a intervalos definidos.	
Cree una política de IAM para restringir el acceso a Secrets Manager.	Restrinja el acceso a Secrets Manager solo a los administradores de Amazon Redshift y a AWS Glue.	Ingeniero de datos

Configuración de AWS Glue

Tarea	Descripción	Habilidades requeridas
En el catálogo de datos de AWS Glue, añada una conexión para Amazon Redshift.	Para obtener instrucciones, consulte la documentación de AWS Glue.	Ingeniero de datos
Cree y asocie un rol de servicio de IAM para que AWS Glue pueda acceder a los buckets de Secrets Manager, Amazon Redshift y S3.	Para obtener más información, consulte la documentación de AWS Glue.	Ingeniero de datos
Defina el catálogo de datos de AWS Glue para el origen.	Este paso implica crear una base de datos y las tablas necesarias en el catálogo de datos de AWS Glue. Puede utilizar un rastreador para catalogar las tablas de la base de datos de AWS Glue o definirlas como tablas externas de Amazon Athena. También puede acceder a las tablas externas definidas en Athena a través del catálogo	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	de datos de AWS Glue. Consulte la documentación de AWS para obtener más información sobre la definición del catálogo de datos y la creación de una tabla externa en Athena.	
Cree un trabajo de AWS Glue para procesar los datos de origen.	El trabajo de AWS Glue puede consistir en un shell de Python o en PySpark estandarizar, deduplicar y limpiar los archivos de datos de origen. Para optimizar el rendimiento y evitar tener que consultar todo el bucket de código fuente de S3, particione el bucket de S3 por fecha, desglosado por año, mes, día y hora como predicado desplegable para el trabajo de AWS Glue. Para obtener más información, consulte la documentación de AWS Glue. Cargue los datos procesados y transformados en las particiones del bucket de S3 procesadas en formato Parquet. Puede consultar los archivos de Parquet en Athena.	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
Cree un trabajo de AWS Glue para cargar datos en Amazon Redshift.	El trabajo de AWS Glue puede consistir en un shell de Python o PySpark cargar los datos alterándolos y, a continuación, realizar una actualización completa. Para obtener más información, consulte la documentación de AWS Glue y la sección de información adicional.	Ingeniero de datos
(Opcional) Programe los trabajos de AWS Glue mediante activadores según sea necesario.	La carga de datos incremental se debe principalmente a un evento de Amazon S3 que hace que una función de AWS Lambda llame a la tarea de AWS Glue. Utilice la programación basada en activadores de AWS Glue para cualquier carga de datos que exija una programación basada en el tiempo en lugar de en los eventos.	Ingeniero de datos

Crear una función de Lambda

Tarea	Descripción	Habilidades requeridas
Cree y adjunte un rol vinculado a un servicio de IAM para que AWS Lambda pueda acceder a los buckets de S3 y al trabajo de AWS Glue.	Cree un rol vinculado a un servicio de IAM para AWS Lambda con una política para leer los objetos y buckets de Amazon S3 y una política para acceder a la API de AWS	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	Glue para iniciar un trabajo de AWS Glue. Para obtener más información, consulte el Centro de conocimientos.	
Cree una función de Lambda para ejecutar el trabajo de AWS Glue en función del evento Amazon S3 definido.	La función de Lambda debe iniciarse con la creación del archivo de manifiesto de Amazon S3. La función Lambda debe pasar la ubicación de la carpeta de Amazon S3 (por ejemplo, source_bucket/year/month/date/hour) al trabajo de AWS Glue como parámetro . El trabajo de AWS Glue utilizará este parámetro como predicado desplegable para optimizar el acceso a los archivos y el rendimiento del procesamiento de los trabajos. Para obtener más información, consulte la documentación de AWS Glue.	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
Cree un evento de objeto PUT de Amazon S3 para detectar la creación de objetos y llame a la función de Lambda correspondiente.	El evento de objeto PUT de Amazon S3 debe iniciarse solo con la creación del archivo de manifiesto. El archivo de manifiesto controla la función de Lambda y la simultaneidad de las tareas de AWS Glue, y procesa la carga como un lote en lugar de procesar los archivos individuales que llegan a una partición específica del bucket de origen de S3. Para más información, consulte la documentación de Lambda.	Ingeniero de datos

Recursos relacionados

- Documentación de Amazon RDS
- Documentación de AWS Glue
- Documentación de Amazon Redshift
- AWS Lambda
- Amazon Athena
- AWS Secrets Manager

Información adicional

Enfoque detallado para una actualización automática y completa

Upsert: se trata de conjuntos de datos que requieren un agrupado histórico, según el caso de uso empresarial. Siga uno de los enfoques descritos en Actualización e inserción de datos nuevos (documentación de Amazon Redshift) en función de las necesidades de su empresa.

Actualización completa: se trata de conjuntos de datos pequeños que no necesitan agrupados históricos. Siga uno de estos enfoques:

1. Trunque la tabla de Amazon Redshift.
2. Cargue la partición actual desde el área de montaje

o bien:

1. Cree una tabla temporal con datos de partición actuales.
2. Elimine la tabla de destino de Amazon Redshift.
3. Cambie el nombre de la tabla temporal a tabla de destino.

Cree una malla de datos empresarial con Amazon DataZone y AWS CDK AWS CloudFormation

Dhrubajyoti Mukherjee, Ravi Kumar, Weizhou Sun y Adjoa Taylor, Amazon Web Services

Resumen

En Amazon Web Services (AWS), los clientes saben que los datos son la clave para acelerar la innovación y favorecer el valor empresarial de su empresa. Para administrar esta enorme cantidad de datos, puede adoptar una arquitectura descentralizada, como una malla de datos. Una arquitectura de malla de datos facilita la reflexión orientada al producto, que incluye una mentalidad que tiene en cuenta a los clientes, los objetivos y el mercado. La malla de datos también ayuda a establecer un modelo de gobierno federado que proporciona un acceso rápido y seguro a los datos.

En Estrategias para crear en AWS una solución empresarial basada en una malla de datos se analiza cómo puede utilizar el marco estratégico de malla de datos para formular e implementar una estrategia de malla de datos para su organización. Al utilizar el marco estratégico de malla de datos, puede optimizar la organización de los equipos y sus interacciones para acelerar su transición a la malla de datos.

Este documento proporciona orientación sobre cómo crear una malla de datos empresarial con Amazon DataZone. Amazon DataZone es un servicio de administración de datos para catalogar, descubrir, compartir y controlar los datos almacenados AWS en fuentes locales y de terceros. El patrón incluye artefactos de código que le ayudan a implementar la infraestructura de soluciones de datos basada en una malla de datos mediante y. AWS Cloud Development Kit (AWS CDK) AWS CloudFormation Este patrón está pensado para arquitectos e ingenieros de nube. DevOps

Para más información sobre los objetivos de este patrón y el alcance de la solución, consulte la sección Información adicional.

Requisitos previos y limitaciones

Requisitos previos

- Un mínimo de dos activos Cuentas de AWS: uno para la cuenta de gobierno central y otro para la cuenta de miembro
- AWS credenciales de administrador para la cuenta de gobierno central en su entorno de desarrollo

- AWS Command Line Interface (AWS CLI) instaladas para administrarlas Servicios de AWS desde la línea de comandos
- Node.js y Node Package Manager (npm) instalados para administrar aplicaciones AWS CDK
- AWS CDK El kit de herramientas se instala globalmente en su entorno de desarrollo mediante npm para sintetizar e implementar aplicaciones AWS CDK

```
npm install -g aws-cdk
```

- La versión 3.12 de Python instalada en su entorno de desarrollo
- TypeScript instalado en su entorno de desarrollo o instalado globalmente mediante el compilador npm:

```
npm install -g typescript
```

- Docker instalado en su entorno de desarrollo
- Un sistema de control de versiones como Git para mantener el código fuente de la solución (recomendado)
- Un entorno de desarrollo integrado (IDE) o un editor de texto compatible con Python y TypeScript (muy recomendable)

Limitaciones

- La solución se ha probado solo en máquinas que ejecutan Linux o macOS.
- En la versión actual, la solución no admite la integración de Amazon DataZone y es de forma AWS IAM Identity Center predeterminada. Sin embargo, puede modificar la configuración para admitir esta integración.

Versiones de producto

- Python versión 3.12

Arquitectura

En el siguiente diagrama se muestra un ejemplo de la arquitectura de referenciade la malla de datos. La arquitectura se basa en Amazon DataZone y utiliza Amazon Simple Storage Service (Amazon S3) AWS Glue Data Catalog y como fuentes de datos. El Servicios de AWS que utilices con Amazon

DataZone en tu implementación de malla de datos puede variar en función de los requisitos de tu organización.

1. En las cuentas de los productores, los datos sin procesar son aptos para el consumo en su forma actual o se transforman para su consumo mediante el uso AWS Glue. Los metadatos técnicos de los datos se almacenan en Amazon S3 y se evalúan mediante un rastreador de AWS Glue datos. La calidad de los datos se mide mediante Calidad de datos de AWS Glue. La base de datos de origen del catálogo de datos está registrada como un activo en el DataZone catálogo de Amazon. El DataZone catálogo de Amazon se aloja en la cuenta de gobierno central mediante los trabajos de la fuente de DataZone datos de Amazon.
2. La cuenta de gobierno central aloja el DataZone dominio de Amazon y el portal de DataZone datos de Amazon. Los productores y consumidores Cuentas de AWS de datos están asociados al DataZone dominio Amazon. Los DataZone proyectos de Amazon de los productores y consumidores de datos se organizan en las correspondientes unidades de DataZone dominio de Amazon.
3. Los usuarios finales de los activos de datos inician sesión en el portal de DataZone datos de Amazon mediante sus credenciales AWS Identity and Access Management (de IAM) o mediante un inicio de sesión único (con integración a través del Centro de identidad de IAM). Buscan, filtran y visualizan la información de los activos (por ejemplo, información sobre la calidad de los datos o metadatos empresariales y técnicos) en el catálogo de DataZone datos de Amazon.
4. Cuando un usuario final encuentra el activo de datos que busca, utiliza la función de DataZone suscripción de Amazon para solicitar el acceso. El propietario de los datos del equipo de productores recibe una notificación y evalúa la solicitud de suscripción en el portal de DataZone datos de Amazon. El propietario de los datos aprueba o rechaza la solicitud de suscripción en función de su validez.
5. Una vez concedida y tramitada la solicitud de suscripción, el consumidor puede acceder al activo desde su cuenta para realizar las siguientes actividades:
   - Desarrollo de modelos de inteligencia artificial y aprendizaje automático mediante Amazon AI SageMaker
   - Análisis e informes mediante Amazon Athena y Amazon Quick

Tools (Herramientas)

Servicios de AWS

- Amazon Athena es un servicio interactivo de consultas que le permite analizar datos directamente en Amazon Simple Storage Service (Amazon S3) usando SQL estándar.
- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir y aprovisionar la Nube de AWS infraestructura en código.
- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todo el Cuentas de AWS mundo Regiones de AWS.
- Amazon DataZone es un servicio de gestión de datos que te ayuda a catalogar, descubrir, compartir y gestionar los datos AWS almacenados en fuentes externas, locales y de terceros.
- Amazon Quick es un servicio de inteligencia empresarial (BI) a escala de nube que le ayuda a visualizar, analizar y elaborar informes sobre sus datos en un único panel.
- Amazon SageMaker AI es un servicio de aprendizaje automático (ML) gestionado que le ayuda a crear y entrenar modelos de aprendizaje automático para luego implementarlos en un entorno hospedado listo para la producción.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Repositorio de código

La solución está disponible en el repositorio GitHub data-mesh-datazone-cdk-cloudformation.

Epics

Configuración del entorno

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Para clonar el repositorio, ejecute el siguiente comando en el entorno de desarrollo local (Linux o macOS):	Arquitecto e ingeniero de nube DevOps

Tarea	Descripción	Habilidades requeridas
	`git clone https://github.com/aws-samples/data-mesh-data zone-cdk-cloudformation`	

Cree el entorno.	Para crear el entorno virtual de Python, ejecute los siguientes comandos:
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	`pip install -r requirements.txt`
		Arquitecto de nube, DevOps ingeniero

Arranque la cuentas.	Para iniciar la cuenta de gobierno central mediante AWS CDK, ejecute el siguiente comando: `cdk bootstrap aws://<GOVERNANCE_ACCOUNT_ID>/<AWS_REGION>` Inicie sesión en Consola de administración de AWS, abra la consola de cuentas de gobierno central y obtenga el nombre de recurso de Amazon (ARN) de la función de AWS CDK ejecución.	Arquitecto e ingeniero de nube DevOps

Tarea	Descripción	Habilidades requeridas
Cree el archivo `DzDataMeshMemberStackSet.yaml` .	Para crear el archivo `DzDataMeshMemberStackSet.yaml` , vaya al directorio raíz del repositorio e inicie el siguiente script de bash: `./lib/scripts/create_dz_data_mesh_member_stack_set.sh`	Arquitecto de nube, DevOps ingeniero
Confirme la creación de la plantilla.	Asegúrese de que el archivo CloudFormation de plantilla se haya creado en la `lib/cfn-templates/DzDataMeshMemberStackSet.yaml` ubicación.	Arquitecto e DevOps ingeniero de la nube

Implementación de recursos en la cuenta de gobernanza central

Tarea	Descripción	Habilidades requeridas

Modifique la configuración.	En el archivo `config/Config.ts` , modifique los siguientes parámetros:
	`DZ_APPLICATION_NAME - Name of the application.`
	`DZ_STAGE_NAME - Name of the stage.`
	`DZ_DOMAIN_NAME - Name of the Amazon DataZone domain`
		Arquitecto de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	DZ_DOMAIN_DESCRIPTIO N - Description of the Amazon DataZone domain DZ_DOMAIN_TAG - Tag of the Amazon DataZone domain DZ_ADMIN_PROJECT_NAM E - Name of the Amazon DataZone project for administrators DZ_ADMIN_PROJECT_DESC RIPTION - Description of the Amazon DataZone project for administr ators CDK_EXEC_ROLE_ARN - ARN of the cdk execution role DZ_ADMIN_ROLE_ARN - ARN of the administr ator role Mantenga los parámetros restantes vacíos.	

Tarea	Descripción	Habilidades requeridas
Actualiza la configuración del DataZone glosario de Amazon.	Para actualizar la configuración del DataZone glosario de Amazon en el `lib/utils/glossary_config.json` archivo, usa el siguiente ejemplo de configuración: `{ "GlossaryName": "PII Data", "GlossaryDescription": "If data source contains PII attributes", "GlossaryTerms": [{ "Name": "Yes", "ShortDescription": "Yes", "LongDescription": "Yes Glossary Term" }, { "Name": "No", "ShortDescription": "No", "LongDescription": "No Glossary Term" } ] }`	Arquitecto e ingeniero de nube DevOps

Tarea	Descripción	Habilidades requeridas
Actualiza la configuración del formulario de DataZone metadatos de Amazon.	Para actualizar la configuración del formulario de DataZone metadatos de Amazon en `lib/utils/metadata_form_config.json file` , utilice el siguiente ejemplo de configuración: `{ "FormName": "ScheduleDataRefresh", "FormDescription": "Form for data refresh schedule", "FormSmithyModel": "@amazon.datazone#displayname(defaultName: \"Data Refresh Schedule\")\nstructure ScheduleDataRefresh {\n @documentation(\"Schedule of Data Refresh\")\n @required\n @amazon.datazone#searchable\n @amazon.datazone#displayname(defaultName: \"Data Refresh Schedule\")\n data_refresh_schedule: String\n}" }`	Arquitecto e DevOps ingeniero de nube

Tarea	Descripción	Habilidades requeridas
Exporte las AWS credencia les.	Para exportar AWS las credenciales a su entorno de desarrollo para el rol de IAM con permisos administrativos, utilice el siguiente formato: `export AWS_ACCES S_KEY_ID= export AWS_SECRE T_ACCESS_KEY= export AWS_SESSI ON_TOKEN=`	Arquitecto de nube, ingeniero DevOps
Sintetice la plantilla.	Para sintetizar la CloudForm ation plantilla, ejecute el siguiente comando: `npx cdk synth`	Arquitecto de nube, ingeniero DevOps
Implemente la solución.	Ejecute el siguiente comando para implementar la solución: `npx cdk deploy --all`	Arquitecto de nube, DevOps ingeniero

Configuración de nuevas cuentas de miembros

Tarea	Descripción	Habilidades requeridas
Implemente la plantilla.	Implemente la CloudFormation plantilla ubicada `lib/cfn-templates/DzDataMes hCfnStackSetExecut ionRole.yaml` en la cuenta del miembro con los	Arquitecto de nube, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	siguientes parámetros de entrada: • `GovernanceAccountID` : ID de cuenta de la cuenta de gobernanza • `DataZoneKMSKeyID` – ID de la clave AWS Key Management Service (AWS KMS) que cifra los metadatos de Amazon DataZone • `NotificationQueueName` : nombre de la cola de notificaciones de Amazon SQS en la cuenta de gobernanza	
Actualice el ARNs.	Para actualizar la lista de funciones de CloudFormation StackSet ejecución ARNs de las cuentas de los miembros, utilice el siguiente código: `DZ_MEMBER_STACK_SET_EXEC_ROLE_LIST - List of Stack set execution role arns for the member accounts.`	Arquitecto de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Sintetice e implemente.	Para sintetizar la CloudFormation plantilla e implementar la solución, ejecute los siguientes comandos:
	`npx cdk synth`
	`npx cdk deploy --all`
		Arquitecto de nube, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
Asocie la cuenta de miembro	Para asociar la cuenta de miembro a la cuenta de gobernanza central, haga lo siguiente: 1. Inicia sesión en la consola de la cuenta de gobierno central y abre la DataZone consola de Amazon en https://console.aws.amazon.com/datazone/. 2. Seleccione el dominio que creó. 3. Desplácese hasta la pestaña Cuentas asociadas y elija Solicitar asociación. 4. Proporcione el ID de la cuenta de AWS y elija AWSRAMPermissionDataZonePortalReadWriteuna política de RAM. 5. Elija Solicitar asociación. 6. Espere a recibir una notificación por correo electrónico donde se indique que su cuenta se ha iniciado correctamente.	Arquitecto e DevOps ingeniero de nube

Tarea	Descripción	Habilidades requeridas
Actualice los parámetros.	Para actualizar los parámetros específicos de la cuenta de miembro en el archivo de configuración de `config/Config.ts`, utilice el siguiente formato: `export const DZ_MEMBER_ACCOUNT_CONFIG: memberAccountConfig = { '123456789012' : { PROJECT_NAME: 'TEST-PROJECT-123456789012', PROJECT_DESCRIPTION: 'TEST-PROJECT-123456789012', PROJECT_EMAIL: 'user@xyz.com' } }`	Arquitecto de nube, DevOps ingeniero

Sintetice e implemente la plantilla.	Para sintetizar la CloudFormation plantilla e implementar la solución, ejecute los siguientes comandos:
	`npx cdk synth`
	`npx cdk deploy --all`
		Arquitecto de nube, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
Agregue cuentas de miembro.	Para crear y configura r cuentas de miembros adicionales en la solución de datos, repita los pasos anteriores para cada cuenta de miembro. Esta solución no diferenci a entre productores y consumidores de datos.	Arquitecto de nube, DevOps ingeniero

Limpieza

Tarea	Descripción	Habilidades requeridas
Elimine la asociación de las cuentas de miembros.	Para desasociar las cuentas, haga lo siguiente: 1. Inicia sesión en la consola y abre la DataZone consola de Amazon. 2. Seleccione Ver dominios. 3. Seleccione el dominio que creó. 4. Seleccione la pestaña Asociaciones de cuentas. 5. Seleccione la cuenta de miembro que quiera desasociar. 6. Elija Desasociar e introduzc a `disassociate` para confirmar.	Arquitecto e DevOps ingeniero de nube

Tarea	Descripción	Habilidades requeridas
	7. Repita los pasos 3 a 6 para todas las cuentas de miembros.	

Tarea	Descripción	Habilidades requeridas
Elimine las instancias de pila.	Para eliminar las instancias de la CloudFormation pila, haga lo siguiente: 1. Abre la CloudFormation consola en https://console.aws.amazon.com/cloudformation/. 2. En el panel de navegación, elija StackSets. 3. Elija el conjunto de pilas denominado StackSet-DataZone - DataMesh - Member y elija la pestaña Instancias de pila. 4. Copia el Cuenta de AWS ID de la cuenta de miembro que quieres eliminar de la membresía. 5. Selecciona Acciones, selecciona Eliminar pilas de y StackSet conserva las opciones predeterminadas. 6. En el campo Números de cuenta, introduzca el ID de la cuenta. 7. En la lista desplegable Especificar regiones, elija Región de AWS. 8. Seleccione Siguiente y, a continuación, elija Enviar. 9. En la pestaña Operaciones, confirme que la	Arquitecto de nube, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	operación se haya realizado correctamente. La eliminación de la pila puede tardar algún tiempo. 10. Repita los pasos 2 a 9 para todas las cuentas de miembros.	
Elimine todos los recursos.	Para eliminar recursos, realice los siguientes pasos en su entorno de desarrollo local (Linux o macOS): 1. Vaya hasta la raíz del directorio de su repositorio. 2. Exporte las AWS credencia les del rol de IAM que utilizó para crear la AWS CDK pila. 3. Ejecute el siguiente comando para eliminar los recursos en la nube: `npx cdk destroy --all`	Arquitecto e ingeniero de nube DevOps

Recursos relacionados

- Guía de DataZone inicio rápido de Amazon con datos AWS Glue
- Tutorial: Crea tu primera aplicación AWS CDK
- ¿Cómo empezar con CloudFormation
- Estrategias para crear una solución empresarial basada en una malla de datos en AWS

Información adicional

Objetivos

Con la implementación de este patrón logrará lo siguiente:

- Propiedad descentralizada de los datos: traslade la propiedad de los datos de un equipo central a equipos que representen los sistemas de origen, las unidades de negocio o los casos de uso de su organización.
- Pensamiento dedicado al producto: introduzca una mentalidad basada en el producto que incluya a los clientes, el mercado y otros factores cuando tenga que considerar los activos de datos de su organización.
- Gobernanza federada: mejore las barreras de protección, los controles y la conformidad en todos los productos de datos de su organización.
- Soporte para varias cuentas y proyectos: ayuda para el intercambio de datos y la colaboración eficientes y seguros entre las unidades de negocio o los proyectos de su organización.
- Supervisión y notificaciones centralizadas: supervise los recursos en la nube de su red de datos mediante Amazon CloudWatch y notifique a los usuarios cuando se asocie una nueva cuenta de miembro.
- Escalabilidad y extensibilidad: añada nuevos casos de uso a la malla de datos a medida que su organización evoluciona.

Alcance de la solución

Al utilizar esta solución, puede empezar poco a poco y ampliarla a medida que avanza en su transición hacia la malla de datos. A menudo, cuando una cuenta de miembro adopta la solución de datos, esta contiene configuraciones de cuenta específicas para la organización, el proyecto o la unidad de negocio. Esta solución se adapta a estas diversas Cuenta de AWS configuraciones al admitir las siguientes funciones:

- AWS Glue Data Catalog como fuente de datos para Amazon DataZone
- Gestión del dominio de DataZone datos de Amazon y el portal de datos relacionado
- Administración de la adición de cuentas de miembros a la solución de datos basada en la malla de datos
- Gestión de DataZone proyectos y entornos de Amazon
- Gestión de los DataZone glosarios y formularios de metadatos de Amazon

- Administración de roles de IAM que corresponden a los usuarios de la solución de datos basada en la malla de datos
- Notificaciones para los usuarios de soluciones de datos basadas en la malla de datos
- Supervisión de la infraestructura en la nube aprovisionada

  Esta solución utiliza AWS CDK y despliega CloudFormation la infraestructura de la nube. Suele CloudFormation hacer lo siguiente:

  - Definir e implementar los recursos de la nube con un nivel de abstracción inferior.
  - Implemente recursos en la nube desde Consola de administración de AWS. Al utilizar este enfoque, puede implementar la infraestructura sin un entorno de desarrollo.

  La solución de malla de datos se utiliza AWS CDK para definir los recursos a un nivel de abstracción superior. Como resultado, la solución proporciona un enfoque desacoplado, modular y escalable al elegir la herramienta adecuada para implementar los recursos de la nube.

Pasos siguientes

Puedes ponerte en contacto con AWSexpertos para que te asesoren sobre cómo crear una malla de datos con Amazon DataZone.

La naturaleza modular de esta solución permite crear soluciones de administración de datos con diferentes arquitecturas, como tejidos y lagos de datos. Además, en función de los requisitos de su organización, puede extender la solución a otras fuentes de DataZone datos de Amazon.

Calcule el valor en riesgo (VaR) mediante los servicios de AWS

Sumon Samanta, Amazon Web Services

Resumen

Este patrón describe cómo implementar un sistema de cálculo del valor en riesgo (VaR) mediante los servicios de AWS. En un entorno en las instalaciones, la mayoría de los sistemas VaR emplean una gran infraestructura dedicada y un software de programación de redes interno o comercial para ejecutar procesos por lotes. Este patrón presenta una arquitectura simple, fiable y escalable para gestionar el procesamiento de VaR en la nube de AWS. Crea una arquitectura sin servidor que utiliza Amazon Kinesis Data Streams como servicio de streaming, Amazon Simple Queue Service (Amazon SQS) como servicio de colas gestionado ElastiCache , Amazon como servicio de almacenamiento en caché y AWS Lambda para procesar los pedidos y calcular el riesgo.

El VaR es una medida estadística que usan los operadores y gestores de riesgos para estimar las posibles pérdidas de su cartera más allá de cierto nivel de confianza. La mayoría de los sistemas VaR implican la ejecución de una gran cantidad de cálculos matemáticos y estadísticos, así como el almacenamiento de los resultados. Estos cálculos requieren importantes recursos de cómputo, por lo que los procesos por lotes del VaR deben dividirse en conjuntos más pequeños de tareas de computación. Es posible dividir un lote grande en tareas más pequeñas, ya que estas tareas son, en su mayoría, independientes (es decir, los cálculos de una tarea no dependen de otras tareas).

Otro requisito importante de una arquitectura de VaR es la escalabilidad de la computación. Este patrón emplea una arquitectura sin servidor que escala vertical u horizontalmente de manera automática en función de la carga de cálculo. Como la demanda de procesamiento por lotes o en línea es difícil de predecir, es necesario contar con un escalado dinámico para completar el proceso dentro del plazo impuesto por un acuerdo de nivel de servicio (SLA). Además, una arquitectura con costos optimizados debería poder reducir verticalmente la escala de cada recurso informático tan pronto como se completen las tareas de ese recurso.

Los servicios de AWS son adecuados para los cálculos de VaR, ya que ofrecen procesamiento y almacenamiento escalables, servicios de análisis para el procesamiento con costos optimizados y diferentes tipos de programadores para ejecutar los flujos de trabajo de administración de riesgos. Además, usted solo paga por los recursos de almacenamiento y computación que usa en AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Archivos de entrada, que dependen de las necesidades de su empresa. Un caso de uso típico incluye los siguientes archivos de entrada:
  - Archivo de datos de mercado (entrada al motor de cálculo del VaR)
  - Archivo de datos comerciales (a menos que los datos comerciales provengan de un flujo).
  - Archivo de datos de configuración (modelo y otros datos de configuración estáticos)
  - Archivos de modelo de motor de cálculo (bibliotecas cuantitativas)
  - Archivo de datos de serie temporal (para datos históricos, como el precio de las acciones de los últimos cinco años)
- Si los datos de mercado u otra entrada provienen de un flujo, permisos de Amazon Kinesis Data Streams y Amazon Identity and Access Management (IAM) configurados para escribir en dicho flujo.

Este patrón crea una arquitectura en la que los datos comerciales se escriben desde un sistema comercial a un flujo de datos de Kinesis. En lugar de usar un servicio de streaming, puede guardar sus datos comerciales en archivos de lotes pequeños, almacenarlos en un bucket de Amazon Simple Storage Service (Amazon S3) e invocar un evento para comenzar a procesar los datos.

Limitaciones

- La secuenciación del flujo de datos de Kinesis está garantizada en cada partición, por lo que no se garantiza que las órdenes comerciales que se escriben en varias particiones se entreguen en el mismo orden que las operaciones de escritura.
- Actualmente, el límite de tiempo de ejecución de AWS Lambda es de 15 minutos. (Para más información, consulte las Preguntas frecuentes sobre Lambda)

Arquitectura

Arquitectura de destino

El siguiente diagrama de arquitectura muestra los servicios y flujos de trabajo de AWS para el sistema de evaluación de riesgos.

En el siguiente diagrama se ilustra lo siguiente:

1. Las operaciones se transmiten desde el sistema de gestión de pedidos.
2. La función de Lambda de compensación de posiciones de tickets procesa los pedidos y escribe los mensajes consolidados de cada ticker en una cola de riesgos de Amazon SQS.
3. La función Lambda del motor de cálculo de riesgos procesa los mensajes de Amazon SQS, realiza cálculos de riesgo y actualiza la información de pérdidas y ganancias (PnL) del VaR en la caché de riesgos de Amazon. ElastiCache
4. La función Lambda de lectura de ElastiCache datos recupera los resultados del riesgo y los almacena en una base de datos ElastiCache y en un bucket de S3.

Para obtener más información sobre estos servicios y pasos, consulte la sección Épica.

Automatización y escala

Puede implementar toda la arquitectura mediante el Kit de desarrollo en la nube de AWS (AWS CDK) o las CloudFormation plantillas de AWS. La arquitectura es compatible tanto con procesamiento por lotes como con procesamiento intradiario (en tiempo real).

El escalado está integrado en la arquitectura. A medida que se escriban más operaciones en el flujo de datos de Kinesis y estén pendientes de ser procesadas, es posible invocar funciones de Lambda adicionales para procesar esas operaciones y, a continuación, reducir verticalmente una vez finalizado el procesamiento. El procesamiento mediante varias colas de cálculo de riesgos de Amazon SQS también es una opción. Si es necesario mantener un orden o consolidación estrictos en todas las colas, el procesamiento no se puede paralelizar. Sin embargo, para un end-of-the-day lote o un minilote intradía, las funciones Lambda pueden procesar en paralelo y almacenar los resultados finales en él. ElastiCache

Tools (Herramientas)

Servicios de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con MySQL y completamente administrado que le permite configurar, administrar y escalar implementaciones de MySQL. Este patrón emplea MySQL como ejemplo, pero puede usar cualquier sistema RDBMS para almacenar datos.
- Amazon le ElastiCache ayuda a configurar, gestionar y escalar entornos de caché en memoria distribuidos en la nube de AWS.

- Amazon Kinesis Data Streams le ayuda a recopilar y procesar grandes secuencias de registros de datos en tiempo real.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Código

Este patrón proporciona un ejemplo de arquitectura para un sistema de VaR en la nube de AWS y describe cómo usar las funciones de Lambda para cálculos de VaR. Para crear las funciones de Lambda, consulte los ejemplos de código en la documentación de Lambda. Para obtener ayuda, póngase en contacto con AWS Professional Services.

Prácticas recomendadas

- Intente que cada tarea de cómputo del VaR sea lo más pequeña y ligera posible. Experimente con diferentes números de operaciones en cada tarea de cómputo para optimizar al máximo el tiempo y costo del cómputo.
- Almacena objetos reutilizables en Amazon ElastiCache. Use un marco como Apache Arrow para reducir la serialización y la deserialización.
- Tenga en cuenta la limitación de tiempo de Lambda. Si cree que sus tareas de computación pueden superar los 15 minutos, intente dividirlas en tareas más pequeñas para evitar el tiempo de espera de Lambda. Si no es posible, considere una solución de orquestación de contenedores con AWS Fargate, Amazon Elastic Container Service (Amazon ECS) y Amazon Elastic Kubernetes Service (Amazon EKS).

Epics

Sistema de flujo comercial a riesgo

Tarea	Descripción	Habilidades requeridas
Comience a escribir operaciones.	Las operaciones nuevas, liquidadas o parcialmente liquidadas se escriben desde el sistema de gestión de pedidos a un flujo de riesgo. Este patrón usa Amazon Kinesis como servicio de flujo gestionado. El hash del ticker de la orden comercial se usa para colocar las órdenes comerciales en varias particiones.	Amazon Kinesis

Ejecute funciones de Lambda para el procesamiento de pedidos

Tarea	Descripción	Habilidades requeridas
Inicie el procesamiento de riesgos con Lambda.	Ejecute una función de AWS Lambda para los nuevos pedidos. En función del número de órdenes comerciales pendientes, Lambda escalará automáticamente. Cada instancia de Lambda tiene uno o más pedidos y recupera la última posición de cada ticker de Amazon. ElastiCache (Puede utilizar un identificador CUSIP, un nombre de curva o un nombre	Amazon Kinesis, AWS Lambda, Amazon ElastiCache

Tarea	Descripción	Habilidades requeridas
	de índice para otros productos derivados financieros como clave para almacenar y recuperar datos). ElasticCache En ElastiCache, la posición total (cantidad) y el par clave-valor < indicador , posición neta >, donde la posición neta es el factor de escala, se actualizan una vez para cada indicador.	

Escriba los mensajes de cada ticker en la cola

Tarea	Descripción	Habilidades requeridas
Escriba mensajes consolidados en la cola de riesgos.	Escriba el mensaje en una cola. Este patrón emplea Amazon SQS como servicio de colas gestionado. Una sola instancia de Lambda puede recibir un minilote de órdenes comerciales en un momento dado, pero solo escribirá un mensaje para cada ticker en Amazon SQS. Se calcula un factor de escala: (posición neta anterior + posición actual) / posición neta anterior.	Amazon SQS, AWS Lambda

Invoque el motor de riesgo

Tarea	Descripción	Habilidades requeridas
Inicie los cálculos de riesgo.	Se invoca la función de Lambda para el motor de riesgo Lambda. Cada posición es procesada por una sola función de Lambda. Sin embargo, con fines de optimización, cada función de Lambda puede procesar varios mensajes de Amazon SQS.	Amazon SQS, AWS Lambda

Recupere los resultados de riesgo de la memoria caché

Tarea	Descripción	Habilidades requeridas
Recupere y actualice la caché de riesgos.	Lambda recupera la posición neta actual de cada ticker de. ElastiCache También recupera una matriz de ganancias y pérdidas (pNL) de VaR para cada ticker de. ElastiCache Si la matriz pNL ya existe, la función de Lambda actualiza la matriz y el VaR con una escala que proviene del mensaje de Amazon SQS escrito por la función de Lambda de compensación. Si la matriz pNL no está incluida ElasticCache, se calculan un	Amazon SQS, AWS Lambda, Amazon ElastiCache

Tarea	Descripción	Habilidades requeridas
	pNL y un VaR nuevos utilizando datos simulados de series de precios de cotizadores.	

Actualice los datos en Elastic Cache y almacénelos en la base de datos

Tarea	Descripción	Habilidades requeridas
Almacene los resultados de riesgo.	Una vez actualizados los números VaR y PnL ElastiCache, se invoca una nueva función Lambda cada cinco minutos. Esta función lee todos los datos almacenados ElastiCache y los almacena en una base de datos compatible con Aurora MySQL y en un bucket de S3.	AWS Lambda, Amazon ElastiCache

Recursos relacionados

- Marco VaR de Basel

Configurar el acceso entre cuentas a un catálogo de datos de AWS Glue compartido con Amazon Athena

Denis Avdonin, Amazon Web Services

Resumen

Este patrón proporciona step-by-step instrucciones, incluidos ejemplos de políticas de AWS Identity and Access Management (IAM), para configurar el uso compartido entre cuentas de un conjunto de datos almacenado en un depósito de Amazon Simple Storage Service (Amazon S3) mediante el catálogo de datos de AWS Glue. Puede almacenar el conjunto de datos en un bucket de S3. Un rastreador de AWS Glue recopila los metadatos y los coloca en el catálogo de datos de AWS Glue. El bucket de S3 y el catálogo de datos de AWS Glue residen en una cuenta de AWS denominada cuenta de datos. Puede proporcionar acceso a las entidades principales de IAM en otra cuenta de AWS denominada cuenta de consumidor. Los usuarios pueden consultar los datos de la cuenta del consumidor mediante el motor de consultas sin servidor Amazon Athena.

Requisitos previos y limitaciones

Requisitos previos

- Dos cuentas de AWS activas
- Un bucket de S3 en una de las cuentas de AWS
- Versión 2 del motor Athena
- Interfaz de línea de comandos de AWS (AWS CLI), instalada y configurada (o CloudShellAWS para ejecutar comandos de la CLI de AWS)

Versiones de producto

Este patrón solo funciona con la versión 2 del motor Athena y la versión 3 del motor Athena. Le recomendamos que actualice a la versión 3 del motor Athena. Si no puede actualizar de la versión 1 del motor Athena a la versión 3, siga el enfoque de Acceso entre cuentas al catálogo de datos de AWS Glue con Amazon Athena en el blog sobre macrodatos de AWS.

Arquitectura

Pila de tecnología de destino

- Amazon Athena
- Amazon Simple Storage Service (Amazon S3)
- AWS Glue
- AWS Identity y Access Management (IAM)
- AWS Key Management Service (AWS KMS)

El siguiente diagrama muestra una arquitectura que usa permisos de IAM para compartir datos de un bucket de S3 en una cuenta de AWS (cuenta de datos) con otra cuenta de AWS (cuenta de consumidor) a través del catálogo de datos de AWS Glue.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. La política de bucket de S3 de la cuenta de datos concede permisos a un rol de IAM en la cuenta de consumidor y al rol de servicio de rastreador de AWS Glue en la cuenta de datos.
2. La clave de AWS KMS de la cuenta de datos concede permisos a un rol de IAM en la cuenta de consumidor y al rol de servicio de rastreador de AWS Glue en la cuenta de datos.
3. El rastreador AWS Glue de la cuenta de datos descubre el esquema de los datos que están almacenados en el bucket de S3.
4. La política de recursos del catálogo de datos de AWS Glue de la cuenta de datos otorga acceso al rol de IAM en la cuenta del consumidor.
5. Un usuario crea una referencia de catálogo con nombre en la cuenta del consumidor mediante un comando de la CLI de AWS.
6. Una política de IAM otorga a un rol de IAM en la cuenta del consumidor el acceso a los recursos de la cuenta de datos. La siguiente política de confianza del rol de IAM permite a los usuarios de la cuenta de consumidor asumir un rol de IAM.
7. Un usuario de la cuenta de consumidor asume el rol de IAM y accede a los objetos del catálogo de datos mediante consultas SQL.
8. El motor sin servidor Athena ejecuta las consultas SQL.

> **Note**
>
> Las prácticas recomendadas de IAM recomiendan conceder permisos a un rol de IAM y utilizar la federación de identidades.

Tools (Herramientas)

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.

Epics

Configura los permisos en la cuenta de datos

Tarea	Descripción	Habilidades requeridas
Conceder acceso a los datos al bucket de S3.	Cree una política de bucket de S3 basada en la siguiente plantilla y asígnela al bucket en el que se almacenan los datos. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": [ "arn:aws:iam::<con`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas

	sumer account id>:role/
	<role name>",
	
	"arn:aws:iam::<dat
	a account id>:role/
	service-role/AWSGl
	ueServiceRole-data-
	bucket-crawler"
	]
	},
	"Action":
	"s3:GetObject",
	"Resource":
	"arn:aws:s3:::data-
	bucket/*"
	},
	{
	"Effect":
	"Allow",
	"Principa
	l": {
	"AWS": [
	
	"arn:aws:iam::<con
	sumer account id>:role/
	<role name>",
	
	"arn:aws:iam::<dat
	a account id>:role/
	service-role/AWSGl
	ueServiceRole-data-
	bucket-crawler"
	]
	},
	"Action":
	"s3:ListBucket",
	"Resource":
	"arn:aws:s3:::data-
	bucket"
	}
	]	

Tarea	Descripción	Habilidades requeridas
	<pre>}</pre> La política de bucket concede permisos a un rol de IAM en la cuenta de consumidor y al rol de servicio de rastreador de AWS Glue en la cuenta de datos.	

Tarea	Descripción	Habilidades requeridas
(Si es necesario) Conceda acceso a la clave de cifrado de datos.	Si el bucket de S3 está cifrado con una clave de AWS KMS, conceda el permiso `kms:Decrypt` sobre la clave al rol de IAM en la cuenta del consumidor y al rol de servicio de rastreador de AWS Glue en la cuenta de datos. Actualice la política de claves con la siguiente declaración: `{ "Effect": "Allow", "Principal": { "AWS": [ "arn:aws:iam::<consumer account id>:role/<role name>", "arn:aws:iam::<data account id>:role/service-role/AWSGlueServiceRole-data-bucket-crawler" ] }, "Action": "kms:Decrypt", "Resource": "arn:aws:kms:<region>:<data account id>:key/<key id>" }`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Conceda al rastreador acceso a los datos.	Adjunte la siguiente política de IAM al rol de servicio del rastreador: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::data-bucket/*" }, { "Effect": "Allow", "Action": "s3:ListBucket", "Resource": "arn:aws:s3:::data-bucket" } ] }`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
(Si es necesario) Conceda acceso al rastreador a la clave de cifrado de datos.	Si el bucket de S3 está cifrado mediante una clave de AWS KMS, conceda el permiso `kms:Decrypt` sobre la clave al rol de servicio de rastreador adjuntándole la siguiente política: `{ "Effect": "Allow", "Action": "kms:Decrypt", "Resource": "arn:aws:kms:<region>:<data account id>:key/<key id>" }`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Conceda el rol de IAM en la cuenta del consumidor y al rastreador el acceso al catálogo de datos.	1. Inicie sesión en la consola de administración de AWS y abra la consola de AWS Glue. 2. En el panel de navegación, en Data Catalog (Catálogo de datos), elija Settings (Configuración). 3. En la sección Permissio ns (Permisos), añada la siguiente declaración y, a continuación, seleccione Save (Guardar). `{ "Version" : "2012-10-17", "Statement" : [ { "Effect" : "Allow", "Principa l" : { "AWS" : [ "arn:aws:iam::<con sumer account id>:role/ <role name>", "arn:aws:iam::<dat a account id>:role/ service-role/AWSGl ueServiceRole-data- bucket-crawler" ] }, ...`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	<pre>"Action" : "glue:*", "Resource" : ["arn:aws:glue:<region>:<data account id>:catalog", "arn:aws:glue:<region>:<data account id>:database/*", "arn:aws:glue:<region>:<data account id>:table/*"] }] }</pre> Esta política permite realizar todas las acciones de AWS Glue en todas las bases de datos y tablas de la cuenta de datos. Puede personalizar la política para conceder únicamente los permisos necesarios a las entidades principales consumidoras. Por ejemplo, puede proporcionar acceso de solo lectura a tablas o vistas específicas de una base de datos.	

Acceda a los datos de la cuenta de consumidor

Tarea	Descripción	Habilidades requeridas
Cree una referencia con nombre para el catálogo de datos.	Para crear una referencia de catálogo de datos con nombre, utilice CloudShell o una AWS CLI instalada localmente para ejecutar el siguiente comando: `aws athena create-data-catalog --name <shared catalog name> --type GLUE --parameters catalog-id=<data account id>`	Administrador de la nube
Conceder acceso a los datos al rol de IAM en la cuenta del consumidor.	Adjunte la siguiente política al rol de IAM en la cuenta de consumidor para conceder al rol acceso entre cuentas a los datos: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::data-bucket/*" }, { "Effect": "Allow",`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	<pre>"Action": "s3:ListBucket", "Resource": "arn:aws:s3:::data-bucket" }, { "Effect": "Allow", "Action": "glue:*", "Resource": ["arn:aws:glue:<region>:<data account id>:catalog", "arn:aws:glue:<region>:<data account id>:database/*", "arn:aws:glue:<region>:<data account id>:table/*"] }] }</pre> A continuación, utilice la siguiente plantilla para especificar qué usuarios pueden aceptar el rol de IAM en su política de confianza: <pre>{ "Version": "2012-10-17", "Statement": [</pre>	

Tarea	Descripción	Habilidades requeridas

	<pre>{
	"Effect": "Allow",
	"Principal": {
	"AWS": "arn:aws:iam::<consumer account id>:user/<IAM user>"
	},
	"Action": "sts:AssumeRole"
	}
	]
	}</pre>
	Por último, conceda permisos a los usuarios para que asuman el rol de IAM adjuntando la misma política al grupo de usuarios al que pertenecen.	

Tarea	Descripción	Habilidades requeridas
(Si es necesario) Conceda acceso a la clave de cifrado de datos al rol de IAM en la cuenta del consumidor.	Si el bucket de S3 está cifrado mediante una clave de AWS KMS, conceda el permiso `kms:Decrypt` sobre la clave al rol de IAM en la cuenta de consumidor adjuntándole la siguiente política: `{ "Effect": "Allow", "Action": "kms:Decrypt", "Resource": "arn:aws:kms:<region>:<data account id>:key/<key id>" }`	Administrador de la nube
Cambie al rol de IAM en la cuenta del consumidor para acceder a los datos.	Cambie al rol de IAM en la cuenta del consumidor para acceder a los datos.	Consumidor de datos

Tarea	Descripción	Habilidades requeridas

Acceda a los datos.	Realizar consultas mediante Athena. Por ejemplo, abra el editor de consultas de Athena y ejecute la siguiente consulta:
	`SELECT * FROM <shared catalog name>.<database name>.<table name>`
	En lugar de utilizar una referencia de catálogo con nombre, también puede hacer referencia al catálogo por su nombre de recurso de Amazon (ARN).
	Note
	Si utiliza una referencia de catálogo dinámica en una consulta o vista, ponga la referencia entre comillas dobles escapadas (\"). Por ejemplo:
	`SELECT * FROM \"glue:arn:aws:glue:<region>:<data account id>:catalog\".<database name>.<table name>`
		Consumidor de datos

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte Acceso entre cuentas a los catálogos de datos de AWS Glue en la Guía del usuario de Amazon Athena.	

Recursos relacionados

- Acceso entre cuentas a los catálogos de datos de AWS Glue (documentación de Athena)
- (AWS CLI) create-data-catalog (Referencia de comandos de la CLI de AWS)
- Acceso entre cuentas al catálogo de datos de AWS Glue con Amazon Athena (blog sobre macrodatos de AWS)
- Prácticas recomendadas de seguridad en IAM (documentación de IAM)

Información adicional

Uso de Lake Formation como alternativa para compartir entre cuentas

También puede usar AWS Lake Formation para compartir el acceso a los objetos del catálogo de AWS Glue entre cuentas. Lake Formation proporciona un control de acceso detallado a nivel de columnas y filas, control de acceso basado en etiquetas, tablas gobernadas para transacciones ACID y otras funciones. Aunque Lake Formation está bien integrado con Athena, requiere una configuración adicional en comparación con el enfoque exclusivo de IAM de este patrón. Recomendamos que considere la decisión de utilizar los controles de acceso exclusivos de Lake Formation o IAM en el contexto más amplio de la arquitectura general de su solución. Las consideraciones incluyen qué otros servicios están involucrados y cómo se integran con ambos enfoques.

Convierta la característica temporal NORMALIZE de Teradata en Amazon Redshift SQL

Po Hong, Amazon Web Services

Resumen

NORMALIZE es una extensión de Teradata del estándar ANSI SQL. Cuando una tabla SQL incluye una columna que tiene un tipo de datos tipo PERIOD, NORMALIZE combina los valores que coinciden o se superponen en esa columna para formar un período único que consolida varios valores de períodos individuales. Para utilizar NORMALIZE, al menos una columna de la lista SQL SELECT debe ser del tipo de datos PERIOD temporal de Teradata. Para obtener más información sobre NORMALIZE, consulte la documentación de Teradata.

Amazon Redshift no admite NORMALIZE, pero puede implementar esta funcionalidad mediante la sintaxis SQL nativa y la función de ventana LAG en Amazon Redshift. Este patrón se centra en el uso de la extensión NORMALIZE de Teradata con la condición ON MEETS OR OVERLAPS, que es el formato más popular. En él se explica cómo funciona esta función en Teradata y cómo se puede convertir a la sintaxis SQL nativa de Amazon Redshift.

Requisitos previos y limitaciones

Requisitos previos

- Conocimientos y experiencia básicos de Teradata SQL
- Conocimiento y experiencia en Amazon Redshift

Arquitectura

Pila de tecnología de origen

- Almacenamiento de datos de Teradata

Pila de tecnología de destino

- Amazon Redshift

Arquitectura de destino

Para obtener una arquitectura de alto nivel para migrar una base de datos de Teradata a Amazon Redshift, consulte el patrón Migración de una base de datos de Teradata a Amazon Redshift mediante agentes de extracción de datos SCT de AWS. La migración no convierte automáticamente la frase NORMALIZE de Teradata en Amazon Redshift SQL. Puede convertir esta extensión de Teradata siguiendo las pautas de este patrón.

Tools (Herramientas)

Código

Para ilustrar el concepto y la funcionalidad de NORMALIZE, considere la siguiente definición de tabla en Teradata:

```
CREATE TABLE systest.project
     (    emp_id        INTEGER,
          project_name  VARCHAR(20),
          dept_id       INTEGER,
          duration      PERIOD(DATE)
     );
```

Ejecute el siguiente código SQL para insertar datos de ejemplo en la tabla:

```
BEGIN TRANSACTION;

INSERT INTO systest.project VALUES (10, 'First Phase', 1000,  PERIOD(DATE '2010-01-10',
 DATE '2010-03-20') );
INSERT INTO systest.project VALUES (10, 'First Phase', 2000,  PERIOD(DATE '2010-03-20',
 DATE '2010-07-15') );

INSERT INTO systest.project VALUES (10, 'Second Phase', 2000,  PERIOD(DATE
 '2010-06-15', DATE '2010-08-18') );
INSERT INTO systest.project VALUES (20, 'First Phase', 2000,  PERIOD(DATE '2010-03-10',
 DATE '2010-07-20') );

INSERT INTO systest.project VALUES (20, 'Second Phase', 1000,  PERIOD(DATE
 '2020-05-10', DATE '2020-09-20') );

END TRANSACTION;
```

Resultados:

```
select * from systest.project order by 1,2,3;
```

```
 *** Query completed. 4 rows found. 4 columns returned.
 *** Total elapsed time was 1 second.

     emp_id  project_name              dept_id  duration
-----------  --------------------  -----------  ------------------------
         10  First Phase                  1000  ('10/01/10', '10/03/20')
         10  First Phase                  2000  ('10/03/20', '10/07/15')
         10  Second Phase                 2000  ('10/06/15', '10/08/18')
         20  First Phase                  2000  ('10/03/10', '10/07/20')
         20  Second Phase                 1000  ('20/05/10', '20/09/20')
```

Caso de uso de Teradata NORMALIZE

Ahora añada la cláusula SQL NORMALIZE de Teradata a la sentencia SELECT::

```
SELECT NORMALIZE ON MEETS OR OVERLAPS emp_id, duration
FROM systest.project
ORDER BY 1,2;
```

Esta operación NORMALIZE se realiza en una sola columna (`emp_id`). En este `emp_id=10` caso, los tres valores de período superpuestos en cuanto a la duración se fusionan en un único valor de período, de la siguiente manera:

```
     emp_id  duration
-----------  ------------------------
         10  ('10/01/10', '10/08/18')
         20  ('10/03/10', '10/07/20')
         20  ('20/05/10', '20/09/20')
```

La siguiente instrucción SELECT realiza una operación NORMALIZE en `project_name` y. `dept_id` Tenga en cuenta que la lista SELECT contiene solo una columna PERIOD,`duration`.

```
SELECT NORMALIZE project_name, dept_id, duration
FROM systest.project;
```

Salida:

```
project_name              dept_id  duration
--------------------  -----------  ------------------------
```

```
First Phase                  1000  ('10/01/10', '10/03/20')
Second Phase                 1000  ('20/05/10', '20/09/20')
First Phase                  2000  ('10/03/10', '10/07/20')
Second Phase                 2000  ('10/06/15', '10/08/18')
```

SQL equivalente a Amazon Redshift

Amazon Redshift actualmente no admite el tipo de datos PERIOD en una tabla. En su lugar, debe dividir un campo de datos PERIOD de Teradata en dos partes:`start_date, end_date`, de la siguiente manera:

```
CREATE TABLE systest.project
     (    emp_id        INTEGER,
          project_name  VARCHAR(20),
          dept_id       INTEGER,
          start_date  DATE,
          end_date    DATE
     );
```

Inserte una fila de datos en la tabla:

```
BEGIN TRANSACTION;

INSERT INTO systest.project VALUES (10, 'First Phase', 1000,  DATE '2010-01-10', DATE
 '2010-03-20' );
INSERT INTO systest.project VALUES (10, 'First Phase', 2000,  DATE '2010-03-20', DATE
 '2010-07-15');

INSERT INTO systest.project VALUES (10, 'Second Phase', 2000,  DATE '2010-06-15', DATE
 '2010-08-18' );
INSERT INTO systest.project VALUES (20, 'First Phase', 2000,  DATE '2010-03-10', DATE
 '2010-07-20' );

INSERT INTO systest.project VALUES (20, 'Second Phase', 1000,  DATE '2020-05-10', DATE
 '2020-09-20' );

END TRANSACTION;
```

Salida:

```
 emp_id | project_name | dept_id | start_date |  end_date
--------+--------------+---------+------------+------------
```

```
     10 | First Phase  |    1000 | 2010-01-10 | 2010-03-20
     10 | First Phase  |    2000 | 2010-03-20 | 2010-07-15
     10 | Second Phase |    2000 | 2010-06-15 | 2010-08-18
     20 | First Phase  |    2000 | 2010-03-10 | 2010-07-20
     20 | Second Phase |    1000 | 2020-05-10 | 2020-09-20
(5 rows)
```

Para reescribir la cláusula NORMALIZE de Teradata, puede utilizar la función de ventana LAG de Amazon Redshift. Esta función devuelve los valores para una fila en un desplazamiento dado arriba (antes) de la fila actual en la partición.

Puede usar la función LAG para identificar cada fila que comienza un nuevo período determinando si un período coincide o se superpone con el período anterior (0 en caso afirmativo y 1 en caso negativo). Cuando este indicador se suma de forma acumulativa, proporciona un identificador de grupo que se puede utilizar en la cláusula externa Group By para obtener el resultado deseado en Amazon Redshift.

A continuación, se muestra un ejemplo de sentencia SQL de Amazon Redshift que utiliza LAG():

```
SELECT emp_id, start_date, end_date,
            (CASE WHEN start_date <= LAG(end_date) OVER (PARTITION BY emp_id ORDER BY
 start_date, end_date) THEN 0 ELSE 1 END) AS GroupStartFlag
FROM systest.project
ORDER BY 1,2;
```

Salida:

```
 emp_id | start_date |  end_date  | groupstartflag
--------+------------+------------+----------------
     10 | 2010-01-10 | 2010-03-20 |              1
     10 | 2010-03-20 | 2010-07-15 |              0
     10 | 2010-06-15 | 2010-08-18 |              0
     20 | 2010-03-10 | 2010-07-20 |              1
     20 | 2020-05-10 | 2020-09-20 |              1
(5 rows)
```

La siguiente sentencia SQL de Amazon Redshift solo se normaliza en la columna: `emp_id`

```
SELECT T2.emp_id, MIN(T2.start_date) as new_start_date, MAX(T2.end_date) as
 new_end_date
FROM
```

```
( SELECT T1.*, SUM(GroupStartFlag) OVER (PARTITION BY emp_id ORDER BY start_date ROWS
 UNBOUNDED PRECEDING) As GroupID
FROM ( SELECT emp_id, start_date, end_date,
            (CASE WHEN start_date <= LAG(end_date) OVER (PARTITION BY emp_id ORDER BY
 start_date, end_date) THEN 0 ELSE 1 END) AS GroupStartFlag
FROM systest.project ) T1
) T2
GROUP BY T2.emp_id, T2.GroupID
ORDER BY 1,2;
```

Salida:

```
 emp_id | new_start_date | new_end_date
--------+----------------+----------------------------------
     10 | 2010-01-10     | 2010-08-18
     20 | 2010-03-10     | 2010-07-20
     20 | 2020-05-10     | 2020-09-20
(3 rows)
```

La siguiente sentencia SQL de Amazon Redshift se normaliza en las columnas y: `project_name` `dept_id`

```
SELECT T2.project_name, T2.dept_id, MIN(T2.start_date) as new_start_date,
 MAX(T2.end_date) as new_end_date
FROM
( SELECT T1.*, SUM(GroupStartFlag) OVER (PARTITION BY project_name, dept_id ORDER BY
 start_date ROWS UNBOUNDED PRECEDING) As GroupID
FROM ( SELECT project_name, dept_id, start_date, end_date,
            (CASE WHEN start_date <= LAG(end_date) OVER (PARTITION BY project_name,
 dept_id ORDER BY start_date, end_date) THEN 0 ELSE 1 END) AS GroupStartFlag
FROM systest.project ) T1
) T2
GROUP BY T2.project_name, T2.dept_id, T2.GroupID
ORDER BY 1,2,3;
```

Salida:

```
 project_name | dept_id | new_start_date | new_end_date
--------------+---------+----------------+--------------
 First Phase  |    1000 | 2010-01-10     | 2010-03-20
```

```
 First Phase  |    2000 | 2010-03-10     | 2010-07-20
 Second Phase |    1000 | 2020-05-10     | 2020-09-20
 Second Phase |    2000 | 2010-06-15     | 2010-08-18
(4 rows)
```

Epics

Convierta NORMALIZE en Amazon Redshift SQL

Tarea	Descripción	Habilidades requeridas
Cree código SQL en Teradata.	Use la frase NORMALIZE en función de sus necesidades.	Desarrollador SQL
Convierta el código a Amazon Redshift SQL.	Para convertir el código, siga las instrucciones de la sección «Herramientas» de este patrón.	Desarrollador SQL
Ejecute el código en Amazon Redshift.	Cree la tabla, cargue los datos en la tabla y ejecute el código en Amazon Redshift.	Desarrollador SQL

Recursos relacionados

Referencias

- Característica temporal NORMALIZE de Teradata (documentación de Teradata)
- Función de ventana LAG (documentación de Amazon Redshift)
- Migración a Amazon Redshift (sitio web de AWS)
- Migración de una base de datos de Teradata a Amazon Redshift con los agentes de extracción de datos de AWS SCT (Recomendaciones de AWS)
- Convertir la característica RESET WHEN de Teradata a Amazon Redshift SQL (Recomendaciones de AWS)

Herramientas

- Herramienta de conversión de esquemas de AWS (AWS SCT)

Socios

- Socios con competencias en migración de AWS

Convierta la característica RESET WHEN de Teradata en Amazon Redshift SQL

Po Hong, Amazon Web Services

Resumen

RESET WHEN es una característica de Teradata que se utiliza en las funciones de la ventana analítica de SQL. Es una extensión del estándar ANSI SQL. RESET WHEN determina la partición sobre la que opera una función de ventana SQL basada en alguna condición específica. Si la condición se evalúa como TRUE, se crea una nueva subpartición dinámica dentro de la partición de ventana existente. Para obtener más información acerca de RESET WHEN, consulte la documentación de Teradat.

Amazon Redshift no admite RESET WHEN en las funciones de ventana de SQL. Para implementar esta funcionalidad, debe convertir RESET WHEN a la sintaxis SQL nativa de Amazon Redshift y utilizar varias funciones anidadas. Este patrón demuestra cómo puede utilizar lacaracterística RESET WHEN de Teradata y cómo puede convertirla a la sintaxis SQL de Amazon Redshift.

Requisitos previos y limitaciones

Requisitos previos

- Conocimientos básicos del almacén de datos de Teradata y su sintaxis SQL
- Buen conocimiento de Amazon Redshift y su sintaxis SQL

Arquitectura

Pila de tecnología de origen

- Almacenamiento de datos de Teradata

Pila de tecnología de destino

- Amazon Redshift

Arquitectura

Para obtener una arquitectura de alto nivel para migrar una base de datos de Teradata a Amazon Redshift, consulte el patrón Migración de una base de datos de Teradata a Amazon Redshift mediante agentes de extracción de datos SCT de AWS. La migración no convierte automáticamente la frase RESET WHEN de Teradata en Amazon Redshift SQL. Puede convertir esta extensión de Teradata siguiendo las pautas de la siguiente sección.

Tools (Herramientas)

Código

Para ilustrar el concepto de RESET WHEN, considere la siguiente definición de tabla en Teradata:

```
create table systest.f_account_balance
( account_id integer NOT NULL,
  month_id integer,
  balance integer )
unique primary index (account_id, month_id);
```

Ejecute el siguiente código SQL para insertar datos de ejemplo en la tabla:

```
BEGIN TRANSACTION;
Insert Into systest.f_account_balance values (1,1,60);
Insert Into systest.f_account_balance values (1,2,99);
Insert Into systest.f_account_balance values (1,3,94);
Insert Into systest.f_account_balance values (1,4,90);
Insert Into systest.f_account_balance values (1,5,80);
Insert Into systest.f_account_balance values (1,6,88);
Insert Into systest.f_account_balance values (1,7,90);
Insert Into systest.f_account_balance values (1,8,92);
Insert Into systest.f_account_balance values (1,9,10);
Insert Into systest.f_account_balance values (1,10,60);
Insert Into systest.f_account_balance values (1,11,80);
Insert Into systest.f_account_balance values (1,12,10);
END TRANSACTION;
```

La tabla de muestra tiene los siguientes datos:

account_id	month_id	balance
1	1	60

1	2	99
1	3	94
1	4	90
1	5	80
1	6	88
1	7	90
1	8	92
1	9	10
1	10	60
1	11	80
1	12	10

Para cada cuenta, digamos que desea analizar la secuencia de aumentos de saldo mensuales consecutivos. Cuando el saldo de un mes es inferior o igual al saldo del mes anterior, es necesario restablecer el contador a cero y reiniciarlo.

Teradata se restablece en caso de uso

Para analizar estos datos, Teradata SQL utiliza una función de ventana con un agregado anidado y una frase RESET WHEN, de la siguiente manera:

```
SELECT account_id, month_id, balance,
 ( ROW_NUMBER() OVER (PARTITION BY account_id ORDER BY month_id
RESET WHEN balance <= SUM(balance) over (PARTITION BY account_id ORDER BY month_id ROWS
 BETWEEN 1 PRECEDING AND 1 PRECEDING) ) -1 ) as balance_increase
FROM systest.f_account_balance
ORDER BY 1,2;
```

Salida:

account_id	month_id	balance	balance_increase
1	1	60	0
1	2	99	1
1	3	94	0
1	4	90	0
1	5	80	0
1	6	88	1
1	7	90	2.
1	8	92	3
1	9	10	0
1	10	60	1
1	11	80	2.
1	12	10	0

La consulta se procesa de la siguiente manera en Teradata:

1. La función de agregado SUM (saldo) calcula la suma de todos los saldos de una cuenta determinada en un mes determinado.
2. Comprobamos si el saldo de un mes determinado (para una cuenta determinada) es superior al saldo del mes anterior.
3. Si el saldo aumentó, registramos un valor de recuento acumulado. Si la condición RESET WHEN se evalúa como false, lo que significa que el saldo ha aumentado durante meses sucesivos, seguiremos aumentando el recuento.
4. La función analítica ordenada ROW_NUMBER () calcula el valor del recuento. Cuando llegamos a un mes cuyo saldo es inferior o igual al saldo del mes anterior, la condición RESET WHEN se evalúa como verdadera. Si es así, iniciamos una nueva partición y ROW_NUMBER () reinicia el

conteo desde 1. Usamos FILAS ENTRE 1 ANTERIOR Y 1 ANTERIOR para acceder al valor de la fila anterior.

5. Restamos 1 para asegurarnos de que el valor del recuento comience por 0.

SQL equivalente a Amazon Redshift

Amazon Redshift no admite la frase RESET WHEN en una función de ventana analítica de SQL. Para obtener el mismo resultado, debe reescribir el SQL de Teradata con la sintaxis SQL nativa de Amazon Redshift y las subconsultas anidadas, de la siguiente manera:

```
SELECT account_id, month_id, balance,
   (ROW_NUMBER() OVER(PARTITION BY account_id, new_dynamic_part ORDER BY month_id) -1)
 as balance_increase
FROM
( SELECT account_id, month_id, balance, prev_balance,
SUM(dynamic_part) OVER (PARTITION BY account_id ORDER BY month_id ROWS BETWEEN
 UNBOUNDED PRECEDING AND CURRENT ROW) As new_dynamic_part
FROM ( SELECT account_id, month_id, balance,
SUM(balance) over (PARTITION BY account_id ORDER BY month_id ROWS BETWEEN 1 PRECEDING
 AND 1 PRECEDING) as prev_balance,
(CASE When balance <= prev_balance Then 1 Else 0 END) as dynamic_part
FROM systest.f_account_balance ) A
) B
ORDER BY 1,2;
```

Como Amazon Redshift no admite funciones de ventana anidadas en la cláusula SELECT de una sola sentencia SQL, debe utilizar dos subconsultas anidadas.

- En la subconsulta interna (alias A), se crea y rellena un indicador de partición dinámica (dynamic_part). dynamic_part se establece en 1 si el saldo de un mes es inferior o igual al saldo del mes anterior; de lo contrario, se establece en 0.
- En la siguiente capa (alias B), se genera un atributo new_dynamic_part como resultado de unacaracterística de ventana SUM.
- Por último, añada new_dynamic_part como un nuevo atributo de partición (partición dinámica) al atributo de partición existente (account_id) y aplique la misma función de ventana ROW_NUMBER() que en Teradata (y menos una).

Tras estos cambios, Amazon Redshift SQL genera el mismo resultado que Teradata.

Epics

Convierta RESET WHEN en Amazon Redshift SQL

Tarea	Descripción	Habilidades requeridas
Cree su función de ventana de Teradata.	Use agregados anidados y la frase RESET WHEN de acuerdo con sus necesidades.	Desarrollador SQL
Convierta el código a Amazon Redshift SQL.	Para convertir el código, siga las instrucciones de la sección «Herramientas» de este patrón.	Desarrollador SQL
Ejecute el código en Amazon Redshift.	Cree la tabla, cargue los datos en la tabla y ejecute el código en Amazon Redshift.	Desarrollador SQL

Recursos relacionados

Referencias

- Frase RESET WHEN (Documentación Teradata)
- Explicación de RESET WHEN (Stack Overflow)
- Migración a Amazon Redshift (sitio web de AWS)
- Migración de una base de datos de Teradata a Amazon Redshift con los agentes de extracción de datos de AWS SCT (Recomendaciones de AWS)
- Convierta la función temporal NORMALIZE de Teradata en Amazon Redshift SQL (AWS Prescriptive Guidance)

Herramientas

- Herramienta de conversión de esquemas de AWS (AWS SCT)

Socios

- Socios con competencias en migración de AWS

Implementar y administrar un lago de datos sin servidor en la nube de AWS mediante el uso de la infraestructura como código

Kirankumar Chandrashekar y Abdel Jaidi, Amazon Web Services

Resumen

Este patrón describe cómo utilizar la computación sin servidor y la infraestructura como código (IaC) para implementar y administrar un lago de datos en la nube de Amazon Web Services (AWS). Este patrón se basa en el taller sobre el marco de lago de datos sin servidor (SDLF) desarrollado por AWS.

El SDLF es un conjunto de recursos reutilizables que aceleran la entrega de lagos de datos empresariales en la nube de AWS y permiten una implementación más rápida en la producción. Se utiliza para implementar la estructura fundamental de un lago de datos siguiendo las prácticas recomendadas.

SDLF implementa un proceso de integración e implementación continuas (CI/CD) durante todo el despliegue del código y la infraestructura mediante servicios de AWS como AWS, CodePipeline AWS CodeBuild y AWS. CodeCommit

Este patrón utiliza varios servicios sin servidor de AWS para simplificar la administración de los lagos de datos. Entre ellas se incluyen Amazon Simple Storage Service (Amazon S3) y Amazon DynamoDB para el almacenamiento, AWS Lambda y AWS Glue para la informática, y Amazon Events, Amazon Simple Queue Service (Amazon SQS) CloudWatch y AWS Step Functions para la orquestación.

AWS CloudFormation y los servicios de código de AWS actúan como capa IaC para proporcionar implementaciones rápidas y reproducibles con operaciones y administración sencillas.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada.
- Un cliente Git, instalado y configurado.
- El taller de SDLF, abierto en la ventana de un navegador web y listo para usar.

Arquitectura

El diagrama de arquitectura ilustra un proceso basado en eventos con los siguientes pasos.

1. Tras añadir un archivo al bucket de datos sin procesar de S3, se coloca una notificación de evento de Amazon S3 en una cola de SQS. Cada notificación se entrega como un archivo JSON, que contiene metadatos como el nombre del bucket de S3, la clave del objeto o la marca de tiempo.
2. Esta notificación la consume una función de Lambda que enruta el evento al proceso correcto de extracción, transformación y carga (ETL) en función de los metadatos. La función de Lambda también puede usar configuraciones contextuales almacenadas en una tabla de Amazon DynamoDB. Este paso permite desacoplar y escalar múltiples aplicaciones en el lago de datos.
3. El evento se dirige a la primera función de Lambda del proceso ETL, que transforma y mueve los datos del área de datos sin procesar al área de almacenamiento del lago de datos. El primer paso es actualizar el catálogo completo. Se trata de una tabla de DynamoDB que contiene todos los metadatos de archivos del lago de datos. Cada fila de esta tabla contiene metadatos operativos sobre un único objeto almacenado en Amazon S3. Se realiza una llamada sincrónica a una función de Lambda que realiza una ligera transformación, que es una operación económica desde el punto de vista computacional (como convertir un archivo de un formato a otro), en el objeto S3. Como se ha agregado un objeto nuevo al bucket provisional de S3, se actualiza el catálogo completo y se envía un mensaje a la cola de SQS a la espera de la siguiente fase de ETL.
4. Una regla de CloudWatch eventos activa una función Lambda cada 5 minutos. Esta función comprueba si los mensajes de la fase ETL anterior se enviaron a la cola de SQS. Si se ha entregado un mensaje, la función de Lambda inicia la segunda función desde AWS Step Functions en el proceso ETL.
5. A continuación, se aplica una transformación profunda a un lote de archivos. Esta importante transformación es una operación costosa desde el punto de vista computacional, como una llamada sincrónica a un trabajo de AWS Glue, una tarea de AWS Fargate, un paso de Amazon EMR o un bloc de notas de Amazon. SageMaker Los metadatos de las tablas se extraen de los archivos de salida mediante un rastreador de AWS Glue, que actualiza el catálogo de AWS Glue. Los metadatos de los archivos también se añaden a la tabla de catálogo completa de DynamoDB. Por último, también se ejecuta un paso de calidad de datos aprovechando Deequ.

Pila de tecnología

- CloudWatch Eventos de Amazon

- AWS CloudFormation
- AWS CodePipeline
- AWS CodeBuild
- AWS CodeCommit
- Amazon DynamoDB
- AWS Glue
- AWS Lambda
- Amazon S3
- Amazon SQS
- AWS Step Functions

Tools (Herramientas)

- Amazon CloudWatch Events — CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS.
- AWS CloudFormation: CloudFormation ayuda a crear y aprovisionar las implementaciones de infraestructura de AWS de forma predecible y repetitiva.
- AWS CodeBuild: CodeBuild es un servicio de compilación totalmente gestionado que compila el código fuente, ejecuta pruebas unitarias y produce artefactos listos para su implementación.
- AWS CodeCommit: CodeCommit es un servicio de control de versiones hospedado por AWS que puede usar para almacenar y administrar activos de forma privada (como código fuente y archivos binarios).
- AWS CodePipeline: CodePipeline es un servicio de entrega continua que puede utilizar para modelar, visualizar y automatizar los pasos necesarios para publicar los cambios de software de forma continua.
- Amazon DynamoDB: DynamoDB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido y predecible, así como escalabilidad.
- AWS Glue: AWS Glue es un servicio ETL totalmente gestionado que facilita la preparación y la carga de datos para su análisis.
- AWS Lambda: Lambda admite la ejecución de código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.

- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable. Amazon S3 se puede utilizar para una amplia gama de soluciones de almacenamiento, incluyendo sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- AWS Step Functions: AWS Step Functions es un orquestador de funciones sin servidor que facilita la secuenciación de las funciones de AWS Lambda y varios servicios de AWS en aplicaciones esenciales desde el punto de vista empresarial.
- Amazon SQS: Amazon Simple Queue Service (Amazon SQS) es un servicio de cola de mensajes totalmente gestionado que le permite desacoplar y escalar microservicios, sistemas distribuidos y aplicaciones sin servidor.
- Deequ: Deequ es una herramienta que le ayuda a calcular las métricas de calidad de los datos para conjuntos de datos de gran tamaño, a definir y verificar las limitaciones de calidad de los datos y a mantenerse informado sobre los cambios en la distribución de los datos.

Repositorio de código

El código fuente y los recursos del SDLF están disponibles en el GitHub repositorio de AWS Labs.

Epics

Configure la CI/CD canalización para aprovisionar el IaC

Tarea	Descripción	Habilidades requeridas
Configure la CI/CD canalización para administrar el IaC para el lago de datos.	Inicie sesión en la consola de administración de AWS y siga los pasos de la sección de Configuración inicial del taller de SDLF. Esto crea los CI/CD recursos iniciales, como los CodeCommit repositorios, los CodeBuild entornos y las CodePipeline canalizaciones que aprovisionan y administran el IaC para el lago de datos.	DevOps ingeniero

Control de versiones de la IaC

Tarea	Descripción	Habilidades requeridas
Clona el CodeCommit repositorio en tu máquina local.	Siga los pasos de la sección Implementación de los fundamentos del taller sobre el SDLF. Esto le ayuda a clonar el repositorio de Git que aloja la IaC en su entorno local. Para obtener más informaci ón, consulte Conectarse a CodeCommit repositorios en la CodeCommit documenta ción.	DevOps ingeniero
Modifique las CloudFormation plantillas.	Utilice su estación de trabajo local y un editor de código para modificar las CloudForm ation plantillas según sus casos de uso o requisitos. Configúrelos en el repositorio de Git clonado localmente. Para obtener más informaci ón, consulte Trabajar con CloudFormation plantillas de AWS en la CloudFormation documentación de AWS.	DevOps ingeniero
Envía los cambios al CodeCommit repositorio.	Su código de infraestructura está ahora bajo control de versiones y se realiza un seguimiento de las modificac iones de su base de código. Cuando introduce un cambio en el CodeCommit repositor	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	io, lo aplica CodePipel ine automáticamente a su infraestructura y lo envía allí CodeBuild. **Important** Si utiliza la CLI de AWS SAM en CodeBuild, ejecute los `sam deploy` comandos `sam package` y. Si usa la CLI de AWS, ejecute los comandos `aws cloudformation package` y `aws cloudformation deploy`.	

Recursos relacionados

Configure la CI/CD canalización para aprovisionar el IaC

- Taller sobre el SDLF: Configuración inicial

Control de versiones de la IaC

- Taller sobre SDLF: Implementando las bases
- Conexión a repositorios CodeCommit
- Trabajar con CloudFormation plantillas de AWS

Otros recursos

- Arquitectura de referencia de la canalización de análisis de datos sin servidor de AWS
- Documentación de SDLF

Imponga el etiquetado de los clústeres de Amazon EMR en el lanzamiento

Priyanka Chaudhary, Amazon Web Services

Resumen

Este patrón proporciona un control de seguridad que garantiza que los clústeres de Amazon EMR se etiqueten cuando son creados.

Amazon EMR es un servicio de Amazon Web Services (AWS) para procesar y analizar grandes cantidades de datos. Amazon EMR ofrece un servicio ampliable de baja configuración como alternativa más simple a la ejecución interna de computación en clústeres. Puede usar el etiquetado para clasificar los recursos de AWS de diversas maneras, por ejemplo, según su finalidad, propietario o entorno. Por ejemplo, puede etiquetar sus clústeres de Amazon EMR asignando metadatos personalizados a cada clúster. Una etiqueta consta de una clave y un valor que define el usuario. Le recomendamos que cree un conjunto de etiquetas coherente para satisfacer los requisitos de su organización. Al añadir una etiqueta a un clúster de Amazon EMR, la etiqueta también se propaga a cada instancia activa de Amazon Elastic Compute Cloud (Amazon EC2) asociada al clúster. Del mismo modo, cuando eliminas una etiqueta de un clúster de Amazon EMR, esa etiqueta también se elimina de cada EC2 instancia activa asociada.

El control de detectives supervisa las llamadas a la API e inicia un evento de Amazon CloudWatch Events para RunJobFlow, AddTagsRemoveTags, y CreateTags APIs. El evento llama a AWS Lambda, que ejecuta un script de Python. La función de Python obtiene el ID del clúster de Amazon EMR de la entrada JSON del evento y realiza las siguientes comprobaciones:

- Comprobar si el clúster de Amazon EMR está configurado con los nombres de etiquetas que especifique.
- Si no lo está, envía una notificación de Amazon Simple Notification Service (Amazon SNS) al usuario con la información pertinente: el nombre del clúster de Amazon EMR, los detalles de la infracción, la región de AWS, la cuenta de AWS y el nombre de recurso de Amazon (ARN) de Lambda del que proviene la notificación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Cargue el código de Lambda proporcionado en un bucket de Amazon Simple Storage Service (Amazon S3). O bien, puede crear un bucket de S3 para este fin, tal y como se describe en la sección Epics.
- Especifique una dirección de correo electrónico activa en la que desee recibir notificaciones de infracciones.
- Una lista de etiquetas obligatorias que desea comprobar.

Limitaciones

- Este control de seguridad es regional. Debe implementarlo en cada región de AWS que desee supervisar.

Versiones de producto

- Amazon EMR 4.8.0 y versiones posteriores.

Arquitectura

Arquitectura de flujo de trabajo

Automatización y escala

- Si utiliza AWS Organizations, puede utilizar AWS Cloudformation StackSets para implementar esta plantilla en varias cuentas que desee supervisar.

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Puede administrar y aprovisionar pilas en varias cuentas y regiones de AWS.

- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS.
- Amazon EMR: Amazon EMR es un servicio web que simplifica la ejecución de marcos de macrodatos y el procesamiento eficiente de grandes cantidades de datos.
- AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.

Código

Este patrón incluye los siguientes archivos adjuntos:

- `EMRTagValidation.zip`: el código de Lambda para el control de seguridad.
- `EMRTagValidation.yml`— La CloudFormation plantilla que configura el evento y la función Lambda.

Epics

Configuración del bucket de S3

Tarea	Descripción	Habilidades requeridas
Defina el bucket de S3.	En la consola Amazon S3, elija o cree un bucket de S3 para alojar el archivo .zip de código de Lambda. El bucket de S3 debe estar en la misma región de AWS que el clúster	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	de Amazon EMR que desea supervisar. Un nombre de bucket de Amazon S3 es globalmente único y todas las cuentas de AWS comparten el espacio de nombres. El nombre de bucket de S3 no puede incluir barras a la izquierda.	
Cargue el código de Lambda.	Cargue el archivo .zip de código de Lambda que se proporciona en la sección Adjuntos en el bucket de S3.	Arquitecto de la nube

Implemente la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Lance la CloudFormation plantilla de AWS.	Abra la CloudFormation consola de AWS en la misma región de AWS que su bucket de S3 e implemente la plantilla . Para obtener más informaci ón sobre la implementación de CloudFormation plantillas de AWS, consulte Crear una pila en la CloudFormation consola de AWS en la CloudFormation documentación.	Arquitecto de la nube
Complete los parámetros de la plantilla.	Al lanzar la plantilla, se le solicitará la siguiente informaci ón:	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	• Bucket de S3: especifique el bucket creado o seleccionado en la primera Epic. Aquí es donde cargó el código de Lambda adjunto (archivo .zip). • Clave S3: especifique la ubicación del archivo .zip de Lambda en el bucket de S3 (por ejemplo, nombre de archivo.zip o controls/nombre de archivo.zip). No incluya barras a la izquierda . • Correo electrónico de notificación: proporcione una dirección de correo electrónico activa en la que desea recibir las notificaciones de Amazon SNS. • Etiquetado de nombres clave: indique las etiquetas que desee comprobar en una lista separada por comas (por ejemplo, `ApplicationID` , `Environment` , `Owner`). El evento CloudWatch Events monitorea el clúster en busca de estas etiquetas y envía una notificación si no las encuentra. • Nivel de registro Lambda: especifique el nivel y la	

Tarea	Descripción	Habilidades requeridas
	frecuencia de registro de la función de Lambda. Utilice Info para registrar mensajes informativos detallados sobre el progreso, Error para los eventos de error que pudieran continuar con la implementación y Advertencia en caso de situaciones potencialmente dañinas.	

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la CloudFormation plantilla se implementa correctamente, envía un correo electrónico de suscripción a la dirección de correo electrónico que has proporcionado. Debe confirmar esta suscripción de correo electrónico para recibir las notificaciones de infracciones.	Arquitecto de la nube

Recursos relacionados

- Guía para desarrolladores de AWS Lambda
- Etiquetado de clústeres de Amazon EMR

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Asegúrese de que el registro de Amazon EMR en Amazon S3 esté habilitado en el lanzamiento

Priyanka Chaudhary, Amazon Web Services

Resumen

Este patrón proporciona un control de seguridad que supervisa la configuración de registro de los clústeres de Amazon EMR ejecutados en Amazon Web Services (AWS).

Amazon EMR es una herramienta de AWS para el procesamiento y el análisis de macrodatos. Amazon EMR ofrece un servicio ampliable de baja configuración como alternativa a la ejecución interna de computación en clústeres. Amazon EMR ofrece dos tipos de clústeres de EMR.

- Clústeres transitorios de Amazon EMR: los clústeres transitorios de Amazon EMR se desactivan automáticamente y dejan de incurrir en costos cuando finaliza el procesamiento.
- Clústeres persistentes de Amazon EMR: los clústeres persistentes de Amazon EMR siguen ejecutándose una vez finalizado el trabajo de procesamiento de datos.

Amazon EMR y Hadoop producen archivos de registro que notifican el estado en el clúster. De forma predeterminada, se escriben en el nodo principal del directorio/mnt/var/log/. En función de cómo configure el clúster en el momento de su lanzamiento, también podrá guardar estos registros en Amazon Simple Storage Service (Amazon S3) y consultarlos a través de la herramienta de depuración gráfica. Tenga en cuenta que el registro de Amazon S3 solo se puede especificar cuando se lanza el clúster. Con esta configuración, los registros se envían desde el nodo principal a la ubicación de Amazon S3 cada 5 minutos. En el caso de los clústeres transitorios, el registro en Amazon S3 es muy importante, ya que los clústeres desaparecen cuando se completa el procesamiento y estos archivos de registro pueden usarse para depurar cualquier trabajo fallido.

El patrón utiliza una CloudFormation plantilla de AWS para implementar un control de seguridad que monitorea las llamadas a la API e inicia Amazon CloudWatch Events en "»RunJobFlow. El disparador invoca AWS Lambda, que ejecuta un script de Python. La función de Lambda recupera la ID del clúster de EMR de la entrada JSON del evento, y también comprueba si hay un URI de registro de Amazon S3. Si no se encuentra un URI de Amazon S3, la función de Lambda envía una notificación de Amazon Simple Notification Service (Amazon SNS) en la que se detalla el nombre del clúster de EMR, los detalles de la infracción, la región de AWS, la cuenta de AWS y el nombre de recurso de Amazon (ARN) de Lambda del que proviene la notificación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un bucket de S3 para el archivo .zip de código de Lambda
- La dirección de correo electrónico en la que desee recibir la notificación de infracción

Limitaciones

- Este control de detección es regional, por lo que debe implementarse en las regiones de AWS que desee supervisar.

Versiones de producto

- Amazon EMR 4.8.0 y versiones posteriores

Arquitectura

Pila de tecnología de destino

- Evento Amazon CloudWatch Events
- Amazon EMR
- Función de Lambda
- Bucket de S3
- Amazon SNS

Arquitectura de destino

Automatización y escala

- Si utiliza AWS Organizations, puede utilizar AWS CloudFormation StackSets para implementar esta plantilla en varias cuentas que desee supervisar.

Tools (Herramientas)

Herramientas

- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar los recursos de AWS utilizando la infraestructura como código.
- AWS Cloudwatch Events: AWS CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS.
- Amazon EMR: Amazon EMR es una plataforma de clúster administrada que simplifica la ejecución de marcos de trabajo de macrodatos.
- AWS Lambda: AWS Lambda permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- Amazon S3: Amazon S3 es una interfaz de servicios web que puede utilizar para almacenar y recuperar cualquier cantidad de datos desde cualquier lugar de la web.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico.

Código

- El archivo .zip del proyecto está disponible como adjunto.

Epics

Cómo definir el bucket de S3

Tarea	Descripción	Habilidades requeridas
Defina el bucket de S3.	Para alojar el archivo .zip de código de Lambda, seleccione o cree un bucket de S3 con un nombre único que no contenga barras diagonales al inicio. Un nombre de bucket de S3 es globalmente	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	único y todas las cuentas de AWS comparten el espacio de nombres. Su bucket de S3 debe estar en la misma región de AWS que el clúster de Amazon EMR que se evalúa.	

Cómo cargar el código de Lambda en el bucket de S3

Tarea	Descripción	Habilidades requeridas
Cargue el código de Lambda en el bucket de S3.	Cargue el archivo .zip de código de Lambda que se proporciona en la sección “Adjuntos” del bucket de S3. El bucket de S3 debe encontrarse en la misma región que el clúster de Amazon EMR que se está evaluando.	Arquitecto de la nube

Implemente la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla de AWS.	En la CloudFormation consola de AWS, en la misma región que su bucket de S3, implemente la CloudForm ation plantilla de AWS que se proporciona como adjunto a este patrón. En la siguiente épica, proporcione los valores de los parámetros. Para	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	obtener más información sobre la implementación de CloudFormation plantillas de AWS, consulte la sección «Recursos relacionados».	

Complete los parámetros de la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Ponga nombre al bucket de S3.	Escriba el nombre del bucket de S3 que ha creado en la primera épica.	Arquitecto de la nube
Proporcione la clave de Amazon S3.	Proporcione la ubicación del archivo .zip del código de Lambda en su bucket de S3, sin barras diagonales iniciales (por ejemplo, <directory>/<file-name>.zip).	Arquitecto de la nube
Proporcione una dirección de correo electrónico.	Proporcione una dirección de correo electrónico activa en la que desea recibir las notificac iones de Amazon SNS.	Arquitecto de la nube
Defina el nivel de registro.	Defina el nivel y la frecuenci a de registro de la función de Lambda. “Info” designa mensajes informativos detallados sobre el progreso de la aplicación. “Error” designa eventos de error que permiten que la aplicación siga ejecutándose. “Adverten	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	cia" designa situaciones potencialmente peligrosas.	

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la plantilla se implementa correctamente, se envía un mensaje de correo electrónico de suscripción a la dirección de correo electróni co proporcionada. Debe confirmar esta suscripción de correo electrónico para recibir las notificaciones de infraccio nes.	Arquitecto de la nube

Recursos relacionados

- AWS Lambda
- Registro de Amazon EMR
- Implementación de CloudFormation plantillas de AWS

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Genere datos de prueba con un trabajo de AWS Glue y Python

Moinul Al-Mamun, Amazon Web Services

Resumen

Este patrón le muestra cómo generar de forma rápida y sencilla millones de archivos de muestra de forma simultánea mediante la creación de un trabajo de AWS Glue escrito en Python. El archivo de ejemplo se almacena en un bucket de Amazon Simple Storage Service (Amazon S3). La capacidad de generar rápidamente una gran cantidad de archivos de muestra es importante para probar o evaluar los servicios en la nube de AWS. Por ejemplo, puede probar el rendimiento de los DataBrew trabajos de AWS Glue Studio o AWS Glue realizando un análisis de datos en millones de archivos pequeños en un prefijo de Amazon S3.

Aunque puede utilizar otros servicios de AWS para generar conjuntos de datos de ejemplo, le recomendamos que utilice AWS Glue. No necesita administrar ninguna infraestructura porque AWS Glue es un servicio de procesamiento de datos sin servidor. Solo tiene que traer su código y ejecutarlo en un clúster de AWS Glue. Además, AWS Glue aprovisiona, configura y escala los recursos necesarios para ejecutar sus trabajos. Solo paga por los recursos que utilizan los trabajos mientras se ejecutan.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada para funcionar con la cuenta AWS.

Versiones de producto

- Python 3.9
- CLI de AWS versión 2

Limitaciones

El número máximo de trabajos de AWS Glue por activador es 50. Para obtener más información, consulte Puntos de conexión y cuotas de AWS Glue.

Arquitectura

El siguiente diagrama muestra un ejemplo de arquitectura centrado en un trabajo de AWS Glue que escribe su salida (es decir, archivos de muestra) en un bucket de S3.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Utilice la AWS CLI, la Consola de administración de AWS o una API para iniciar el trabajo de AWS Glue. La API o la CLI de AWS le permiten automatizar la paralelización del trabajo invocado y reducir el tiempo de ejecución necesario para generar archivos de muestra.
2. El trabajo de AWS Glue genera el contenido del archivo de forma aleatoria, lo convierte en formato CSV y, a continuación, lo almacena como un objeto de Amazon S3 con un prefijo común. Cada archivo ocupa menos de un kilobyte. El trabajo de AWS Glue acepta dos parámetros de trabajo definidos por el usuario: `START_RANGE` y `END_RANGE`. Puede utilizar estos parámetros para establecer los nombres de los archivos y el número de archivos generados en Amazon S3 por cada ejecución de trabajo. Puede ejecutar varias instancias de este trabajo en paralelo (por ejemplo, 100 instancias).

Tools (Herramientas)

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.

Prácticas recomendadas

Tenga en cuenta las siguientes prácticas recomendadas de AWS Glue al implementar este patrón:

- Utilice el tipo de trabajador de AWS Glue adecuado para reducir los costos. Recomendamos que comprenda las diferentes propiedades de los tipos de trabajadores y, a continuación, elija el tipo de trabajador adecuado para su carga de trabajo en función de los requisitos de CPU y memoria. Para este patrón, recomendamos que utilice un trabajo de intérprete de comandos de Python como tipo de trabajo para minimizar la DPU y reducir los costos. Para obtener más información, consulte Cómo agregar trabajos en AWS Glue en la Guía del desarrollador de AWS Glue.
- Use el límite de simultaneidad correcto para escalar su trabajo. Le recomendamos que base la simultaneidad máxima de su trabajo de AWS Glue en sus requisitos de tiempo y en la cantidad de archivos requerida.
- Comience a generar una cantidad pequeña de archivos al principio. Para reducir los costos y ahorrar tiempo a la hora de crear sus trabajos de AWS Glue, comience con un número reducido de archivos (por ejemplo, 1000). Esto puede facilitar la solución de problemas. Si la generación de un número reducido de archivos se realiza correctamente, puede escalar a un número mayor de archivos.
- Ejecute primero de forma local. Para reducir los costos y ahorrar tiempo a la hora de crear sus trabajos de AWS Glue, inicie el desarrollo de forma local y pruebe el código. Para obtener instrucciones sobre cómo configurar un contenedor de Docker que pueda ayudarlo en la escritura de trabajos de AWS Glue de extracción, transformación y carga (ETL), tanto en un intérprete de comandos como en un entorno de desarrollo integrado (IDE), consulte la entrada Desarrollo y prueba de trabajos de ETL de AWS Glue de forma local mediante un contenedor en la el blog de AWS Big Data.

Para obtener más información sobre las prácticas recomendadas de AWS Glue, consulte las Prácticas recomendadas en la documentación de AWS Glue.

Epics

Creación del bucket de Amazon S3 de destino y un rol de IAM

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3; para almacenar los archivos.	Cree un bucket de S3 y un prefijo dentro de él.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	Note Este patrón utiliza la ubicación `s3://{your-s3-bucket-name}/small-files/` con fines de demostración.	

Tarea	Descripción	Habilidades requeridas
Creación y configuración de un rol de IAM	Debe crear un rol de IAM que su trabajo de AWS Glue pueda usar para escribir en su bucket de S3. 1. Cree un rol de IAM (por ejemplo, llamado `"AWSGlueServiceRole-smallfiles"`). 2. Elija AWS Glue como entidad de confianza de la política. 3. Asocie la política administrada de AWS llamada `"AWSGlueServiceRole"` a este rol. 4. Cree una política en línea o una Política administrada por el cliente, denominada `"s3-small-file-access"` en base a la siguiente configuración. Reemplace `"{bucket}"` con el nombre del bucket. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "s3:GetObject",`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	<pre>"s3:PutObject"
	],
	"Resource": [
	"arn:aws:s3:::{bucket}/small-files/input/*"
	]
	}
	]
	}</pre>
	5. Asocie la política `"s3-small-file-access"` al rol.	

Cree y configure un trabajo de AWS Glue para gestionar ejecuciones simultáneas

Tarea	Descripción	Habilidades requeridas
Crear un trabajo de AWS Glue.	Debe crear un trabajo de AWS Glue que genere su contenido y lo almacene en un bucket de S3. Cree un trabajo de AWS Glue y, a continuación, configure su trabajo siguiendo estos pasos: 1. Inicie sesión en la consola de administración de AWS y abra la consola de AWS Glue.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	2. En el panel de navegación, en Integración de datos y ETL, elija Trabajos. 3. En la sección Create job (Crear trabajo), seleccione el Python Shell script editor (editor de intérprete de comandos de Python). 4. En la sección Options (Opciones), seleccione Create a new script with boilerplate code (Crear un nuevo script con código reutilizable) y, a continuación, seleccione Create (Crear). 5. Elija Job details (Detalles del trabajo). 6. En Nombre, introduzca create_small_files. 7. Para IAM role (Rol de IAM), seleccione el rol de IAM que creó previamente. 8. En la sección This job runs (Este trabajo ejecuta), elija A new script to be authored by you (Un script nuevo para que lo cree usted). 9. Elija Advanced properties (Propiedades avanzadas). 10. En Máxima simultaneidad, introduzca 100 con fines de demostración.	

Tarea	Descripción	Habilidades requeridas
	Nota: La simultaneidad máxima define el número de instancias del trabajo que se pueden ejecutar en paralelo. 11. Seleccione Save.	

Tarea	Descripción	Habilidades requeridas

Actualizar el código del trabajo.	1. Abra la consola de AWS Glue.
	2. En el panel de navegación, seleccione Trabajos.
	3. En la sección Your jobs (Sus trabajos), elija el trabajo que creó anteriormente.
	4. Seleccione la pestaña Script y, a continuación, actualice la secuencia de comandos en función del siguiente código. Actualice las variables `BUCKET_NAME` , `PREFIX` y `text_str` con sus valores.
	`from awsglue.utils import getResolvedOptions`
	`import sys`
	`import boto3`
	`from random import randrange`
	
	`# Two arguments`
	`args = getResolvedOptions(sys.argv, ['START_RANGE', 'END_RANGE'])`
	
	`START_RANGE = int(args['START_RANGE'])`
	`END_RANGE = int(args['END_RANGE'])`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	``` BUCKET_NAME = '{BUCKET_NAME}' PREFIX = 'small-fi les/input/' s3 = boto3.res ource('s3') for x in range(STA RT_RANGE, END_RANGE): # generate file name file_name = f"input_{x}.txt" # generate text text_str = str(randrange(1000 00))+","+str(randr ange(100000))+", " + str(randrange(1000 0000)) + "," + str(randrange(1000 0)) # write in s3 s3.Object(BUCKE T_NAME, PREFIX + file_name).put(Bod y=text_str) ``` 5. Seleccione Save.	

Ejecute el trabajo de AWS Glue desde la línea de comandos o la consola

Tarea	Descripción	Habilidades requeridas
Ejecute el trabajo de AWS Glue desde la línea de comandos.	Para ejecutar su trabajo de AWS Glue desde la CLI de AWS, ejecute el siguiente comando con sus valores:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	`cmd:~$ aws glue start-job-run --job-name create_small_files --arguments '{"--START_RANGE":"0","--END_RANGE":"1000000"}'`
	`cmd:~$ aws glue start-job-run --job-name create_small_files --arguments '{"--START_RANGE":"1000000","--END_RANGE":"2000000"}'`
	
	Note
	Para obtener instrucciones sobre cómo ejecutar el trabajo de AWS Glue desde la consola de administración de AWS, consulte el artículo Ejecute el trabajo de AWS Glue en la consola de administración de AWS de este patrón.
	
	Tip
	Recomendamos que utilice la AWS CLI para ejecutar trabajos de AWS Glue	

Tarea	Descripción	Habilidades requeridas

	si quiere llevar a cabo varias ejecuciones a la vez con distintos parámetros, como se muestra en el ejemplo anterior.
	
	Para generar todos los comandos de la CLI de AWS necesarios para generar un número definido de archivos con un factor de paraleliz ación determinado, ejecute el siguiente código bash (con sus valores):
	
	`# define parameters`
	`NUMBER_OF_FILES=`
	`10000000;`
	`PARALLELIZATION=50;`
	
	`# initialize`
	`_SB=0;`
	
	`# generate commands`
	`for i in $(seq 1`
	` $PARALLELIZATION);`
	`do`
	`  echo aws glue`
	` start-job-run --`
	`job-name create_sm`
	`all_files --argumen`
	`ts "'"'{"--START_RANG`
	`E":"'$(((NUMBER_OF`
	`_FILES/PARALLELIZA`
	`TION) * (i-1) +`
	` _SB))'","--END_RAN`	

Tarea	Descripción	Habilidades requeridas

	<pre>GE":"'$(((NUMBER_O
	F_FILES/PARALLELIZ
	ATION) * (i)))'"}'"'";
	_SB=1;
	done</pre>
	Si utiliza el script anterior, tenga en cuenta lo siguiente:
	• El script simplifica la invocación y la generación de archivos pequeños a escala.
	• Actualice `NUMBER_OF_FILES` y `PARALLELIZATION` con sus valores.
	• El script anterior imprime una lista de comandos que debe ejecutar. Copie esos comandos de salida y ejecútelos en su terminal.
	• Si desea ejecutar los comandos directamente desde el script, elimine la instrucción `echo` de la línea 11.
	
	Note
	Para ver un ejemplo del resultado del script anterior, consulte Resultado del script de intérprete de comandos en la	

Tarea	Descripción	Habilidades requeridas
	sección de Informaci ón adicional de este patrón.	
Ejecute el trabajo de AWS Glue en la consola de administración de AWS.	1. Inicie sesión en la consola de administración de AWS y abra la consola de AWS Glue. 2. En el panel de navegació n, en Integración de datos y ETL, elija Trabajos. 3. En la sección Your jobs (Sus trabajos), elija su trabajo. 4. En la sección Parameter s (optional) (Parámetros (opcional)), actualice sus parámetros. 5. Elija Action (Acción) y, a continuación, seleccione Run job (Ejecutar trabajo). 6. Repita los pasos 3 a 5 tantas veces como sea necesario. Por ejemplo, para crear 10 millones de archivos, repita este proceso 10 veces.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Verifique el estado de su trabajo de AWS Glue.	1. Abra la consola de AWS Glue. 2. En el panel de navegación, seleccione Trabajos. 3. En la sección Your jobs (Sus trabajos), elija el trabajo que creó anteriorm ente (el `create_sm all_files`). 4. Para obtener informaci ón sobre el progreso y la generación de sus archivos, revise las columnas ID de ejecución, Estado de ejecución y otras columnas.	Desarrollador de aplicaciones

Recursos relacionados

Referencias

- Registro de datos abiertos en AWS
- Conjuntos de datos para análisis
- Datos abiertos en AWS
- Cómo añadir trabajos en AWS Glue
- Introducción a AWS Glue

Guías y patrones

- Prácticas recomendadas de AWS Glue
- Aplicaciones de pruebas de carga

Información adicional

Prueba de evaluación comparativa

Este patrón se utilizó para generar 10 millones de archivos utilizando diferentes parámetros de paralelización como parte de una prueba de evaluación comparativa. El resultado de la prueba mostrará lo siguiente:

Paralelización	Número de archivos generados por la ejecución de una tarea	Duración del trabajo	Velocidad
10	1 000 000	6 horas, 40 minutos	Muy lento
50	200.000	80 minutos	Moderado
100	100 000	40 minutos	Fast

Si desea acelerar el proceso, puede configurar más ejecuciones simultáneas en la configuración de su trabajo. Puede ajustar fácilmente la configuración del trabajo en función de sus requisitos, pero tenga en cuenta que existe un límite de cuota de servicio de AWS Glue. Para obtener más información, consulte Puntos de conexión y cuotas de AWS Glue.

Resultado del script de intérprete de comandos

En el siguiente ejemplo, se muestra el resultado del script de intérprete de comandos de la historia Ejecute the AWS Glue desde la línea de comandos siguiendo este patrón.

```
user@MUC-1234567890 MINGW64 ~
  $ # define parameters
  NUMBER_OF_FILES=10000000;
  PARALLELIZATION=50;
  # initialize
  _SB=0;

  # generate commands
  for i in $(seq 1 $PARALLELIZATION);
   do
```

```
        echo aws glue start-job-run --job-name create_small_files --arguments
 "'"'{"--START_RANGE":"'$(((NUMBER_OF_FILES/PARALLELIZATION)  (i-1) + SB))'","--
ENDRANGE":"'$(((NUMBER_OF_FILES/PARALLELIZATION)  (i)))'"}'"'";
        _SB=1;
   done

  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"0","--END_RANGE":"200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"200001","--END_RANGE":"400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"400001","--END_RANGE":"600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"600001","--END_RANGE":"800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"800001","--END_RANGE":"1000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1000001","--END_RANGE":"1200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1200001","--END_RANGE":"1400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1400001","--END_RANGE":"1600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1600001","--END_RANGE":"1800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1800001","--END_RANGE":"2000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2000001","--END_RANGE":"2200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2200001","--END_RANGE":"2400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2400001","--END_RANGE":"2600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2600001","--END_RANGE":"2800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2800001","--END_RANGE":"3000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3000001","--END_RANGE":"3200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3200001","--END_RANGE":"3400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3400001","--END_RANGE":"3600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3600001","--END_RANGE":"3800000"}'
```

```
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3800001","--END_RANGE":"4000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4000001","--END_RANGE":"4200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4200001","--END_RANGE":"4400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4400001","--END_RANGE":"4600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4600001","--END_RANGE":"4800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4800001","--END_RANGE":"5000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5000001","--END_RANGE":"5200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5200001","--END_RANGE":"5400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5400001","--END_RANGE":"5600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5600001","--END_RANGE":"5800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5800001","--END_RANGE":"6000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6000001","--END_RANGE":"6200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6200001","--END_RANGE":"6400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6400001","--END_RANGE":"6600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6600001","--END_RANGE":"6800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6800001","--END_RANGE":"7000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7000001","--END_RANGE":"7200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7200001","--END_RANGE":"7400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7400001","--END_RANGE":"7600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7600001","--END_RANGE":"7800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7800001","--END_RANGE":"8000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8000001","--END_RANGE":"8200000"}'
```

```
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8200001","--END_RANGE":"8400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8400001","--END_RANGE":"8600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8600001","--END_RANGE":"8800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8800001","--END_RANGE":"9000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9000001","--END_RANGE":"9200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9200001","--END_RANGE":"9400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9400001","--END_RANGE":"9600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9600001","--END_RANGE":"9800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9800001","--END_RANGE":"10000000"}'

  user@MUC-1234567890 MINGW64 ~
```

Preguntas frecuentes

¿Cuántas ejecuciones simultáneas o trabajos paralelos debo usar?

El número de ejecuciones simultáneas y trabajos paralelos depende del tiempo requerido y del número deseado de archivos de prueba. Le recomendamos que compruebe el tamaño de los archivos que va a crear. En primer lugar, compruebe cuánto tiempo tarda un trabajo de AWS Glue en generar la cantidad de archivos deseada. A continuación, utilice el número correcto de ejecuciones simultáneas para cumplir sus objetivos. Por ejemplo, si supone que 100 000 archivos tardan 40 minutos en completar la ejecución, pero el tiempo objetivo es de 30 minutos, debe aumentar la configuración de simultaneidad para su trabajo de AWS Glue.

¿Qué tipo de contenido puedo crear con este patrón?

Puede crear cualquier tipo de contenido, como archivos de texto con distintos delimitadores (por ejemplo, PIPE, JSON o CSV). Este patrón usa Boto3 para escribir en un archivo y, a continuación, guarda el archivo en un bucket de S3.

¿Qué nivel de permiso de IAM necesito en el bucket de S3?

Debe tener una política basada en identidad que le permita a `Write` acceso a objetos de su bucket de S3. Para obtener más información, consulte Amazon S3: permite el acceso de lectura y escritura a objetos de un bucket de S3 en la documentación de Amazon S3.

Capturar datos de IoT directamente en Amazon S3 de forma rentable con AWS IoT Greengrass

Sebastian Viviani y Rizwan Syed, Amazon Web Services

Resumen

Este patrón le muestra cómo incorporar datos de Internet de las cosas (IoT) de forma rentable directamente en un depósito de Amazon Simple Storage Service (Amazon S3) mediante un dispositivo AWS IoT Greengrass versión 2. El dispositivo ejecuta un componente personalizado que lee los datos de IoT y los guarda en un almacenamiento persistente (es decir, un disco o volumen local). A continuación, el dispositivo comprime los datos de IoT en un archivo de Apache Parquet y los carga periódicamente en un bucket de S3.

La cantidad y la velocidad de los datos de IoT que ingiere están limitadas únicamente por las capacidades de su hardware periférico y el ancho de banda de la red. Puede utilizar Amazon Athena para analizar de forma rentable los datos ingeridos. Athena admite archivos comprimidos de Apache Parquet y la visualización de datos mediante el uso de Amazon Managed Grafana.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una puerta de enlace perimetral que se ejecuta en AWS IoT Greengrass versión 2 y recopila datos de los sensores (las fuentes de datos y el proceso de recopilación de datos están fuera del alcance de este patrón, pero puede usar casi cualquier tipo de datos de sensores). Este patrón utiliza un intermediario MQTT local con sensores o puertas de enlace que publican los datos de forma local.
- Componentes, roles y dependencias del SDK de AWS IoT Greengrass
- Un componente de administrador de transmisiones para cargar los datos al bucket de S3
- AWS SDK para Java, AWS SDK para JavaScript o AWS SDK para Python (Boto3) para ejecutar el APIs

Limitaciones

- Los datos de este patrón no se cargan en tiempo real en el bucket de S3. Hay un período de retraso y puede configurarlo. Los datos se almacenan temporalmente en el dispositivo perimetral y, una vez transcurrido el período, se cargan.
- El SDK está disponible en Java, Node.js o Python.

Arquitectura

Pila de tecnología de destino

- Amazon S3
- AWS IoT Greengrass
- Intermediario MQTT
- Componente Stream Manager

Arquitectura de destino

El siguiente diagrama muestra una arquitectura diseñada para capturar datos de sensores de IoT y almacenarlos en un bucket de S3.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Las actualizaciones de varios sensores (por ejemplo, de temperatura y válvula) se publican en un agente de MQTT local.
2. El compresor de archivos Parquet que está suscrito a estos sensores actualiza los temas y recibe estas actualizaciones.
3. El compresor de archivos Parquet almacena las actualizaciones de forma local.
4. Una vez transcurrido el período, los archivos almacenados se comprimen en archivos Parquet y se pasan al administrador de flujos para cargarlos en el bucket de S3 especificado.
5. El administrador de transmisión carga los archivos de Parquet en el bucket de S3.

> **Note**
>
> El administrador de transmisiones (`StreamManager`) es un componente administrado. Para ver ejemplos de cómo exportar datos a Amazon S3, consulte Stream Manager en

la documentación de AWS IoT Greengrass. Puede utilizar un bróker MQTT local como componente u otro bróker como Eclipse Mosquitto.

Tools (Herramientas)

Herramientas de AWS

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS IoT Greengrass es un servicio en la nube y de tiempo de ejecución de borde de IoT de código abierto que le ayuda a crear, implementar y administrar aplicaciones de IoT en los dispositivos.

Otras herramientas

- Apache Parquet es un formato de archivo de datos de código abierto orientado por columnas diseñado para el almacenamiento y la recuperación.
- El MQTT (Message Queuing Telemetry Transport) es un protocolo de mensajería ligero diseñado para dispositivos restringidos.

Prácticas recomendadas

Utilice el formato de partición adecuado para los datos cargados

No hay requisitos específicos para los nombres de los prefijos raíz del bucket de S3 (por ejemplo, `"myAwesomeDataSet/"` o`"dataFromSource"`), pero le recomendamos que utilice una partición y un prefijo significativos para que sea fácil entender el propósito del conjunto de datos.

También le recomendamos que utilice la partición correcta en Amazon S3 para que las consultas se ejecuten de forma óptima en el conjunto de datos. En el siguiente ejemplo, los datos se dividen en formato HIVE para optimizar la cantidad de datos escaneados por cada consulta de Athena. Esto puede mejorar el rendimiento y reducir los costos.

```
s3://<ingestionBucket>/<rootPrefix>/year=YY/month=MM/day=DD/
HHMM_<suffix>.parquet
```

Epics

Configure su entorno

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	1. Cree un bucket de S3 o utilice uno existente. 2. Cree un prefijo significativo para el depósito de S3 en el que desee capturar los datos de IoT (por ejemplo,`s3:\\<bucket>\<prefix>`). 3. Registre su prefijo para usarlo más adelante.	Desarrollador de aplicaciones
Añada permisos de IAM al bucket de S3.	Para conceder a los usuarios acceso de escritura al bucket y al prefijo de S3 que creó anteriormente, añada la siguiente política de IAM a su rol de AWS IoT Greengrass: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "S3DataUpload", "Effect": "Allow", "Action": [ "s3:List*", "s3:Put*" ],`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	<pre>"Resource":
	[
	"arn:aws:s3:::<ingestionBucket>",
	"arn:aws:s3:::<ingestionBucket>/<prefix>/*"
	]
	}
	]
	}</pre>
	Para obtener más información, consulte Creación de una política de IAM para acceder a los recursos de Amazon S3 en la documentación de Aurora.
	
	A continuación, actualice la política de recursos (si es necesario) del bucket de S3 para permitir el acceso de escritura con los principios de AWS correctos.	

Cree e implemente el componente AWS IoT Greengrass

Tarea	Descripción	Habilidades requeridas
Actualizar la receta del componente.	Actualice la configuración del componente al crear una implementación según el siguiente ejemplo: <pre>{</pre>	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	<pre>"region": "<region>",
	"parquet_period":
	<period>,
	"s3_bucket":
	"<s3Bucket>",
	"s3_key_prefix":
	"<s3prefix>"
	}</pre>
	<region>Sustitúyalo por su región <period> de AWS, su intervalo periódico, <s3Bucket> su bucket de S3 y <s3prefix> por su prefijo.	

Tarea	Descripción	Habilidades requeridas
Cree el componente.	Realice una de las siguientes acciones: • Cree el componente. • Añada el componente a la CI/CD canalización (si existe). Asegúrese de copiar el artefacto del repositorio de artefactos al depósito de artefactos de AWS IoT Greengrass. A continuación, cree o actualice su componente AWS IoT Greengrass. • **Note** Añada el agente MQTT como componente o agréguelo manualmente más adelante. : Esta decisión afecta al esquema de autenticación que puede utilizar con el agente. Al añadir manualmente un agente, se desvincula el agente de AWS IoT Greengrass y se habilita cualquier esquema de autentica	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	ción compatible del agente. Los componentes de agente proporcionados por AWS tienen esquemas de autenticación predefinidos. Para obtener más información, consulte el agente MQTT 3.1.1 (Moquette) y el agente MQTT 5 (EMQX).	
Actualice el cliente MQTT.	El código de ejemplo no utiliza la autenticación porque el componente se conecta localmente al intermediario. Si su situación es diferente, actualice la sección del cliente de MQTT según sea necesario. Además, realice lo siguiente: 1. Actualice los temas de MQTT de la suscripción. 2. Actualice el analizador de mensajes MQTT según sea necesario, ya que los mensajes de cada fuente pueden diferir.	Desarrollador de aplicaciones

Añada el componente al dispositivo principal de AWS IoT Greengrass versión 2

Tarea	Descripción	Habilidades requeridas
Actualice la implementación del dispositivo principal.	Si la implementación del dispositivo principal de AWS IoT Greengrass versión 2 ya existe, revise la implement ación. Si la implementación no existe, cree una nueva. Para asignar al componente el nombre correcto, actualice la configuración del administr ador de registros para el nuevo componente (si es necesario) en función de lo siguiente: `{ "logsUploaderConfi guration": { "systemLogsConfigu ration": { ... }, "componentLogsConf igurationMap": { "<com.iot .ingest.parquet>": { "minimumL ogLevel": "INFO", "diskSpac eLimit": "20", "diskSpac eLimitUnit": "MB", "deleteLo gFileAfterCloudUpl oad": "false" } ...`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	<pre> }
	  },
	  "periodicUploadInt
	ervalSec": "300"
	}</pre>
	Por último, complete la revisión de la implementación de su dispositivo principal AWS IoT Greengrass.	

Verifique la captura de datos en el depósito de S3

Tarea	Descripción	Habilidades requeridas
Compruebe los registros del volumen de AWS IoT Greengrass.	Compruebe lo siguiente: • El cliente MQTT se ha conectado correctamente al agente MQTT local. • El cliente MQTT está suscrito a los temas correctos. • Están llegando al bróker mensajes de actualización de sensores sobre temas relacionados con el MQTT. • La compresión de parquet se produce en cada intervalo periódico.	Desarrollador de aplicaciones
Compruebe el bucket de S3.	Compruebe si los datos se cargan en el bucket de S3. Puede ver los archivos que	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	se están cargando en cada período. También puede comprobar si los datos se han cargado en el depósito de S3 consultando los datos en la siguiente sección.	

Configurar consultas desde Athena

Tarea	Descripción	Habilidades requeridas
Crear una base de datos y tabla.	1. Cree una base de datos de AWS Glue (si es necesario). 2. Cree una tabla en AWS Glue manualmente o ejecute un rastreador en AWS Glue.	Desarrollador de aplicaciones
Concede a Athena acceso a los datos.	1. Actualice los permisos para permitir que Athena acceda al bucket de S3. Para obtener más información, consulte Acceso detallado a bases de datos y tablas en el catálogo de datos de AWS Glue en la documentación de Athena. 2. Consulte la tabla en su base de datos.	Desarrollador de aplicaciones

Resolución de problemas

Problema	Solución
El cliente MQTT no se puede conectar	• Validar los permisos en el bróker MQTT. Si tiene un bróker MQTT de AWS, consulte Broker MQTT 3.1.1 (Moquette) y MQTT 5 Broker (EMQX). • Validar las credenciales en el cliente MQTT. Si tiene un bróker MQTT de AWS, consulte Broker MQTT 3.1.1 (Moquette) y MQTT 5 Broker (EMQX).
El cliente MQTT no se suscribe	Validar los permisos en el bróker MQTT. Si tiene un bróker MQTT de AWS, consulte Broker MQTT 3.1.1 (Moquette) y MQTT 5 Broker (EMQX).
Los archivos Parquet no se crean	• Compruebe que los temas de MQTT son correctos. • Compruebe que los mensajes de MQTT de los sensores tengan el formato correcto.
Los objetos no se cargan en el bucket de S3	• Compruebe que dispone de conectividad a Internet y de un punto de conexión. • Compruebe que la política de recursos de su bucket de S3 sea correcta. • Compruebe los permisos para la función de dispositivo principal de AWS IoT Greengrass versión 2.

Recursos relacionados

- DataFrame(documentación de Pandas)
- Documentación de Apache Parquet (documentación de Parquet)

- Desarrollo de componentes de AWS IoT Greengrass (Guía para desarrolladores de AWS IoT Greengrass, versión 2)
- Implemente componentes de AWS IoT Greengrass en dispositivos (Guía para desarrolladores de AWS IoT Greengrass, versión 2)
- Interactúe con dispositivos de IoT locales (Guía para desarrolladores de AWS IoT Greengrass, versión 2)
- Broker MQTT 3.1.1 (Moquette) (Guía para desarrolladores de AWS IoT Greengrass, versión 2)
- Broker MQTT 5 (EMQX) (Guía para desarrolladores de AWS IoT Greengrass, versión 2)

Información adicional

Análisis de costos

El siguiente escenario de análisis de costos demuestra cómo el enfoque de captura de datos incluido en este patrón puede afectar los costos de captura de datos en la nube de AWS. Los ejemplos de precios de este escenario se basan en los precios vigentes en el momento de la publicación. Los precios están sujetos a cambios. Además, los costos pueden variar en función de la región de AWS, las Service quotas de AWS y otros factores relacionados con el entorno de nube.

Conjunto de señales de entrada

Este análisis utiliza el siguiente conjunto de señales de entrada como base para comparar los costos de captura de IoT con otras alternativas disponibles.

Número de señales	Frecuencia	Datos por señal
125	25 Hz	8 bytes

En este escenario, el sistema recibe 125 señales. Cada señal es de 8 bytes y se produce cada 40 milisegundos (25 Hz). Estas señales pueden venir individualmente o agrupadas en una carga útil común. Tiene la opción de dividir y empaquetar estas señales según sus necesidades. También puede determinar la latencia. La latencia consiste en el período de tiempo para recibir, acumular y capturar los datos.

A modo de comparación, la operación de captura de este escenario se basa en la región de AWS de `us-east-1`. La comparación de costos se aplica únicamente a los servicios de AWS. Otros costos, como el hardware o la conectividad, no se tienen en cuenta en el análisis.

Comparaciones de costos

La siguiente tabla muestra el costo mensual en dólares estadounidenses (USD) de cada método de ingestión.

Método	Costo mensual
AWS SiteWise IoT*	331,77 USD
AWS IoT SiteWise Edge con paquete de procesamiento de datos (mantiene todos los datos en el borde)	200 USD
Reglas de AWS IoT Core y Amazon S3 para acceder a datos sin procesar	84,54 USD
Compresión de archivos Parquet en el borde y carga a Amazon S3	0,5 USD

*Los datos se deben reducir para cumplir con las Service quotas. Esto significa que se pierden algunos datos con este método.

Métodos alternativos

En esta sección se muestran los costos equivalentes de los siguientes métodos alternativos:

- AWS IoT SiteWise: cada señal debe cargarse en un mensaje individual. Por lo tanto, la cantidad total de mensajes por mes es de 125 × 25 × 3600 × 24 × 30, o sea, 8 100 millones de mensajes por mes. Sin embargo, AWS IoT solo SiteWise puede gestionar 10 puntos de datos por segundo por propiedad. Suponiendo que los datos se reduzcan a 10 Hz, la cantidad de mensajes por mes se reduce a 125 × 10 × 3600 × 24 × 30, o sea, 3,24 mil millones. Si utiliza el componente de publicación que agrupa las medidas en grupos de 10 (a 1 USD por millón de mensajes), el costo mensual será de 324 USD al mes. Suponiendo que cada mensaje tenga 8 bytes (1 Kb/125), se trata de 25,92 GB de almacenamiento de datos. Esto añade un costo mensual de 7,77 USD. El costo total del primer mes es de 331,77 USD y aumenta 7,77 USD cada mes.
- AWS IoT SiteWise Edge con paquete de procesamiento de datos, que incluye todos los modelos y señales completamente procesados en el borde (es decir, sin ingesta de nubes): puede usar el paquete de procesamiento de datos como alternativa para reducir los costos y configurar todos

los modelos que se calculan en el borde. Esto puede funcionar solo para el almacenamiento y la visualización, incluso si no se realiza ningún cálculo real. En este caso, es necesario utilizar un hardware potente para la puerta de enlace perimetral. Hay un costo fijo de 200 USD al mes.

- Ingesta directa a AWS IoT Core por parte de MQTT y una regla de IoT para almacenar los datos sin procesar en Amazon S3: suponiendo que todas las señales se publiquen en una carga útil común, el número total de mensajes publicados en AWS IoT Core es de 25 × 3600 × 24 × 30, es decir, 64,8 millones por mes. A 1 USD por millón de mensajes, se trata de un costo mensual de 64,8 USD al mes. A 0,15 USD por millón de activaciones de reglas y con una regla por mensaje, esto añade un costo mensual de 19,44 USD. Con un costo de 0,023 USD por GB de almacenamiento en Amazon S3, se añaden otros 1,5 USD al mes (aumentando cada mes para reflejar los nuevos datos). El costo total del primer mes es de 84,54 USD y aumenta 1,5 USD cada mes.
- Comprimir los datos en el borde de un archivo Parquet y subirlos a Amazon S3 (método propuesto): la relación de compresión depende del tipo de datos. Con los mismos datos industriales probados para MQTT, el total de datos de salida de un mes completo es de 1,2 Gb. Esto cuesta 0,03 USD al mes. Los índices de compresión (que utilizan datos aleatorios) descritos en otros puntos de referencia son del orden del 66 por ciento (lo que se acerca más al peor de los casos). El total de datos es de 21 Gb y cuesta 0,5 USD al mes.

Generador de archivos de parquet

El siguiente ejemplo de código muestra la estructura de un generador de archivos Parquet escrito en Python. El ejemplo de código es solo para fines ilustrativos y no funcionará si se pega en su entorno.

```
import queue
import paho.mqtt.client as mqtt
import pandas as pd

#queue for decoupling the MQTT thread
messageQueue = queue.Queue()
client = mqtt.Client()
streammanager = StreamManagerClient()

def feederListener(topic, message):
    payload = {
        "topic" : topic,
        "payload" : message,
    }
    messageQueue.put_nowait(payload)
```

```
def on_connect(client_instance, userdata, flags, rc):
    client.subscribe("#",qos=0)

def on_message(client, userdata, message):
    feederListener(topic=str(message.topic),
 message=str(message.payload.decode("utf-8")))


filename = "tempfile.parquet"
streamname = "mystream"
destination_bucket= "amzn-s3-demo-bucket"
keyname="mykey"
period= 60

client.on_connect = on_connect
client.on_message = on_message
streammanager.create_message_stream(
            MessageStreamDefinition(name=streamname,
 strategy_on_full=StrategyOnFull.OverwriteOldestData)
        )


while True:
   try:
       message = messageQueue.get(timeout=myArgs.mqtt_timeout)
   except (queue.Empty):
       logger.warning("MQTT message reception timed out")

   currentTimestamp = getCurrentTime()
   if currentTimestamp >= nextUploadTimestamp:
       df = pd.DataFrame.from_dict(accumulator)
       df.to_parquet(filename)
       s3_export_task_definition = S3ExportTaskDefinition(input_url=filename,
 bucket=destination_bucket, key=key_name)
       streammanager.append_message(streamname,
 Util.validate_and_serialize_to_json_bytes(s3_export_task_definition))
       accumulator = {}
       nextUploadTimestamp += period
   else:
        accumulator.append(message)
```

Lanzar un trabajo de Spark en un clúster EMR transitorio mediante una función de Lambda

Dhrubajyoti Mukherjee, Amazon Web Services

Resumen

Este patrón utiliza la acción de la RunJobFlow API Amazon EMR para lanzar un clúster transitorio para ejecutar un trabajo de Spark desde una función de Lambda. Un clúster EMR transitorio está diseñado para finalizar tan pronto como se complete el trabajo o si se produce algún error. Un clúster transitorio permite ahorrar costos porque solo se ejecuta durante el tiempo de cálculo y proporciona escalabilidad y flexibilidad en un entorno de nube.

El clúster EMR transitorio se lanza mediante la API Boto3 y el lenguaje de programación Python en una función de Lambda. La función de Lambda, escrita en Python, proporciona la flexibilidad adicional de iniciar el clúster cuando es necesario.

Para demostrar un ejemplo de cálculo y salida por lotes, este patrón lanzará un trabajo de Spark en un clúster de EMR desde una función de Lambda y ejecutará un cálculo por lotes con los datos de ventas de ejemplo de una empresa ficticia. El resultado del trabajo de Spark será un archivo de valores separados por comas (CSV) en Amazon Simple Storage Service (Amazon S3). El archivo de datos de entrada, el archivo.jar de Spark, un fragmento de código y una CloudFormation plantilla de AWS para una nube privada virtual (VPC) y las funciones de AWS Identity and Access Management (IAM) para ejecutar el cálculo se proporcionan como datos adjuntos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa

Limitaciones

- Solo se puede iniciar un trabajo de Spark a partir del código a la vez.

Versiones de producto

- Probado en Amazon EMR 6.0.0

Arquitectura

Pila de tecnología de destino

- Amazon EMR
- AWS Lambda
- Amazon S3
- Apache Spark

Arquitectura de destino

Automatizar y escalar

Para automatizar el cálculo por lotes de Spark-EMR, puede utilizar cualquiera de las siguientes opciones.

- Implemente una EventBridge regla de Amazon que pueda iniciar la función Lambda en una programación cron. Para obtener más información, consulte el tutorial: Programe funciones de AWS Lambda mediante. EventBridge
- Configure las notificaciones de eventos de Amazon S3 para iniciar la función de Lambda al llegar el archivo.
- Transfiera los parámetros de entrada a la función de AWS Lambda a través del cuerpo del evento y de las variables de entorno de Lambda.

Tools (Herramientas)

Servicios de AWS

- Amazon EMR es una plataforma de clúster administrada que simplifica la ejecución de marcos de macrodatos en AWS para procesar y analizar grandes cantidades de datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

- Apache Spark es un motor de análisis en varios idiomas para el procesamiento de datos a gran escala.

Epics

Cree las funciones de IAM de Amazon EMR y Lambda y la VPC

Tarea	Descripción	Habilidades requeridas
Crear las funciones de IAM y la VPC.	Si ya tiene las funciones de IAM de AWS Lambda y Amazon EMR y una VPC, puede omitir este paso. Para ejecutar el código, tanto el clúster de EMR como la función de Lambda requieren funciones de IAM. El clúster de EMR también requiere una VPC con una subred pública o una subred privada con una gateway NAT. Para crear automáticamente todas las funciones de IAM y una VPC, implemente la plantilla de CloudFormation AWS adjunta tal cual, o bien, puede crear las funciones y la VPC manualmente, tal como se especifica en la sección Información adicional.	Arquitecto de la nube
Anote las claves de salida CloudFormation de la plantilla de AWS.	Una vez que la CloudForm ation plantilla se haya implementado correctamente, vaya a la pestaña Outputs de	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	la CloudFormation consola de AWS. Tenga en cuenta las cinco claves de salida: • `S3Bucket` • `LambdaExecutionRole` • `ServiceRole` • `JobFlowRole` • `Ec2SubnetId` Utilizará los valores de estas claves cuando cree la función de Lambda.	

Cargue el archivo .jar de Spark

Tarea	Descripción	Habilidades requeridas
Subir el archivo.jar de Spark.	Cargue el archivo.jar de Spark en el depósito de S3 que creó la CloudFormation pila de AWS. El nombre del bucket es el mismo que el de la clave de salida`S3Bucket`.	AWS general

Crear la función de Lambda para lanzar el clúster de EMR

Tarea	Descripción	Habilidades requeridas
Creación de una función de Lambda.	En la consola Lambda, cree una función de Lambda de Python 3.9+ con un rol de ejecución. La política de	Ingeniero de datos, ingeniero de nube

Tarea	Descripción	Habilidades requeridas
	funciones de ejecución debe permitir a Lambda lanzar un clúster de EMR. (Consulte la CloudFormation plantilla de AWS adjunta).	
Copie y pegue el código.	Sustituya el código del archivo `lambda_function.py` por el código de la sección de Información adicional de este patrón.	Ingeniero de datos, ingeniero de nube
Cambie los parámetros del código.	Siga los comentarios del código para cambiar los valores de los parámetro s para que se ajusten a su cuenta de AWS.	Ingeniero de datos, ingeniero de nube
Inicie la función para iniciar el clúster.	Inicie la función para iniciar la creación de un clúster EMR transitorio con el archivo .jar de Spark proporcionado. Ejecutará el trabajo de Spark y finalizará automáticamente cuando se complete el trabajo.	Ingeniero de datos, ingeniero de nube
Compruebe el estado del clúster de EMR.	Una vez iniciado el clúster de EMR, aparece en la consola de Amazon EMR, en la pestaña Clústeres. Se puede comprobar en consecuen cia cualquier error que se produzca al lanzar el clúster o al ejecutar el trabajo.	Ingeniero de datos, ingeniero de nube

Crear y ejecutar la ejemplo de ejemplo

Tarea	Descripción	Habilidades requeridas
Subir el archivo.jar de Spark.	Descargar el archivo.jar de Spark de la sección de Adjuntos y cárgalo en el bucket de S3.	Ingeniero de datos, ingeniero de nube
Cargue el conjunto de datos de entrada.	Cargue el archivo `fake_sales_data.csv` en el bucket de S3.	Ingeniero de datos, ingeniero de nube
Pegue el código de Lambda y cambie los parámetros.	Copie el código de la sección Herramientas y péguelo en una función de Lambda, sustituyendo el archivo de código `lambda_function.py` . Cambie los valores de los parámetros para que se ajusten a su cuenta.	Ingeniero de datos, ingeniero de nube
Iniciar la función y verificar la salida.	Una vez que la función de Lambda inicia el clúster con el trabajo de Spark proporcionado, genera un archivo.csv en el bucket de S3.	Ingeniero de datos, ingeniero de nube

Recursos relacionados

- Construyendo Spark
- Apache Spark y Amazon EMR
- Documentación sobre run_job_flow de Boto3 Docs
- Información y documentación de Apache Spark

Información adicional

Código

```
"""
Copy paste the following code in your Lambda function. Make sure to change the
 following key parameters for the API as per your account

-Name (Name of Spark cluster)
-LogUri (S3 bucket to store EMR logs)
-Ec2SubnetId (The subnet to launch the cluster into)
-JobFlowRole (Service role for EC2)
-ServiceRole (Service role for Amazon EMR)

The following parameters are additional parameters for the Spark job itself. Change the
 bucket name and prefix for the Spark job (located at the bottom).

-s3://your-bucket-name/prefix/lambda-emr/SparkProfitCalc.jar (Spark jar file)
-s3://your-bucket-name/prefix/fake_sales_data.csv (Input data file in S3)
-s3://your-bucket-name/prefix/outputs/report_1/ (Output location in S3)
"""
import boto3

client = boto3.client('emr')


def lambda_handler(event, context):
    response = client.run_job_flow(
        Name='spark_job_cluster',
        LogUri='s3://your-bucket-name/prefix/logs',
        ReleaseLabel='emr-6.0.0',
        Instances={
            'MasterInstanceType': 'm5.xlarge',
            'SlaveInstanceType': 'm5.large',
            'InstanceCount': 1,
            'KeepJobFlowAliveWhenNoSteps': False,
            'TerminationProtected': False,
            'Ec2SubnetId': 'subnet-XXXXXXXXXXXXX'
        },
        Applications=[{'Name': 'Spark'}],
        Configurations=[
            {'Classification': 'spark-hive-site',
             'Properties': {
```

```
                'hive.metastore.client.factory.class':
'com.amazonaws.glue.catalog.metastore.AWSGlueDataCatalogHiveClientFactory'}
            }
        ],
        VisibleToAllUsers=True,
        JobFlowRole='EMRLambda-EMREC2InstanceProfile-XXXXXXXXX',
        ServiceRole='EMRLambda-EMRRole-XXXXXXXXX',
        Steps=[
            {
                'Name': 'flow-log-analysis',
                'ActionOnFailure': 'TERMINATE_CLUSTER',
                'HadoopJarStep': {
                    'Jar': 'command-runner.jar',
                    'Args': [
                        'spark-submit',
                        '--deploy-mode', 'cluster',
                        '--executor-memory', '6G',
                        '--num-executors', '1',
                        '--executor-cores', '2',
                        '--class', 'com.aws.emr.ProfitCalc',
                        's3://your-bucket-name/prefix/lambda-emr/SparkProfitCalc.jar',
                        's3://your-bucket-name/prefix/fake_sales_data.csv',
                        's3://your-bucket-name/prefix/outputs/report_1/'
                    ]
                }
            }
        ]
    )
```

Funciones de IAM y creación de VPC

Para lanzar el clúster de EMR en una función de Lambda, se necesitan funciones de VPC e IAM. Puede configurar las funciones de VPC e IAM mediante la CloudFormation plantilla de AWS de la sección de adjuntos de este patrón, o puede crearlas manualmente mediante los siguientes enlaces.

Las siguientes funciones de IAM son necesarias para ejecutar Lambda y Amazon EMR.

Rol de ejecución de Lambda

El rol de ejecución de una función de AWS Lambda concede permiso a la función para que tenga acceso a los servicios y recursos de AWS.

Roles de servicio para Amazon EMR

La función Amazon EMR define las acciones permitidas para Amazon EMR al aprovisionar recursos y realizar tareas de nivel de servicio que no se realizan en el contexto de una instancia de Amazon Elastic Compute Cloud (Amazon) que se ejecuta dentro de un clúster. EC2 Por ejemplo, la función de servicio se utiliza para aprovisionar EC2 instancias cuando se lanza un clúster.

Función de servicio para EC2 instancias

La función de servicio para EC2 las instancias de clúster (también denominada perfil de EC2 instancia para Amazon EMR) es un tipo especial de función de servicio que se asigna a todas las instancias de un clúster de Amazon EMR cuando se lanza la EC2 instancia. Los procesos de aplicación que se ejecutan sobre el ecosistema de Apache asumen este rol para los permisos, e interactuar así con otros servicios de AWS.

Creación de VPC y subredes

Puede crear una VPC desde la consola de VPC.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migración de cargas de trabajo de Apache Cassandra a Amazon Keyspaces mediante AWS Glue

Nikolai Kolesnikov, Karthiga Priya Chandran y Samir Patel, Amazon Web Services

Resumen

Este patrón le muestra cómo migrar sus cargas de trabajo actuales de Apache Cassandra a Amazon Keyspaces (para Apache Cassandra) mediante AWS Glue. CQLReplicator Puede usarlo CQLReplicator en AWS Glue para minimizar el retraso en la replicación que se produce al migrar sus cargas de trabajo en cuestión de minutos. También aprenderá a usar un bucket de Amazon Simple Storage Service (Amazon S3) para almacenar los datos necesarios para la migración, incluidos los archivos de configuración, los scripts y los archivos de Apache Parquet. Este patrón supone que las cargas de trabajo de Cassandra están alojadas en instancias de Amazon Elastic Compute Cloud EC2 (Amazon) en una nube privada virtual (VPC).

Requisitos previos y limitaciones

Requisitos previos

- Clúster de Cassandra con tabla de origen
- Tabla objetivo en Amazon Keyspaces para replicar la carga de trabajo
- Bucket de S3 para almacenar archivos intermedios de Parquet que contienen cambios de datos graduales
- Bucket de S3 para almacenar archivos de configuración de trabajos y scripts

Limitaciones

- CQLReplicator en AWS Glue se necesita algún tiempo para aprovisionar las unidades de procesamiento de datos (DPUs) para las cargas de trabajo de Cassandra. El retraso de la replicación entre el clúster de Cassandra y el espacio de claves y la tabla de destino en Amazon Keyspaces se reducirá a pocos minutos.

Arquitectura

Pila de tecnología de origen

- Apache Cassandra
- DataStax Servidor
- ScyllaDB

Pila de tecnología de destino

- Amazon Keyspaces

Arquitectura de migración

El siguiente diagrama muestra un ejemplo de arquitectura en el que un clúster de Cassandra se aloja en EC2 instancias y se distribuye en tres zonas de disponibilidad. Los nodos de Cassandra están alojados en subredes privadas.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un rol de servicio personalizado proporciona acceso a Amazon Keyspaces y al bucket de S3.
2. Un trabajo de AWS Glue lee la configuración del trabajo y los scripts del bucket de S3.
3. El trabajo de AWS Glue se conecta a través del puerto 9042 para leer los datos del clúster de Cassandra.
4. El trabajo de AWS Glue se conecta a través del puerto 9142 para escribir los datos en Amazon Keyspaces.

Tools (Herramientas)

Servicios y herramientas de AWS

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- AWS CloudShell es un shell basado en navegador que puede utilizar para administrar los servicios de AWS mediante la interfaz de línea de comandos de AWS (AWS CLI) y una gama de herramientas de desarrollo preinstaladas.
- AWS Glue es un servicio de ETL totalmente gestionado que le permite clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.

- Amazon Keyspaces (para Apache Cassandra) es un servicio de base de datos administrada que le permite migrar, ejecutar y escalar sus cargas de trabajo de Cassandra en la nube de AWS.

Código

El código de este patrón está disponible en el repositorio. GitHub CQLReplicator

Prácticas recomendadas

- Para determinar los recursos de AWS Glue necesarios para la migración, calcule el número de filas de la tabla de Cassandra de origen. Por ejemplo, 250 000 filas por 0,25 DPU (2 vCPUs, 4 GB de memoria) con un disco de 84 GB.
- Calienta previamente las mesas de Amazon Keyspaces antes de ponerlas en marcha. CQLReplicator Por ejemplo, ocho CQLReplicator mosaicos (trabajos con AWS Glue) pueden escribir hasta 22 K WCUs por segundo, por lo que el objetivo debe precalentarse entre 25 y 30 K WCUs por segundo.
- Para permitir la comunicación entre los componentes de AWS Glue, utilice una regla de entrada con autorreferencia para todos los puertos TCP del grupo de seguridad.
- Utilice la estrategia de tráfico gradual para distribuir la carga de trabajo de migración a lo largo del tiempo.

Epics

Implemente CQLReplicator

Tarea	Descripción	Habilidades requeridas
Cree un espacio de claves y una tabla de destino.	1. Cree un espacio de claves y una tabla en Amazon Keyspaces. Para obtener más información sobre la capacidad de escritura, consulte Cálculos de unidades de escritura en la sección Información adicional de este patrón.	Propietario de la aplicación, administrador de AWS, administrador de bases de datos, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	También puede crear un espacio de claves mediante el Lenguaje de consultas Cassandra (CQL). Para obtener más información, consulte Creación de un espacio de claves con CQL en la sección de Información adicional de este patrón. **Note** Después de crear la tabla, considere la posibilidad de cambiarla al modo de capacidad bajo demanda para evitar cargos innecesarios. 2. Para actualizar al modo de rendimiento, ejecute el siguiente script: `ALTER TABLE target_keyspace.target_table WITH CUSTOM_PROPERTIES = { 'capacity_mode': { 'throughput_mode': 'PAY_PER_REQUEST'} }`	

Tarea	Descripción	Habilidades requeridas
Configure el controlador de Cassandra para conectarse a Cassandra.	Utilice el siguiente script dde configuración: `Datastax-java-driver { basic.request.consistency = "LOCAL_QUORUM" basic.contact-points = ["127.0.0.1:9042"] advanced.reconnect-on-init = true basic.load-balancing-policy { local-datacenter = "datacenter1" } advanced.auth-provider = { class = PlainTextAuthProvider username = "user-at-sample" password = "S@MPLE=PASSWORD=" } }` **Note** El anterior script usa el conector Spark Cassandra. Para obtener más información, consulte la configuración	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de referencia para Cassandra.	

Tarea	Descripción	Habilidades requeridas
Configure el controlador de Cassandra para conectarse a Amazon Keyspaces.	Utilice el siguiente script dde configuración: `datastax-java-driver { basic { load-balancing-pol icy { local-datacenter = us-west-2 } contact-points = ["cassandr a.us-west-2.amazon aws.com:9142"] request { page-size = 2500 timeout = 360 seconds consistency = LOCAL_QUORUM } } advanced { control-connection { timeout = 360 seconds } session-leak.thres hold = 6 connection { connect-timeout = 360 seconds init-query-timeout = 360 seconds warn-on-init-error = false } auth-provider = { class = software. aws.mcs.auth.SigV4 AuthProvider`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	<pre> aws-region = us-
	west-2
	 }
	
	 ssl-engine-factory {
	  class = DefaultSs
	lEngineFactory
	  }
	  }
	}</pre>
	Note
	El anterior script usa el conector Spark Cassandra. Para obtener más información, consulte la configuración de referencia para Cassandra.	

Tarea	Descripción	Habilidades requeridas
Cree un rol de IAM para el trabajo de AWS Glue.	Cree un nuevo rol de servicio de AWS denominado `glue-cassandra-migration` con AWS Glue como entidad de confianza. **Note** La `glue-cassandra-migration` debería proporcionar acceso de lectura y escritura al bucket de S3 y a Amazon Keyspaces. El bucket de S3 contiene los archivos .jar, los archivos de configuración para Amazon Keyspaces y Cassandra y los archivos Parquet intermedios. Por ejemplo, contiene las políticas administradas `AWSGlueServiceRole` , `AmazonS3FullAccess` y `AmazonKeyspacesFullAccess` .	AWS DevOps

Tarea	Descripción	Habilidades requeridas

CQLReplicator Descárguelo en AWS CloudShell.	Para descargar el proyecto en la carpeta de inicio, ejecute el siguiente comando:
	`git clone https://github.com/aws-samples/cql-replicator.git`
	`cd cql-replicator/glue`
	`# Only for AWS CloudShell, the bc package includes bc and dc. Bc is an arbitrary precision numeric processing arithmetic language`
	`sudo yum install bc -y`	

Modifique los archivos de configuración de referencia.	Copie `CassandraConnector.conf` y `KeyspacesConnector.conf` en el directorio `../glue/conf` de la carpeta del proyecto.	AWS DevOps

Tarea	Descripción	Habilidades requeridas

Inicie el proceso de migración.	El siguiente comando inicializa el CQLReplicator entorno. La inicialización implica copiar los artefactos .jar y crear un conector de AWS Glue, un bucket de S3, un trabajo de AWS Glue, el espacio de claves `migration` y la tabla `ledger`:
	
	`cd cql-replicator/glue/bin`
	`./cqlreplicator --state init --sg '"sg-1","sg-2"' \`
	`--subnet "subnet-XXXXXXXXXXXX" \`
	`--az us-west-2a --region us-west-2 \`
	`--glue-iam-role glue-cassandra-migration \`
	`--landing-zone s3://cql-replicator-1234567890-us-west-2`
	
	Este script incluye los siguientes parámetros:
	
	• `--sg`: grupos de seguridad que permiten el acceso al clúster de Cassandra desde AWS Glue e incluyen la regla de entrada con
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	autorreferencia para todo el tráfico • `--subnet`: subred a la que pertenece el clúster de Cassandra • `--az`: zona de disponibilidad de la subred • `--region`: región de AWS en la que se implementa el clúster de Cassandra • `--glue-iam-role` : permisos del rol de IAM que AWS Glue puede asumir al llamar a Amazon Keyspaces y Amazon S3 en su nombre • `--landing zone`: parámetro opcional para reutilizar un bucket de S3 (si no proporciona ningún valor para el parámetro `--landing zone`, el proceso `init` intentará crear un nuevo bucket para almacenar los archivos de configuración, los artefactos .jar y los archivos intermedios).	

Tarea	Descripción	Habilidades requeridas
Valide la implementación.	Tras ejecutar el comando anterior, la cuenta de AWS debe contener lo siguiente: • El trabajo de CQLReplicator AWS Glue y el conector de AWS Glue en AWS Glue • El bucket de S3 que almacena los artefactos • La `migration` del espacio de claves de destino y la tabla `ledger` en Amazon Keyspaces	AWS DevOps

Corre CQLReplicator

Tarea	Descripción	Habilidades requeridas
Inicie el proceso de migración.	Para operar CQLReplicator en AWS Glue, debe usar el `--state run` comando seguido de una serie de parámetros. Sus requisitos de migración únicos determinan principal mente la configuración precisa de estos parámetros. Por ejemplo, esta configuración puede variar si decide replicar los valores y las actualiza ciones del periodo de vida (TTL) o si descarga objetos que superen 1 MB a Amazon S3.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Para replicar la carga de trabajo del clúster de Cassandra a Amazon Keyspaces, ejecute el siguiente comando: `./cqlreplicator --state run --tiles 8 \ --landing-zone s3://cql-replicator-1234567890-us-west-2 \ --region us-west-2 \ --src-keyspace source_keyspace \ --src-table source_table \ --trg-keyspace taget_keyspace \ --writetime-column column_name \ --trg-table target_table --inc-traffic` El espacio de claves y la tabla de origen son `source_keyspace.source_table` en el clúster de Cassandra. El espacio de claves y la tabla de destino son `target_keyspace.target_table` en Amazon Keyspaces	

Tarea	Descripción	Habilidades requeridas
	. El parámetro `--inc-traffic` ayuda a evitar que el tráfico gradual sobrecargue el clúster de Cassandra y Amazon Keyspaces con un número elevado de solicitudes. Para replicar las actualizaciones, agregue `--writetime-column regular_column_name` a la línea de comandos. La columna normal se utilizará como origen de la marca de tiempo de escritura.	

Supervisión del proceso de migración

Tarea	Descripción	Habilidades requeridas
Valide las filas de Cassandra migradas durante la fase de migración del historial.	Para obtener el número de filas replicadas durante la fase de relleno, ejecute el siguiente comando: `./cqlreplicator --state stats \ --landing-zone s3://cql-replicator-1234567890-us-west-2 \ --src-keyspace source_keyspace --src-table source_table --region us-west-2`	AWS DevOps

Detención del proceso de migración

Tarea	Descripción	Habilidades requeridas
Utilice el comando `cqlreplicator` o la consola de AWS Glue.	Para detener el proceso de migración correctamente, ejecute el siguiente comando: `./cqlreplicator --state request-stop --tiles 8 \ --landing-zone s3://cql-replicator-1234567890-us-west-2 \ --region us-west-2 \ --src-keyspace source_keyspace --src-table source_table` Para detener el proceso de migración de forma inmediata, utilice la consola AWS Glue.	AWS DevOps

Limpieza

Tarea	Descripción	Habilidades requeridas
Elimine los recursos implementados.	El siguiente comando eliminará el trabajo de AWS Glue, el conector, el bucket de S3 y la tabla `ledger` de Keyspaces:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`./cqlreplicator --state cleanup --landing-zone s3://cql-replicator-1234567890-us-west-2`	

Resolución de problemas

Problema	Solución
Los trabajos de AWS Glue fallaron y devolvieron el error de memoria insuficiente (OOM).	1. Cambie el tipo de trabajador (escalado vertical). Por ejemplo, cambie `G0.25X` a `G.1X` o `G.1X` a `G.2X`. Como alternativa, aumente la cantidad de entradas DPUs por trabajo de AWS Glue (escale horizontalmente) CQLReplicator. 2. Inicie el proceso de migración desde el punto en el que se interrumpió. Para reiniciar los CQLReplicator trabajos fallidos, vuelva a ejecutar el `--state run` comando con los mismos parámetros.

Recursos relacionados

- CQLReplicator con AWS Glue README.MD
- Documentación de AWS Glue
- Documentación de Amazon Keyspaces
- Apache Cassandra

Información adicional

Consideraciones sobre la migración

Puede usar AWS Glue para migrar la carga de trabajo de Cassandra a Amazon Keyspaces y, al mismo tiempo, mantener por completo la funcionalidad de sus bases de datos de origen de Cassandra durante el proceso de migración. Una vez completada la replicación, puede transferir sus aplicaciones a Amazon Keyspaces con un retraso de replicación mínimo (inferior a minutos) entre el clúster de Cassandra y Amazon Keyspaces. Para mantener la coherencia de datos, también puede seguir un proceso similar para replicar los datos de nuevo en el clúster de Cassandra desde Amazon Keyspaces.

Cálculos de unidades de escritura

Pongamos que, por ejemplo, desea escribir 500.000.000 con un tamaño de fila de 1 KiB durante una hora. El número total de unidades de escritura de Amazon Keyspaces (WCUs) que necesita se basa en este cálculo:

`(number of rows/60 mins 60s) 1 WCU per row = (500,000,000/(60*60s) * 1 WCU) = 69,444 WCUs required`

La tarifa de 1 hora es de 69.444 WCUs por segundo, pero podría añadir algo de amortiguación a los gastos generales. Por ejemplo, `69,444 * 1.10 = 76,388` WCUs tiene una capacidad adicional del 10 por ciento.

Creación de un espacio de claves con CQL

Para crear un espacio de claves con CQL, ejecute los siguientes comandos:

```
CREATE KEYSPACE target_keyspace WITH replication = {'class': 'SingleRegionStrategy'}
CREATE TABLE target_keyspace.target_table ( userid uuid, level text, gameid int,
 description text, nickname text, zip text, email text, updatetime text, PRIMARY KEY
 (userid, level, gameid) ) WITH default_time_to_live = 0 AND CUSTOM_PROPERTIES =
 {'capacity_mode':{ 'throughput_mode':'PROVISIONED', 'write_capacity_units':76388,
 'read_capacity_units':3612 }} AND CLUSTERING ORDER BY (level ASC, gameid ASC)
```

Migración de Oracle Business Intelligence 12c a la nube de AWS desde servidores en las instalaciones

Lanre (Lan-Ray) Showunmi y Patrick Huang, Amazon Web Services

Resumen

Este patrón muestra cómo migrar Oracle Business Intelligence Enterprise Edition 12c de los servidores locales a la nube de AWS mediante AWS. CloudFormation También describe cómo puede usar otros servicios de AWS para implementar componentes de Oracle BI 12c y obtener alta disponibilidad, seguridad, flexibilidad y capacidad de escalado dinámico.

Para ver una lista de las prácticas recomendadas relacionadas con la migración de Oracle BI 12c a la nube de AWS, consulte la sección de Información adicional de este patrón.

> **Note**
>
> Una práctica recomendada es ejecutar varias migraciones de prueba antes de transferir los datos existentes de Oracle BI 12c a la nube. Estas pruebas le ayudarán a ajustar su enfoque de migración, identificar y solucionar posibles problemas y estimar los requisitos de tiempo de inactividad con mayor precisión.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Conectividad de red segura entre los servidores en las instalaciones y AWS a través de los servicios de AWS Virtual Private Network (AWS VPN) o AWS Direct Connect
- Licencias de software para su sistema operativo Oracle, Oracle BI 12c, Oracle Database, Oracle WebLogic Server y Oracle HTTP Server

Limitaciones

Para obtener más información sobre límites de almacenamiento, consulte la documentación de Amazon Relational Database Service (Amazon RDS) para Oracle.

Versiones de producto

- Oracle Business Intelligence Enterprise Edition 12c
- WebLogic Servidor Oracle 12c
- Oracle HTTP Server 12c
- Oracle Database 12c (o posterior)
- Oracle Java SE 8

Arquitectura

El siguiente diagrama muestra un ejemplo de arquitectura para ejecutar componentes de Oracle BI 12c en la nube de AWS:

En el siguiente diagrama se muestra la arquitectura:

1. Amazon Route 53 para proporcionar la configuración de sistema de nombres de dominio (DNS).
2. Elastic Load Balancing (ELB) distribuye el tráfico de red para mejorar la escalabilidad y la disponibilidad de los componentes de Oracle BI 12c en múltiples zonas de disponibilidad.
3. Los grupos de Auto Scaling de Amazon Elastic Compute Cloud (Amazon EC2) alojan los servidores HTTP de Oracle, el servidor Weblogic Admin y los servidores de BI gestionados en varias zonas de disponibilidad.
4. Amazon Relational Database Service (Amazon RDS) para bases de datos de Oracle almacena metadatos de BI Server en varias zonas de disponibilidad.
5. Amazon Elastic File System (Amazon EFS) está montado en todos los componentes de Oracle BI 12c para el almacenamiento de archivos compartidos.

Pila de tecnología

- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic File System (Amazon EFS)
- Amazon RDS para Oracle

- AWS Certificate Manager (ACM)
- Elastic Load Balancing (ELB)
- Oracle BI 12c
- WebLogic Servidor Oracle 12c
- Oracle HTTP Server (OHS)

Tools (Herramientas)

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS Certificate Manager (ACM) le ayuda a crear, almacenar y renovar claves y certificados SSL/TLS X.509 públicos y privados que protegen sus sitios web y aplicaciones de AWS.
- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon EC2 Auto Scaling le ayuda a mantener la disponibilidad de las aplicaciones y le permite añadir o eliminar automáticamente EC2 instancias de Amazon según las condiciones que defina.
- Amazon Elastic File System (Amazon EFS) le ayuda a crear y configurar sistemas de archivos compartidos en la nube de AWS.
- Elastic Load Balancing permite distribuir el tráfico entrante de las aplicaciones entre distintos destinos. Por ejemplo, puede distribuir el tráfico entre instancias, contenedores y direcciones IP de Amazon Elastic Compute Cloud (Amazon EC2) en una o más zonas de disponibilidad.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.
- Oracle Data Pump le ayuda a trasladar datos y metadatos de una base de datos a otra a altas velocidades.

- Oracle Fusion Middleware es un conjunto de herramientas de desarrollo de aplicaciones y soluciones de integración para la gestión de identidades, la colaboración y la generación de informes de inteligencia empresarial.
- Oracle le GoldenGate ayuda a diseñar, ejecutar, organizar y supervisar sus soluciones de procesamiento de datos y de replicación de datos en streaming en Oracle Cloud Infrastructure.
- La herramienta Oracle WebLogic Scripting Tool (WLST) proporciona una interfaz de línea de comandos que le ayuda a escalar horizontalmente sus clústeres. WebLogic

Epics

Evalúe el entorno de origen

Tarea	Descripción	Habilidades requeridas
Recopile información sobre el inventario de software.	Identifique las versiones y los niveles de parches de cada uno de los component es de software de su pila de tecnología de origen, incluidos los siguientes: • El sistema operativo de Oracle • Oracle Database • Oracle BI 12c • Servidor Oracle WebLogic • Servidor de Oracle HTTP • Java	Arquitecto de migración, arquitecto de soluciones, propietario de la aplicación, administrador de Oracle BI
Recopile información sobre el inventario de cómputo y almacenamiento.	En su entorno de origen, revise las métricas de uso actuales e históricas para comprobar lo siguiente: • Uso de la CPU • Uso de memoria	Arquitecto de migración, arquitecto de soluciones, propietario de la aplicación, administrador de Oracle BI, administrador de sistema

Tarea	Descripción	Habilidades requeridas
	• Uso del almacenamiento ⚠ Important Asegúrese de tener en cuenta los picos históricos de uso.	
Recopile información sobre la arquitectura del entorno de origen y sus requisitos.	Comprenda por completo la arquitectura de su entorno de origen y sus requisito s, incluidos los siguientes aspectos: • Configuración WebLogic del dominio de Oracle Server • Agrupamiento en clústeres • Equilibrio de carga • Conectividad • Disponibilidad. • Requisitos de recuperación de desastres	Arquitecto de migración, arquitecto de soluciones, propietario de la aplicación, administrador de Oracle BI
Identifique orígenes de datos de Java Database Connectiv ity (JDBC).	Recopile información sobre los orígenes de datos JDBC y los controladores de su entorno de origen para cada motor de base de datos que utilice.	Arquitecto de migración, propietario de la aplicación, administrador de Oracle BI, ingeniero o administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Recopile información sobre la configuración específica del entorno.	Recopile información sobre los ajustes y configuraciones específicos de su entorno de origen, incluidos los siguientes: • Scripts de inicio y cierre personalizados • Java y otras variables de entorno • Certificados	Arquitecto de migración, arquitecto de soluciones, propietario de la aplicación, administrador de Oracle BI
Identifique cualquier dependencia de otras aplicaciones.	Recopile información sobre las integraciones de su entorno de origen que crean dependencias con otras aplicaciones. **Important** Asegúrese de identificar las integraciones de Lightweight Directory Access Protocol (LDAP) y otros requisitos de red.	Arquitecto de migración, arquitecto de soluciones, propietario de la aplicación, administrador de Oracle BI

Diseñe su entorno de destino

Tarea	Descripción	Habilidades requeridas
Cree un documento de diseño de alto nivel.	Cree un documento de diseño de arquitectura de destino. Asegúrese de usar	Arquitecto de soluciones, arquitecto de aplicaciones,

Tarea	Descripción	Habilidades requeridas
	la información que recopiló al evaluar su entorno de origen para elaborar el documento de diseño.	ingeniero de bases de datos, arquitecto de migraciones
Obtenga la aprobación del documento de diseño.	Revise el documento de diseño con las partes interesadas y obtenga las aprobaciones necesarias.	Propietario de la aplicación o servicio, arquitecto de soluciones, arquitecto de aplicaciones

Implementación de la infraestructura

Tarea	Descripción	Habilidades requeridas
Prepare el código de infraestructura en CloudFormation.	Cree CloudFormation plantillas para aprovisionar su infraestructura de Oracle BI 12c en la nube de AWS. Para obtener más información, consulte Trabajar con CloudFormation plantillas de AWS en la Guía del CloudFormation usuario de AWS. **Note** Se recomienda crear CloudFormation plantillas modulares para cada nivel de Oracle BI 12c, en lugar de crear una plantilla grande para	Arquitecto de infraestructura de nube, arquitecto de soluciones y arquitecto de aplicaciones

Tarea	Descripción	Habilidades requeridas
	todos los recursos. Para obtener más información sobre las prácticas CloudForm ation recomendadas, consulte 8 prácticas recomendadas para automatizar las implementaciones con AWS CloudFormation en el blog de AWS.	
Descargue el software necesario.	DDownload el siguiente software junto con las versiones y los parches necesarios del sitio web de Oracle: • Java JDK8 • WebLogic Servidor Oracle 12c • Oracle BI 12c	Arquitecto de migraciones, ingeniero de bases de datos, arquitecto de aplicaciones

Tarea	Descripción	Habilidades requeridas
Prepare los scripts de instalación.	Cree scripts de instalación de software que ejecuten una instalación silenciosa. Estos scripts simplifican la automatización de la implementación. Para obtener más información, consulte OBIEE 12c: ¿Cómo realizar una instalación silenciosa? en el sitio de Oracle Support. Necesitará una cuenta de Oracle Support para acceder a estos documentos.	Arquitecto de migraciones, ingeniero de bases de datos, arquitecto de aplicaciones

Tarea	Descripción	Habilidades requeridas
Cree una AMI de Linux con respaldo Amazon EBS para los niveles de web y aplicaciones.	1. Implemente y configure EC2 instancias de Amazon para sus niveles web y de aplicaciones. Asegúrese de que las instancias cumplan los requisitos previos para ejecutar lo siguiente: • Entorno de sistema operativo Oracle configurado • Cuenta de usuario de sistema operativo Oracle configurada • Instalación de software Java 2. Cree Amazon Machine Images (AMIs) de las instancias y guarde copias para usarlas en el futuro. Para obtener instrucciones, consulte Creación de una AMI de Linux respaldada por Amazon EBS en la Guía EC2 del usuario de Amazon para instancias de Linux.	Arquitecto de migraciones, ingeniero de bases de datos, arquitecto de aplicaciones

Tarea	Descripción	Habilidades requeridas
Lance su infraestructura de AWS mediante CloudFormation.	Implemente sus niveles web y de aplicaciones de Oracle BI 12c en módulos mediante las CloudFormation plantillas que ha creado. Para obtener instrucciones, consulte Introducción a AWS CloudFormation en la Guía del CloudFormation usuario de AWS.	Arquitecto de infraestructura de nube, arquitecto de soluciones y arquitecto de aplicaciones

Migración de Oracle BI 12c a AWS mediante una instalación nueva

Tarea	Descripción	Habilidades requeridas
Prepare el software necesario.	Coloca el software necesario en una ubicación a la que puedan acceder las EC2 instancias de Amazon. Por ejemplo, puede instalar el software en Amazon S3 u otra EC2 instancia de Amazon a la que puedan acceder sus servidores web y de aplicaciones.	Arquitecto de migración, arquitecto de Oracle BI, arquitecto de infraestructura en la nube, arquitecto de soluciones y arquitecto de aplicaciones
Prepare la base de datos del repositorio para la instalación de Oracle BI 12c.	Cree esquemas de Oracle BI 12c ejecutando la utilidad de creación de repositorios de Oracle (RCU) en una nueva instancia de base de datos Amazon RDS para Oracle.	Arquitecto de infraestructura en la nube, arquitecto de soluciones, arquitecto de aplicaciones, arquitecto de migración, arquitecto de Oracle BI

Tarea	Descripción	Habilidades requeridas
Instale Oracle Fusion Middleware 12c y Oracle BI 12c.	1. A partir de una EC2 instancia de Amazon, instale la infraestructura Oracle Fusion Middlewar e 12c y OBIEE 12c. Para obtener más información, consulte las siguientes secciones de la Guía de implementación empresarial de Oracle Fusion Middlewar e para Oracle Business Intelligence: • Iniciar el instalador de infraestructura en BIHOST1 • Instalación de Oracle Business Intelligence como preparación para una implementación empresarial **Note** Utilice Amazon EFS para alojar los directorios que se compartirán entre los nodos del clúster de Oracle BI 12c. 2. Aplique los parches necesarios a la instalación.	Arquitecto de migración, arquitecto de Oracle BI

Tarea	Descripción	Habilidades requeridas
	3. Cree AMIs las instancias y guarde las copias para usarlas en el futuro.	
Configure su dominio WebLogic de Oracle Server para Oracle BI 12c.	Configure su dominio de Oracle BI 12c como implement ación no agrupada en clúster. Para obtener más informaci ón, consulte Configurar el dominio BI en la Guía de implementación empresarial de Oracle Fusion Middleware para Oracle Business Intellige nce.	Arquitecto de migración, arquitecto de Oracle BI
Realice un escalado horizontal a partir de Oracle BI 12c.	Escale horizontalmente el nodo único hasta el número deseado de nodos. Para obtener más información, consulte Escalado horizonta l de Oracle Business Intellige nce en la Guía de implement ación empresarial de Oracle Fusion Middleware para Oracle Business Intelligence.	Arquitecto de migración, arquitecto de Oracle BI

Tarea	Descripción	Habilidades requeridas
Instale el servidor HTTP 12c de Oracle.	1. Instale el servidor HTTP 12c de Oracle en las EC2 instancias de Amazon de nivel web de Oracle. Para obtener más instrucciones, consulte Instalación del servidor HTTP 12c de Oracle en Instalación y configuración del servidor HTTP de Oracle para Oracle Access Management 12c. 2. Aplique los parches necesarios a la instalación. 3. Cree AMIs las instancias y guarde las copias para usarlas en el futuro.	Arquitecto de migración, arquitecto de Oracle BI
Configure los equilibradores de carga para la finalización de SSL.	1. Solicite o importe un certificado en ACM. 2. Asocie los certificados SSL con ELB.	Arquitecto de infraestructura de nube, arquitecto de migraciones

Tarea	Descripción	Habilidades requeridas
Migre los artefactos de metadatos de inteligencia empresarial a AWS.	1. Exporte los archivos de Oracle Business Intelligence Application Archive (BAR) desde la instalación de Oracle BI 12c en las instalaciones. Para exportar los archivos BAR, utilice la herramienta de WebLogic secuencias de comandos (WLST) para ejecutar el exportServiceInstancecomando. 2. Importe los archivos BAR en las instalaciones a la instalación de AWS Oracle BI 12c. Para importar los archivos BAR, ejecute el comando importServiceInstanceWLST.	Arquitecto de migración, arquitecto de Oracle BI

Tarea	Descripción	Habilidades requeridas
Realice las tareas posteriores a la migración.	Después de importar los archivos BAR, haga lo siguiente: • Configure cualquier origen de datos JDBC adicional. • Instale controladores para otros orígenes de datos, como PostgreSQL o Amazon Redshift. • Configure LDAP, SSL, el inicio de sesión único (SSO) y el almacén de seguridad de Oracle. WebLogic • Configuración de políticas de AWS Identity and Access Management (IAM). • Active el seguimiento del uso. • Configure integraciones con otros sistemas. • Migre cualquier script personalizado.	Arquitecto de migración, arquitecto de Oracle BI

Pruebe el nuevo entorno

Tarea	Descripción	Habilidades requeridas
Pruebe el nuevo entorno de Oracle BI 12c.	Realice end-to-end pruebas en el nuevo entorno Oracle BI 12c. Utilice la automatización en la medida de lo posible.	Arquitecto de migración, arquitecto de soluciones, propietario de la aplicación, administrador de Oracle BI

Tarea	Descripción	Habilidades requeridas
	A continuación se muestran ejemplos de actividades de prueba: • Validación de paneles, informes y URLs • Pruebas de aceptación de usuarios (UAT) • Pruebas de aceptación operativa (OAT) **Note** Lleve a cabo pruebas y validaciones adicionales según sea necesario.	

Realizar la transición al nuevo entorno

Tarea	Descripción	Habilidades requeridas
Desconecte el tráfico al entorno Oracle BI 12c en las instalaciones.	En la ventana de transición designada, detenga todo el tráfico al entorno Oracle BI 12c en las instalaciones.	Arquitecto de migración, arquitecto de soluciones, propietario de la aplicación, administrador de Oracle BI
Vuelva a sincronizar la nueva base de datos del repositorio Oracle BI 12c con la base de datos de origen.	Vuelva a sincronizar la base de datos del repositorio Oracle Oracle BI 12c de Amazon RDS con la base de datos en las instalaciones.	Administrador de BI, ingeniero /administrador de bases de datos de Oracle

Tarea	Descripción	Habilidades requeridas
	Para sincronizar las bases de datos, puede realizar una actualización de Oracle Data Pump o una captura de datos de cambios (CDC) de AWS DMS.	
Cambie su Oracle BI 12c URLs para que apunte al nuevo entorno de AWS.	Actualice Oracle BI 12c URLs en sus servidores DNS internos para que apunten a la nueva instalación de AWS.	Arquitecto de migración, arquitecto de soluciones, propietario de la aplicación, administrador de Oracle BI
Supervise el nuevo entorno.	Supervise el nuevo entorno de Oracle BI 12c con cualquier a de las siguientes herramien tas: • Amazon CloudWatch • Amazon RDS Performance Insights • Oracle Enterprise Manager	Administrador de Oracle BI, ingeniero/administrador de bases de datos, administrador de aplicaciones
Obtenga la aprobación del proyecto.	Revise los resultados de las pruebas con las partes interesadas y obtenga las aprobaciones necesarias para finalizar la migración.	Propietario de la aplicació n, propietario del servicio, arquitecto de infraestructura de nube, arquitecto de migración, arquitecto de BI de Oracle

Recursos relacionados

- Uso de Oracle Repository Creation Utility en Amazon RDS para Oracle (Guía de usuario de Amazon RDS)
- Amazon RDS en Oracle (Guía de usuario de Amazon RDS)
- Oracle WebLogic Server 12c en AWS (documento técnico de AWS)

- Implementación de Oracle Business Intelligence para una alta disponibilidad (Centro de ayuda de Oracle)
- Archivos Oracle Business Intelligence Application (BAR) (Centro de ayuda de Oracle)
- Cómo migrar OBI 12c entre entornos (Soporte de Oracle)

Información adicional

La siguiente es una lista de prácticas recomendadas relacionadas con la migración de Oracle BI 12c a la nube de AWS.

Bases de datos de repositorio

Se recomienda alojar los esquemas de bases de datos de Oracle BI 12c en una instancia de Amazon RDS para Oracle. Este tipo de instancia proporciona una capacidad rentable y redimensionable, a la vez que automatiza tareas de administración como el aprovisionamiento de hardware, la configuración de bases de datos, la aplicación de parches y las copias de seguridad.

Para obtener más información, consulte Uso de la utilidad de creación de repositorios de Oracle en RDS para Oracle en la Guía del usuario de Amazon RDS.

Niveles web y de aplicaciones

Las EC2 instancias de Amazon con memoria optimizada suelen ser adecuadas para los servidores Oracle BI 12c. Sea cual sea el tipo de instancia que elija, asegúrese de que las instancias que aprovisione cumplan con los requisitos de uso de memoria del sistema. Además, asegúrate de configurar un tamaño de pila de máquina virtual WebLogic Java (JVM) suficiente en función de la memoria disponible de tu EC2 instancia de Amazon.

Almacenamiento local

La E/S desempeña un papel importante en el rendimiento general de su aplicación Oracle BI 12c. Amazon Elastic Block Store (Amazon EBS) ofrece diferentes clases de almacenamiento optimizadas para distintos patrones de carga de trabajo. Asegúrese de elegir un tipo de volumen de Amazon EBS que se adapte a su caso de uso.

Para obtener más información acerca de tipo de volúmenes de EBS, consulte Características de Amazon EBS en la documentación de Amazon EBS.

Almacenamiento compartido

Un dominio Oracle BI 12c agrupado en clúster requiere almacenamiento compartido para los siguientes recursos:

- Archivos de configuración
- Directorio de datos singleton (SDD) de Oracle BI 12c
- Caché global de Oracle
- Scripts de Oracle BI Scheduler
- Binarios de Oracle Server WebLogic

Puede satisfacer este requisito de almacenamiento compartido con Amazon EFS, que proporciona un sistema de archivos Network File System (NFS) elástico, escalable y totalmente administrado.

Optimizar el rendimiento del almacenamiento compartido

Amazon EFS tiene dos modos de rendimiento: aprovisionado y en ráfaga. El servicio también tiene dos modos de rendimiento: de uso general y de E/S máxima.

Para ajustar el rendimiento, comience por probar sus cargas de trabajo en el modo de rendimiento de uso general y en el modo de rendimiento aprovisionado. Realizar estas pruebas le ayudará a determinar si dichos modos de referencia son suficientes para cumplir con los niveles de servicio deseados.

Para obtener más información, consulte Rendimiento de Amazon EFS en la Guía del usuario de Amazon EFS.

Disponibilidad y recuperación de desastres

Se recomienda implementar los componentes de Oracle BI 12c en varias zonas de disponibilidad para proteger los recursos en caso de que se produzca un fallo en una zona de disponibilidad. La siguiente lista incluye las prácticas recomendadas de disponibilidad y recuperación de desastres para recursos específicos de Oracle BI 12c alojados en la nube de AWS:

- Bases de datos de repositorios Oracle BI 12c: implemente una instancia de base de datos de Amazon RDS con múltiples zonas de disponibilidad en su base de datos de repositorios Oracle BI 12c. En un despliegue Multi-AZ, Amazon RDS aprovisiona y mantiene automáticamente una réplica en espera sincrónica en una AZ diferente. Ejecutar una instancia de base de datos de repositorio de Oracle BI 12c entre regiones de alta disponibilidad puede mejorar la disponibilidad durante el mantenimiento de sistema planificado y ayuda a proteger sus bases de datos contra los errores de las instancias de base de datos y las interrupciones de las zonas de disponibilidad.

- Servidores gestionados Oracle BI 12c: Para lograr la tolerancia a errores, se recomienda implementar los componentes del sistema Oracle BI 12c en los servidores gestionados de un grupo de Amazon EC2 Auto Scaling configurado para abarcar varias zonas de disponibilidad. Auto Scaling reemplaza las instancias defectuosas según los controles de EC2 estado de Amazon. En caso de que se produzca un error en la zona de disponibilidad, los servidores HTTP de Oracle seguirán dirigiendo el tráfico a los servidores gestionados de la zona de disponibilidad en funcionamiento. Después, Auto Scaling lanzará instancias para cumplir con sus requisitos de recuento de hosts. Se recomienda activar la replicación del estado de la sesión HTTP para garantizar que las sesiones existentes se conmuten por error a los servidores gestionados en funcionamiento.
- Servidores de administración Oracle BI 12c: para asegurarse de que su Servidor de administración tiene alta disponibilidad, hospételo en un grupo de Amazon EC2 Auto Scaling configurado para abarcar varias zonas de disponibilidad. A continuación, defina el tamaño mínimo y máximo del grupo en 1. Si se produce un error en una zona de disponibilidad, Amazon EC2 Auto Scaling inicia un servidor de administración de reemplazo en una zona de disponibilidad alternativa. Para recuperar cualquier host subyacente que haya fallado dentro de la misma zona de disponibilidad, puede activar Amazon EC2 Auto Recovery.
- Servidores Oracle Web Tier: se recomienda asociar su servidor HTTP de Oracle con su dominio de Oracle WebLogic Server. Para obtener una alta disponibilidad, despliegue su servidor HTTP de Oracle en un grupo de Amazon EC2 Auto Scaling configurado para abrir múltiples zonas de disponibilidad. A continuación, instale el servidor detrás de un equilibrador de carga elástico ELB. Para ofrecer protección adicional contra errores en el host, puede activar Amazon EC2 Auto Recovery.

Escalabilidad

La elasticidad de la nube de AWS le ayuda a escalar las aplicaciones horizontal o verticalmente en respuesta a las necesidades de su carga de trabajo.

Escalado vertical

Para escalar verticalmente la aplicación, puede cambiar el tamaño y el tipo de las EC2 instancias de Amazon en las que se ejecutan los componentes de Oracle BI 12c. No necesita aprovisionar en exceso las instancias al inicio de la implementación, ni incurrir en costos innecesarios.

Escalado horizontal

Amazon EC2 Auto Scaling le ayuda a escalar horizontalmente su aplicación al añadir o eliminar automáticamente servidores gestionados en función de los requisitos de carga de trabajo.

> **Note**
>
> El escalado horizontal con Amazon EC2 Auto Scaling requiere habilidades de creación de scripts y pruebas exhaustivas para su implementación.

Copia de seguridad y recuperación

La siguiente lista incluye las prácticas recomendadas de disponibilidad y recuperación de desastres para recursos específicos de Oracle BI 12c alojados en la nube de AWS:

- Repositorios de metadatos de Oracle Business Intelligence: Amazon RDS crea y guarda automáticamente copias de seguridad de las instancias de sus bases de datos. Estas copias de seguridad se retienen durante el período que usted especifique. Asegúrese de configurar la duración y retención de las copias de seguridad de Amazon RDS en función de sus requisitos de protección de datos. Para obtener información adicional, consulte Copia de seguridad y restauración de Amazon RDS.
- Servidores gestionados, servidores de administración y servidores de nivel web: asegúrese de configurar las instantáneas de Amazon EBS en función de sus requisitos de protección y retención de datos.
- Almacenamiento compartido: puede gestionar las copias de seguridad y la recuperación de los archivos almacenados en Amazon EFS mediante AWS Backup. El servicio AWS Backup también se puede implementar para gestionar de forma centralizada las copias de seguridad y la recuperación de otros servicios, como Amazon EC2, Amazon EBS y Amazon RDS. Para obtener más información, consulte ¿Qué es AWS Backup? En la guía para desarrolladores de AWS Lambda.

Seguridad y conformidad

La siguiente lista de prácticas recomendadas de seguridad y servicios de AWS puede ayudarle a proteger sus aplicaciones de Oracle BI 12c en la nube de AWS:

- Cifrado en reposo: Amazon RDS, Amazon EFS y Amazon EBS son compatibles con los algoritmos de cifrado estándar del sector. Puede utilizar AWS Key Management Service (AWS KMS) para crear y administrar claves criptográficas, así como a controlar su uso en una amplia gama de

servicios de AWS y en sus aplicaciones. También puede configurar Oracle Transparent Data Encryption (TDE) en la instancia de base de datos Amazon RDS para Oracle que aloja la base de datos del repositorio Oracle BI 12c.

- Cifrado en tránsito: se recomienda activar los protocolos SSL o TLS para proteger los datos en tránsito entre las distintas capas de la instalación de Oracle BI 12c. Puede usar AWS Certificate Manager (ACM) para aprovisionar, administrar e implementar certificados SSL y TLS públicos y privados para los recursos de Oracle BI 12c.
- Seguridad de la red: asegúrese de implementar los recursos de Oracle BI 12c en una VPC de Amazon con los controles de acceso adecuados configurados para su caso de uso. Configure sus grupos de seguridad para filtrar el tráfico entrante y saliente de las EC2 instancias de Amazon en las que se ejecuta la instalación. Además, asegúrese de configurar las listas de control de acceso a la red (NACLs) que permitan o denieguen el tráfico en función de las reglas definidas.
- Supervisión y registro: puede utilizar AWS CloudTrail para realizar un seguimiento de las llamadas a las API a su infraestructura de AWS, incluidos los recursos de Oracle BI 12c. Esta funcionalidad resulta útil para supervisar los cambios en la infraestructura o para realizar análisis de seguridad. También puede utilizar Amazon CloudWatch para ver datos operativos que le proporcionarán información útil sobre el rendimiento y el estado de su aplicación Oracle BI 12c. Puede configurar alarmas y tomar medidas automatizadas en función de esas alarmas. Amazon RDS proporciona herramientas de supervisión adicionales, incluidas Enhanced Monitoring y Performance Insights.

Migración de ELK Stack a Elastic Cloud en AWS

Battulga Purevragchaa y Antony Prasad Thevaraj, Amazon Web Services

uday reddy, None

Resumen

Elastic ha prestado servicios durante muchos años y, por lo general, sus usuarios y clientes administran Elastic ellos mismos en las instalaciones. Elastic Cloud, el servicio gestionado de Elasticsearch, proporciona una forma de consumir Elastic Stack (ELK Stack) y soluciones de búsqueda empresarial, observabilidad y seguridad. Puede acceder a las soluciones de Elastic con aplicaciones de registro, métricas, APM (supervisión del rendimiento de las aplicaciones) y SIEM (administración de eventos e información de seguridad). También puede usar características integradas como machine learning, gestión de ciclo de vida de índices y Kibana Lens (para visualizaciones de arrastrar y soltar).

Cuando transiciona de Elasticsearch autogestionado a Elastic Cloud, el servicio de Elasticsearch se ocupa de lo siguiente:

- Aprovisionamiento y administración de la infraestructura subyacente
- Creación y administración de clústeres de Elasticsearch
- Escalado vertical y horizontal de los clústeres
- Actualizaciones, parches y toma de instantáneas

Todo esto le brinda más tiempo para resolver otros desafíos.

Este patrón define cómo migrar de Elasticsearch 7.13 en las instalaciones a Elasticsearch en Elastic Cloud en Amazon Web Services (AWS). Es posible que otras versiones requieran pequeñas modificaciones de los procesos descritos en este patrón. Para obtener más información, contacte con su representante de Elastic.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa con acceso a Amazon Simple Storage Service (Amazon S3) para las instantáneas

- Un enlace privado seguro y con un ancho de banda suficientemente alto para copiar archivos de datos de instantáneas a Amazon S3
- Amazon S3 Transfer Acceleration
- Políticas de Elastic Snapshot para garantizar que la ingesta de datos se archive con regularidad, ya sea en un almacén de datos local lo suficientemente grande o en un almacenamiento remoto (Amazon S3)

Debe conocer el tamaño de sus instantáneas y las políticas de ciclo de vida de los índices correspondientes en las instalaciones antes de iniciar la migración. Para obtener más información, póngase en contacto con Elastic.

Roles y habilidades

El proceso de migración también requiere los roles y la experiencia que se describen en la siguiente tabla.

Rol	Experiencia	Responsabilidades
Compatibilidad con aplicaciones	Familiaridad con Elastic Cloud y Elastic en las instalaciones	Todas las tareas relacionadas con Elastic
Administrador de sistemas o administrador de base de datos	Conocimiento profundo del entorno de Elastic en las instalaciones y su configuración	Capacidad de aprovisionar almacenamiento, instalar y usar la Interfaz de la línea de comandos de AWS (AWS CLI) e identificar todos los orígenes de datos que alimentan Elastic en las instalaciones
Administrador de red	Conocimiento de la conectividad, la seguridad y el rendimiento de la red en las instalaciones a AWS	Creación de enlaces de red desde las instalaciones a Amazon S3 y conocimiento del ancho de banda de conectividad

Limitaciones

- Elasticsearch en Elastic Cloud solo está disponible en regiones de AWS compatibles (septiembre de 2021).

Versiones de producto

- Elasticsearch 7.13

Arquitectura

Pila de tecnología de origen

Elasticsearch 7.13 o posterior en las instalaciones:

- Instantáneas del clúster
- Instantáneas de índice
- Configuración de Beats

Arquitectura de la tecnología de origen

El siguiente diagrama muestra una arquitectura típica en las instalaciones con diferentes métodos de ingesta, tipos de nodos y Kibana. Los distintos tipos de nodos reflejan las funciones de clúster, autenticación y visualización de Elasticsearch.

1. Ingestión de Beats a Logstash
2. Ingestión de Beats a cola de mensajes de Apache Kafka
3. Ingestión de Filebeat a Logstash
4. Ingestión de cola de mensajes de Apache Kafka a Logstash
5. Ingestión de Logstash a clúster de Elasticsearch
6. Clúster de destino de Elasticsearch
7. Nodo de autenticación y notificación
8. Nodos de Kibana y blob

Pila de tecnología de destino

Elastic Cloud se implementa en su cuenta de software como servicio (SaaS) en varias regiones de AWS con replicación entre clústeres.

- Instantáneas del clúster
- Instantáneas de índice
- Configuraciones de Beats
- Elastic Cloud
- Equilibrador de carga de red
- Amazon Route 53
- Amazon S3

Arquitectura de destino

La infraestructura gestionada de Elastic Cloud es:

- De alta disponibilidad, ya que está presente en varias zonas de disponibilidad y varias regiones de AWS.
- Tolerante a fallos en la región, ya que los datos (índices e instantáneas) se replican mediante la replicación entre clústeres (CCR) de Elastic Cloud
- De archivo, porque las instantáneas se archivan en Amazon S3
- Tolerante a particiones de red mediante una combinación de equilibradores de carga de red y Route 53
- La ingesta de datos se origina, entre otros, en Elastic APM, Beats y Logstash

Pasos de migración de alto nivel

Elastic ha desarrollado su propia metodología prescriptiva para migrar de Elastic Cluster en las instalaciones a Elastic Cloud. La metodología de Elastic está directamente alineada y complementa la guía y las prácticas recomendadas de migración de AWS, incluidos el marco Well-Architected y el Programa de aceleración de la migración (MAP). Por lo general, las tres fases de migración a AWS son las siguientes:

- Evaluación
- Movilización

- Migración y modernización

Elastic sigue fases de migración similares con terminología complementaria:

- Iniciar
- Planificar
- Implementar
- Entregar
- Cerrar

Elastic usa la metodología de implementación de Elastic para facilitar la entrega de los resultados del proyecto. Su diseño es inclusivo para garantizar que Elastic, los equipos de consultoría y los equipos de cliente trabajen juntos con claridad para lograr, de forma conjunta, los resultados esperados.

La metodología de Elastic combina fases tradicionales en cascada con Scrum en la fase de implementación. Las configuraciones de los requisitos técnicos se proporcionan de forma iterativa y colaborativa, minimizando el riesgo.

Tools (Herramientas)

Servicios de AWS

- Amazon Route 53: Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad. Puede utilizar Route 53 para realizar tres funciones principales en cualquier combinación: registro de dominio, direccionamiento DNS y comprobación de estado.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web. Este patrón emplea un bucket de S3 y Amazon S3 Transfer Acceleration.
- Elastic Load Balancing: Elastic Load Balancing distribuye automáticamente el tráfico entrante entre varios destinos, como EC2 instancias, contenedores y direcciones IP, en una o más zonas de disponibilidad.

Otras herramientas

- Beats: Beats envía datos desde Logstash o Elasticsearch
- Elastic Cloud: Elastic Cloud es un servicio gestionado para alojar Elasticsearch.
- Elasticsearch: Elasticsearch es un motor de búsqueda y análisis que usa Elastic Stack para almacenar de forma centralizada los datos con el fin de realizar búsquedas y análisis escalables. Este patrón también emplea creación de instantáneas y replicación entre clústeres.
- Logstash: Logstash es un sistema de procesamiento de datos del servidor que ingiere datos de varias fuentes, los transforma y, a continuación, los envía al almacenamiento de datos.

Epics

Preparativos para la migración

Tarea	Descripción	Habilidades requeridas
Identifique los servidores que ejecutan la solución Elastic en las instalaciones.	Confirme que se puede realizar la migración a Elastic.	Propietario de la aplicación
Comprenda la configuración del servidor en las instalaciones.	Para comprender la configuración del servidor necesaria para gestionar correctamente las cargas de trabajo en las instalaciones, averigüe el tamaño del hardware del servidor, la configuración de la red y las características del almacenamiento actual	Compatibilidad con aplicaciones
Recopile la información del usuario y de la cuenta de la aplicación.	Identifique los nombres de usuario y los nombres de las aplicaciones que emplea el entorno de Elastic en las instalaciones.	Administrador de sistemas, soporte de aplicaciones
Documente la configuración de Beats y del remitente de datos.	Para documentar las configuraciones, consulte los orígenes de datos y los receptores de	Compatibilidad con aplicaciones

Tarea	Descripción	Habilidades requeridas
	datos existentes. Para obtener más información, consulte la documentación de Elastic.	
Determine la velocidad y el volumen de los datos.	Establezca una línea base para la cantidad de datos que gestiona el clúster.	Administrador de sistemas, soporte de aplicaciones
Documente los escenarios de RPO y RTO.	Documente los escenario s de objetivo de punto de recuperación (RPO) y objetivo de tiempo de recuperac ión (RTO) en términos de interrupciones y acuerdos de nivel de servicio (). SLAs	Propietario de aplicaciones, administrador de sistemas, soporte de aplicaciones
Determine la configuración óptima del ciclo de vida de las instantáneas.	Defina la frecuencia con la que se deben proteger los datos mediante el uso de instantáneas de Elastic durante y después de la migración.	Propietario de aplicaciones, administrador de sistemas, soporte de aplicaciones
Defina las expectativas de rendimiento tras la migración.	Genere métricas sobre las actualizaciones de pantalla actuales y esperadas, los tiempos de ejecución de las consultas y el comportamiento de la interfaz de usuario.	Administrador de sistemas, soporte de aplicaciones
Documente los requisitos de acceso a Internet, ancho de banda y disponibilidad.	Compruebe la velocidad, la latencia y la resistencia de las conexiones a Internet para copiar instantáneas en Amazon S3.	Administrador de red

Tarea	Descripción	Habilidades requeridas
Documente los costos actuales del tiempo de ejecución de Elastic en las instalaciones.	Asegúrese de que el tamaño del entorno de destino de AWS esté diseñado para ser rentable y de alto rendimiento.	Administrador de base de datos, administrador de sistemas, soporte de aplicaciones
Identifique las necesidades de autenticación y autorización.	Las características de seguridad de Elastic Stack proporcionan dominios integrados, como Protocolo ligero de acceso a directorios (LDAP), lenguaje de marcado de aserciones de seguridad (SAML) y OpenID Connect (OIDC).	Administrador de base de datos, administrador de sistemas, soporte de aplicaciones
Conozca los requisitos regulatorios específicos en función de la ubicación geográfica.	Asegúrese de que los datos se exportan y cifran según sus necesidades y los requisitos regulatorios pertinentes.	Administrador de base de datos, administrador de sistemas, soporte de aplicaciones

Implemente la migración

Tarea	Descripción	Habilidades requeridas
Prepare el área de almacenamiento en Amazon S3.	Para recibir instantáneas en Amazon S3, cree un bucket de S3 y un rol temporal de AWS Identity and Access Management (IAM) con acceso total al bucket recién creado. Para obtener más información, consulte Creación de un rol para delegar permisos a un usuario de IAM. También	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	puede utilizar AWS Security Token Service para solicitar credenciales de seguridad temporales. Proteja la ID de clave de acceso, la clave de acceso secreta y el token de sesión. Activar Amazon S3 Transfer Acceleration en el bucket.	
Instale AWS CLI y el complemento Amazon S3 en las instalaciones.	En cada nodo de Elasticse arch, ejecute el siguiente comando. `sudo bin/elasticsearch-plugin install repository-s3` A continuación, reinicie el nodo.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

Configure el acceso de cliente de Amazon S3.	Añada las claves creadas anteriormente ejecutando los siguientes comandos.
	`elasticsearch-keystore add s3.client.default.access_key`
	`elasticsearch-keystore add s3.client.default.secret_key`
	`elasticsearch-keystore add s3.client.default.session_token`
		Administrador de AWS

Registre un repositorio de instantáneas para los datos de Elastic	Use Kibana Dev Tools para indicar al clúster local en las instalaciones en qué bucket remoto de S3 debe escribir.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure la política de instantáneas.	Para configurar la administración del ciclo de vida de las instantáneas, en la pestaña Políticas de Kibana, seleccione Política de SLM y defina qué horas, flujos de datos o índices deben incluirse y qué nombres usar. Configure una política que tome instantáneas frecuentes. Las instantáneas son graduales, y hacen un uso eficiente del almacenamiento. Adecue esta configuración a la evaluación realizada. La política también puede especificar una política de retención y eliminar automáticamente las instantáneas cuando ya no las necesite.	Compatibilidad con aplicaciones
Compruebe que las instantáneas funcionan.	En Kibana Dev Tools, ejecute el siguiente comando. `GET _snapshot/<your_repo_name>/_all`	Administrador de sistemas, soporte de aplicaciones
Implemente un nuevo clúster en Elastic Cloud.	Inicie sesión en Elastic y elija un clúster de “observabilidad, búsqueda o seguridad” según el resultado de la evaluación de preparación empresarial llevada a cabo.	Administrador de sistemas, soporte de aplicaciones

Tarea	Descripción	Habilidades requeridas
Configure el acceso al almacén de claves del clúster.	El nuevo clúster debe tener acceso al bucket de S3 que almacenará las instantáneas. En la consola de servicio de Elasticsearch, seleccione Seguridad e introduzca las claves de acceso y de IAM secretas que creó anteriorm ente.	Administrador de AWS
Configure el clúster alojado de Elastic Cloud para acceder a Amazon S3.	Configure un nuevo acceso de clúster al repositorio de instantáneas creado anteriorm ente en Amazon S3. También puede hacer lo siguiente de Kibana: 1. Elija Stack Managemen t, Snapshot Settings,. RegisterRepo 2. En el campo Alias, introduzca el nombre del repositorio. 3. En Nombre del cliente de S3, seleccione secundario. 4. Agregue al repositorio el bucket de S3 que creó anteriormente. 5. Seleccione Comprimir instantánea. 6. En la sección de Cifrado, mantenga la configuración predeterminada.	Administrador de sistemas, soporte de aplicaciones

Tarea	Descripción	Habilidades requeridas
Verifique el nuevo repositorio de Amazon S3.	Asegúrese de poder acceder a su nuevo repositorio alojado en el clúster de Elastic Cloud.	Administrador de AWS

Inicialice el clúster de servicios de Elasticsearch.	En la consola de servicio de Elasticsearch, inicialic e el clúster de servicios de Elasticsearch a partir de la instantánea de S3.
	
	Ejecute los siguientes comandos como POST.
	
	`*/_close?expand_wi ldcards=all`
	
	`/_snapshot/<your-r epo-name>/ <your-sna pshot-name>/_restore`
	
	`*/_open?expand_wil dcards=all`
		Soporte de aplicaciones

Complete la migración

Tarea	Descripción	Habilidades requeridas
Compruebe que la restaurac ión de la instantánea se ha realizado correctamente.	En Kibana Dev Tools, ejecute el siguiente comando. `GET _cat/indices`	Compatibilidad con aplicacio nes
Vuelva a implementar los servicios de ingestión.	Conecte los puntos de conexión de Beats y Logstash	Compatibilidad con aplicacio nes

Tarea	Descripción	Habilidades requeridas
	al nuevo punto de conexión del servicio Elasticsearch.	

Pruebe el entorno del clúster y límpielo

Tarea	Descripción	Habilidades requeridas
Valide el entorno del clúster.	Tras migrar el entorno de clúster de Elastic en las instalaciones a AWS, puede conectarse a él y usar sus propias herramientas de pruebas de aceptación de usuarios (UAT) para validar el nuevo entorno.	Compatibilidad con aplicaciones
Limpie los recursos.	Tras validar la correcta migración del clúster, elimine el bucket de S3 y el rol de IAM usado para la migración.	Administrador de AWS

Recursos relacionados

Referencias de Elastic

- Elastic Cloud
- Elasticsearch gestionado y Kibana en AWS
- Búsqueda empresarial de Elastic
- Integraciones de Elastic
- Observabilidad de Elastic
- Seguridad de Elastic
- Beats
- Elastic APM

- Migración a gestión de ciclo de vida de índice
- Suscripciones de Elastic
- Contacte con Elastic

Publicaciones de blog de Elastic

- Cómo migrar de Elasticsearch autogestionado a Elastic Cloud en AWS (publicación de blog)
- Migrar a Elastic Cloud (publicación de blog)

Documentación de Elastic

- Tutorial: Automatice las copias de seguridad con SLM
- ILM: gestión del ciclo de vida del índice
- Logstash
- Replicación entre clústeres (CCR)
- Procesos de ingesta
- Ejecute solicitudes de API de Elasticsearch
- Retención de instantáneas

Video y seminario web de Elastic

- Migración a Elastic Cloud
- Elastic Cloud: ¿Por qué migran los clientes? (seminario web)

Referencias de AWS

- Elastic Cloud en AWS Marketplace
- Interfaz de línea de comandos de AWS
- AWS Direct Connect
- Programa de aceleración de la migración AWS
- Equilibrador de carga de red
- Regiones y zonas de disponibilidad
- Amazon Route 53

- Amazon Simple Storage Service
- Amazon S3 Transfer Acceleration
- Conexiones de VPN
- Marco de buena arquitectura

Información adicional

Si desea migrar cargas de trabajo complejas, contrate los servicios de consultoría de Elastic. Si tiene dudas básicas sobre las configuraciones y los servicios, contacte con el equipo de soporte de Elastic.

Migre datos al Nube de AWS mediante Starburst

Antony Prasad Thevaraj y Suresh Veeragoni, Amazon Web Services

Shaun Van Staden, ninguno

Resumen

Starburst ayuda a acelerar su migración de datos a Amazon Web Services (AWS) con un motor de consultas empresarial que reúne los orígenes de datos existentes en un único punto de acceso. Puede realizar análisis en varios orígenes de datos para obtener información valiosa antes de finalizar cualquier plan de migración. Sin interrumpir el business-as-usual análisis, puede migrar los datos mediante el motor Starburst o una aplicación dedicada a extraer, transformar y cargar (ETL).

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Una nube privada virtual (VPC)
- Un clúster de Amazon Elastic Kubernetes Service (Amazon EKS)
- Un grupo de Auto Scaling de Amazon Elastic Compute Cloud (Amazon EC2)
- Lista de las cargas de trabajo actuales del sistema que deben migrarse
- Conectividad de red desde AWS su entorno local

Arquitectura

Arquitectura de referencia

En el siguiente diagrama de arquitectura de alto nivel se muestra una implementación típica de Starburst Enterprise en la Nube de AWS:

1. El clúster de Starburst Enterprise se ejecuta en su Cuenta de AWS.
2. El usuario se autentica mediante el Protocolo ligero de acceso a directorios (LDAP) o la autorización abierta (OAuth) e interactúa directamente con el clúster de Starburst.
3. Starburst puede conectarse a varias fuentes de AWS datos AWS Glue, como Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS) y Amazon

Redshift. Starburst proporciona capacidades de consulta federadas en todas las fuentes de datos en entornos de nube Nube de AWS, locales o en otros entornos de nube.

4. Para lanzar Starburst Enterprise en un clúster de Amazon EKS, use gráficos de Helm.
5. Starburst Enterprise utiliza los grupos de Amazon EC2 Auto Scaling y Amazon EC2 Spot Instances para optimizar la infraestructura.
6. Starburst Enterprise se conecta directamente a sus orígenes de datos existentes en las instalaciones para leer los datos en tiempo real. Además, si ya tiene una implementación de Starburst Enterprise en este entorno, puede conectar directamente su nuevo clúster de Starburst en él Nube de AWS a este clúster existente.

Tenga en cuenta lo siguiente:

- Starburst no es una plataforma de virtualización de datos. Es un motor de consultas de procesamiento paralelo masivo (MPP) basado en SQL que conforma la base de una estrategia global de malla de datos para el análisis.
- Cuando Starburst se implementa como parte de una migración, tiene conectividad directa con la infraestructura existente en las instalaciones.
- Starburst proporciona varios conectores empresariales y de código abierto integrados que facilitan la conectividad con diferentes sistemas heredados. Para obtener una lista completa de los conectores y sus capacidades, consulte Conectores en la Guía del usuario de Starburst Enterprise.
- Starburst puede consultar datos en tiempo real desde orígenes de datos en las instalaciones. Esto permite migrar los datos sin interrumpir las operaciones empresariales habituales.
- Si vas a migrar desde una implementación local de Starburst Enterprise existente, puedes usar un conector especial, Stargate, para conectar tu clúster de Starburst Enterprise directamente a tu clúster local. AWS Esto proporciona beneficios de rendimiento adicionales cuando los usuarios empresariales y los analistas de datos federan las consultas de su entorno local. Nube de AWS

Descripción general del proceso

Puede acelerar los proyectos de migración de datos con Starburst, ya que Starburst le permite obtener información de todos sus datos antes de migrarlos. La siguiente imagen muestra el proceso típico de migración de datos mediante Starburst.

Roles

Por lo general, son necesarios los siguientes roles para completar una migración con Starburst:

- Administrador de la nube: responsable de que los recursos de la nube estén disponibles para ejecutar la aplicación Starburst Enterprise
- Administrador de Starburst: responsable de instalar, configurar, administrar y dar soporte a la aplicación Starburst
- Ingeniero de datos: responsable de:
  - Migración de los datos antiguos a la nube
  - Crear vistas semánticas para respaldar la analítica
- Propietario de la solución o del sistema: responsable de la implementación general de la solución

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática escalable en el Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar AWS Kubernetes sin necesidad de instalar o mantener su propio plano de control o nodos de Kubernetes.

Otras herramientas

- Helm: Helm es un administrador de paquetes para Kubernetes que le ayuda a instalar y administrar aplicaciones en su clúster de Kubernetes.
- Starburst Enterprise: Starburst Enterprise es un motor de consulta de procesamiento paralelo masivo (MPP) basado en SQL que constituye la base de una estrategia global de malla de datos para análisis.
- Starburst Stargate: vincula los catálogos y los orígenes de datos de un entorno de Starburst Enterprise, como un clúster de un centro de datos en las instalaciones, con los catálogos y orígenes de datos de otro entorno de Starburst Enterprise, como un clúster en la Nube de AWS.

Epics

Evalúe los datos

Tarea	Descripción	Habilidades requeridas
Identifique y priorice sus datos.	Identifique los datos que desea transferir. Los grandes sistemas heredados en las instalaciones pueden incluir datos cruciales que desee migrar y, además, datos que no quiera o pueda mover por motivos de cumplimie nto. Comenzar inventari ando sus datos le ayudará a priorizar cuáles deben migrarse primero. Para obtener más información, consulte Introducción a la detección automática de cartera.	Ingeniero de datos, Administr ador de base de datos
Explore, realice un inventario y haga copias de seguridad de sus datos.	Valide la calidad, cantidad y relevancia de los datos según su caso de uso. Realice copias de seguridad o cree una instantánea de los datos según sea necesario, y finalice el entorno de destino para los datos.	Ingeniero de datos, Administr ador de base de datos

Configure el entorno Starburst Enterprise

Tarea	Descripción	Habilidades requeridas
Configure Starburst Enterprise en la Nube de AWS.	Mientras se catalogan los datos, configure Starburst Enterprise en un clúster gestionado de Amazon EKS. Para obtener más información, consulte Implementación con Kubernetes en la Documenta ción de referencia de Starburst Enterprise. Esto permite realizar análisis mientras la migración de datos está en proceso. business-as-usual	Administrador de AWS, desarrollador de aplicaciones
Connect Starburst a los orígenes de datos.	Una vez que haya identific ado los datos y configurado Starburst Enterprise, conecte Starburst a los orígenes de datos. Starburst lee los datos directamente del origen de datos como una consulta SQL. Para más información, consulte la documentación de referencia de Starburst Enterprise.	Administrador de AWS, desarrollador de aplicaciones

Migración de datos

Tarea	Descripción	Habilidades requeridas
Cree y ejecute los procesos de ETL.	Comience el proceso de migración de datos. Esta actividad se puede	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	realizar al mismo tiempo que la business-as-usual analítica. Puede realizar la migración con Starburst o con un producto de terceros. Starburst puede leer y escribir datos en diferentes fuentes. Para más información, consulte la documentación de referencia de Starburst Enterprise.	
Valide los datos.	Una vez migrados los datos, valídelos para asegurarse de que todos los datos necesarios se hayan trasladado y estén intactos.	Ingeniero de datos, DevOps ingeniero

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Transicione los datos.	Una vez finalizada la migración y validación de los datos, puede realizar la transición. Deberá cambiar los enlaces de conexión de datos en Starburst. En lugar de apuntar a las fuentes en las instalaciones, apunte a las nuevas fuentes en la nube y actualice las vistas semánticas. Para más información, consulte Conectores en la	Ingeniero de datos, responsable de transición

Tarea	Descripción	Habilidades requeridas
	documentación de referencia de Starburst Enterprise.	
Implemente para los usuarios.	Los consumidores de datos comienzan a trabajar con los orígenes de datos migrados. Este proceso es invisible para los usuarios finales de análisis.	Responsable de transición; Ingeniero de datos

Recursos relacionados

AWS Marketplace

- Starburst Galaxy
- Starburst Enterprise
- Datos de Starburst JumpStart
- Starburst Enterprise con Graviton

Documentación de Starburst

- Guía del usuario de Starburst Enterprise
- Documentación de referencia de Starburst Enterprise

Otra documentación AWS

- Comience con la detección automática de carteras (guía AWS prescriptiva)
- Optimización del costo y el rendimiento de la infraestructura en la nube con Starburst on AWS (AWS entrada del blog)

Optimice la incorporación ETL del tamaño del archivo de entrada en AWS

Apoorva Patrikar, Amazon Web Services

Resumen

Este patrón muestra cómo optimizar el paso de incorporación del proceso de extracción, transformación y carga (ETL) para macrodatos y cargas de trabajo de Apache Spark en AWS Glue optimizando el tamaño de los archivos antes de procesarlos. Puede usar este patrón para evitar o resolver el problema de los archivos pequeños. Es decir, cuando un gran número de archivos pequeños ralentiza el procesamiento de datos debido al tamaño agregado de los archivos. Por ejemplo, cientos de archivos de solo unos pocos cientos de kilobytes cada uno pueden reducir considerablemente la velocidad de procesamiento de datos de sus trabajos de AWS Glue. Esto se debe a que AWS Glue realiza funciones de lista internas en Amazon Simple Storage Service (Amazon S3), y YARN (Yet Another Resource Negotiator) debe almacenar una gran cantidad de metadatos. Para mejorar la velocidad del procesamiento de datos, puede usar la agrupación de modo que sus tareas de ETL lean un grupo de archivos de entrada en una sola partición en memoria. La partición agrupa automáticamente los archivos más pequeños. Como alternativa, puede usar un código personalizado para añadir lógica de lotes a los archivos existentes.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Uno o más trabajos de AWS Glue
- Una o más cargas de trabajo de macrodatos o Apache Spark
- Un bucket de S3

Arquitectura

El siguiente patrón muestra cómo un trabajo de AWS Glue procesa los datos en distintos formatos y, a continuación, los almacena en un bucket de S3 para obtener visibilidad del rendimiento.

En el diagrama, se muestra el siguiente flujo de trabajo:

1.
> **Note**
>
> Un trabajo de AWS Glue convierte archivos pequeños en formato CSV, JSON y Parquet en marcos dinámicos. : El tamaño del archivo de entrada es lo que más influye en el rendimiento del trabajo de AWS Glue.

2. El trabajo de AWS Glue realiza funciones de lista internas en un bucket de S3.

Tools (Herramientas)

- AWS Glue es un servicio ETL completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Epics

Use la agrupación para optimizar la incorporación de ETL durante la lectura

Tarea	Descripción	Habilidades requeridas
Especifique el tamaño del grupo.	Si tiene más de 50 000 archivos, la agrupación se habilita de forma predeterminada. Sin embargo, también puede agrupar menos de 50 000 archivos especificando el tamaño del grupo en el parámetro `connectionOptions` . El parámetro `connectionOptions` está en el método `create_dynamic_frame.from_options` .	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
Escriba el código de agrupamiento.	Use el método `create_dynamic_frame` para crear un marco dinámico. Por ejemplo: `S3bucket_node1 = glueContext.create_dynamic_frame.from_options(format_options={"multiline": False}, connection_type="s3", format="json", connection_options={ "paths": ["s3://bucket/prefix/file.json"], "recurse": True, "groupFiles": 'inPartition', "groupSize": 1048576 }, transformation_ctx="S3bucket_node1",)`  **Note** Use `groupFiles` para agrupar archivos en un grupo de particiones de Amazon S3. Se usa `groupSize` para	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	establecer el tamaño objetivo del grupo que se va a leer en la memoria. Especifique `groupSize` en bytes (1048576 = 1 MB).	
Añada el código al flujo de trabajo.	Añada el código de agrupación a su flujo de trabajo en AWS Glue.	Ingeniero de datos

Use lógica personalizada para optimizar la incorporación de ETL

Tarea	Descripción	Habilidades requeridas
Elija el lenguaje y la plataforma de procesamiento.	Elija el lenguaje de scripting y la plataforma de procesamiento adecuados a su caso de uso.	Arquitecto de la nube
Escribir el código.	Escriba la lógica personalizada para agrupar sus archivos.	Arquitecto de la nube
Añada el código al flujo de trabajo.	Añada el código a su flujo de trabajo en AWS Glue. Esto permite que su lógica personalizada se aplique cada vez que se ejecute el trabajo.	Ingeniero de datos

Vuelva a crear particiones al escribir datos después de la transformación

Tarea	Descripción	Habilidades requeridas
Analice los patrones de consumo.	Descubra cómo las aplicaciones posteriores usarán los datos que escriba. Por ejemplo, si consultan datos todos los días y solo crea particiones de los datos por región o tiene archivos de salida muy pequeños, como 2,5 KB por archivo, esto no es óptimo para el consumo.	Administrador de base de datos
Vuelva a crear particiones de los datos antes de escribir.	Cree las nuevas particiones en función de uniones o consultas durante el procesamiento (según la lógica de procesamiento) y después del procesamiento (según el consumo). Por ejemplo, vuelva a crear particiones en función del tamaño de los bytes, como `.repartition(100000)` , o vuelva a crear particiones en función de las columnas, como `.repartition("column_name")` .	Ingeniero de datos

Recursos relacionados

- Lectura de archivos de entrada en grupos más grandes
- Supervisión de AWS Glue
- Supervisión de AWS Glue mediante CloudWatch métricas de Amazon

- Monitorización y depuración de trabajo
- Introducción a ETL sin servidor en AWS Glue

Información adicional

Determinar el tamaño del archivo

No existe una forma sencilla de determinar si el tamaño de un archivo es demasiado grande o demasiado pequeño. El impacto del tamaño del archivo en el rendimiento del procesamiento dependerá de la configuración del clúster. En Hadoop básico, se recomienda usar archivos de 128 MB o 256 MB para aprovechar al máximo el tamaño del bloque.

Para la mayoría de las cargas de trabajo de archivos de texto en AWS Glue, recomendamos un tamaño de archivo de entre 100 MB y 1 GB para un clúster de 5 a 10 DPU. Para determinar el tamaño óptimo de los archivos de entrada, supervise la sección de preprocesamiento de su trabajo de AWS Glue y, a continuación, compruebe el uso de CPU y memoria del trabajo.

Consideraciones adicionales

Si el rendimiento en las primeras etapas de la ETL supone un obstáculo, considere agrupar o fusionar los archivos de datos antes de procesarlos. Si controla por completo el proceso de generación de archivos, puede resultar aún más eficiente agregar puntos de datos en el propio sistema de origen antes de enviar los datos sin procesar a AWS.

Organice una canalización de ETL con validación, transformación y particionamiento mediante AWS Step Functions

Sandip Gangapadhyay, Amazon Web Services

Resumen

Este patrón describe cómo crear un proceso de extracción, transformación y carga (ETL) sin servidor para validar, transformar, comprimir y particionar un conjunto de datos CSV de gran tamaño con el fin de optimizar el rendimiento y los costos. La canalización está orquestada por funciones de gestión de errores, reintentos automatizados AWS Step Functions y notificación al usuario, e incluye estas funciones.

Cuando se carga un archivo CSV a una carpeta de origen en un bucket de Amazon Simple Storage Service (Amazon S3), el proceso de ETL comienza a ejecutarse. El proceso valida el contenido y el esquema del archivo CSV de origen, transforma el archivo CSV a un formato comprimido de Apache Parquet, particiona el conjunto de datos por año, mes y día y lo almacena en una carpeta independiente para que las herramientas de análisis lo procesen.

El código que automatiza este patrón está disponible en el GitHub repositorio ETL Pipeline with. AWS Step Functions

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.
- AWS Command Line Interface (AWS CLI) instalado y configurado con su Cuenta de AWS, para que pueda crear AWS recursos mediante el despliegue de una AWS CloudFormation pila. Recomendamos usar la AWS CLI versión 2. Para obtener instrucciones, consulte Instalación o actualización a la última versión de AWS CLI en la AWS CLI documentación. Para obtener instrucciones de configuración, consulte los ajustes de configuración y del archivo de credenciales en la AWS CLI documentación.
- Un bucket de Amazon S3.
- Un conjunto de datos CSV con el esquema correcto. (El repositorio de código incluido en este patrón proporciona un archivo CSV de muestra con el esquema y tipo de datos correctos para su uso).

- Un navegador web compatible con. Consola de administración de AWS(Consulte la lista de los navegadores compatibles).
- AWS Glue acceso a la consola.
- AWS Step Functions acceso a la consola.

Limitaciones

- En AWS Step Functions, el límite máximo para conservar los registros del historial es de 90 días. Para obtener más información, consulte las cuotas de servicio de Step Functions en la AWS Step Functions documentación.

Versiones de producto

- Python 3.13 para AWS Lambda
- AWS Glue versión 4.0

Arquitectura

El flujo de trabajo que se muestra en el diagrama consta de los siguientes pasos de alto nivel:

1. El usuario carga un archivo CSV en la carpeta de origen de Amazon S3.
2. Un evento de notificación de Amazon S3 inicia una AWS Lambda función que inicia la máquina de AWS Step Functions estados.
3. La función de Lambda valida el esquema y el tipo de datos del archivo CSV sin procesar.
4. En función de los resultados de la validación:
   a. Si la validación del archivo de origen se realiza correctamente, el archivo se mueve a la carpeta transitoria para su posterior procesamiento.
   b. Si el archivo no se valida, se mueve a la carpeta de errores y se envía una notificación de error a través de Amazon Simple Notification Service (Amazon SNS).
5. Un AWS Glue rastreador crea el esquema del archivo sin procesar a partir de la carpeta del escenario en Amazon S3.
6. Un AWS Glue trabajo transforma, comprime y particiona el archivo sin procesar en formato Parquet.

7. El AWS Glue trabajo también mueve el archivo a la carpeta de transformación de Amazon S3.
8. El AWS Glue rastreador crea el esquema a partir del archivo transformado. El esquema resultante se puede utilizar en cualquier trabajo de análisis. Puede utilizar Amazon Athena para ejecutar consultas ad-hoc.
9. Si el proceso se completa sin errores, el archivo de esquema se mueve a la carpeta de almacenamiento. Si se encuentra algún error, el archivo se mueve a la carpeta de errores.
10. Amazon SNS envía una notificación en la que se indica el éxito o el error en función del estado de finalización del proceso.

Todos los AWS recursos utilizados en este patrón no tienen servidor. No es necesario administrar servidores.

Tools (Herramientas)

Servicios de AWS

- AWS Glue— AWS Glue es un servicio ETL totalmente gestionado que facilita a los clientes la preparación y carga de sus datos para su análisis.
- AWS Step Functions— AWS Step Functions es un servicio de organización sin servidor que le permite combinar AWS Lambda funciones y otras Servicios de AWS para crear aplicaciones críticas para la empresa. A través de la consola AWS Step Functions gráfica, puede ver el flujo de trabajo de su aplicación como una serie de pasos basados en eventos.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento líderes del sector.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio de mensajería de alta disponibilidad, duradero, seguro y totalmente pub/sub gestionado que le permite desvincular microservicios, sistemas distribuidos y aplicaciones sin servidor.
- AWS Lambda— AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. AWS Lambda ejecuta el código solo cuando es necesario y se escala automáticamente, desde unas pocas solicitudes por día hasta miles por segundo.

Código

El código de este patrón está disponible en el GitHub AWS Step Functions repositorio ETL Pipeline with. El repositorio de código contiene los siguientes archivos y carpetas:

- `template.yml`— AWS CloudFormation plantilla con la que crear la canalización de ETL AWS Step Functions.
- `parameter.json` – Contiene todos los parámetros y valores de los parámetros. Actualice este archivo para cambiar los valores de los parámetros, tal y como se describe en la sección Épica.
- `myLayer/python`carpeta: contiene los paquetes de Python necesarios para crear la AWS Lambda capa requerida para este proyecto.
- Carpeta `lambda` – Contiene las siguientes funciones de Lambda:
  - `move_file.py` – Mueve el conjunto de datos de origen a la carpeta de almacenamiento, transformación o errores.
  - `check_crawler.py`— Comprueba el estado del AWS Glue rastreador tantas veces como lo haya configurado la variable de `RETRYLIMIT` entorno antes de enviar un mensaje de error.
  - `start_crawler.py`— Inicia el AWS Glue rastreador.
  - `start_step_function.py`— Empieza AWS Step Functions.
  - `start_codebuild.py`— Inicia el AWS CodeBuild proyecto.
  - `validation.py` – Valida el conjunto de datos sin procesar de entrada.
  - `s3object.py`: crea la estructura de directorios requerida dentro del bucket de Amazon S3.
  - `notification.py` – Envía notificaciones de éxito o error al final del proceso.

Para usar el código de muestra, siga las instrucciones en la sección Epics .

Epics

Preparación del archivo de origen

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código de muestra.	1. Abra el repositorio ETL Pipeline with AWS Step Functions. 2. Elija Código en la página principal del repositorio, sobre la lista de archivos, y copie la URL que aparece en Clonar con HTTPS.	Desarrollador

Tarea	Descripción	Habilidades requeridas
	3. Cambie el directorio de trabajo a la ubicación en la que desee almacenar los archivos de muestra. 4. Ejecute el siguiente comando en un terminal o en la línea de comandos: `git clone <repoURL>` `<repoURL>` es la URL que copió en el paso 2.	

Tarea	Descripción	Habilidades requeridas
Actualice los valores de los parámetros.	En la copia local del repositorio, edite el archivo `parameter.json` y actualice los valores de los parámetros predeterminados de la siguiente manera: • `pS3BucketName` : el nombre del bucket de Amazon S3 para almacenar los conjuntos de datos. La plantilla creará este bucket automáticamente. El nombre del bucket tiene que ser único de forma global. • `pSourceFolder` : el nombre de la carpeta en el bucket de Amazon S3 que se usará para cargar el archivo CSV de origen. • `pStageFolder` : el nombre de la carpeta en el bucket de Amazon S3 que se usará como área transitoria durante el proceso. • `pTransformFolder` : el nombre de la carpeta en el bucket de Amazon S3 que se usará para almacenar conjuntos de datos transformados y particion ados.	Desarrollador

Tarea	Descripción	Habilidades requeridas
	• `pErrorFolder` : la carpeta en el bucket de Amazon S3 a la que se moverá el archivo CSV de origen si no se puede validar. • `pArchiveFolder` : el nombre de la carpeta en el bucket de Amazon S3 que se usará para archivar el archivo CSV de origen. • `pEmailforNotification` — Una dirección de correo electrónico válida para recibir success/error notificaciones. • `pPrefix`— Una cadena de prefijo que se utilizará en el nombre del AWS Glue rastreador. • `pDatasetSchema` : el esquema del conjunto de datos con el que se validará el archivo de origen. Para la validación del conjunto de datos de origen se usa el paquete Python Cerberus. Para obtener más información, consulte el sitio web de Cerberus.	

Tarea	Descripción	Habilidades requeridas
Cargue el código fuente en el bucket de Amazon S3.	Antes de implementar la AWS CloudFormation plantilla que automatiza la canalización de ETL, debe empaqueta r los archivos fuente de la plantilla y subirlos a un bucket de Amazon S3. Para ello, ejecute el siguiente AWS CLI comando con su perfil preconfigurado: `aws cloudformation package --template-file template.yml --s3-bucket <bucket_name> --output-template-file packaged.template --profile <profile_name>` donde: • `<bucket_name>` es el nombre de un bucket de Amazon S3 existente Región de AWS en el que desea implementar la pila. Este depósito se utiliza para almacenar el paquete de código fuente de la CloudFormation plantilla. • `<profile_name>` es un AWS CLI perfil válido que preconfiguró al configurarla. AWS CLI	Desarrollador

Creación de la pila

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla.	Para implementar la AWS CloudFormation plantilla, ejecute el siguiente AWS CLI comando: `aws cloudformation deploy --stack-name <stack_name> --template-file packaged.template --parameter-overrides file://parameter.json --capabilities CAPABILITY_IAM --profile <profile_name>` donde: • `<stack_name>` es un identificador único de la CloudFormation pila. • `<profile-name>` es su AWS CLI perfil preconfigurado.	Desarrollador
Compruebe el progreso.	En la consola de AWS CloudFormation, compruebe el progreso del desarrollo de la pila. Cuando el estado sea `CREATE_COMPLETE` , la pila se habrá implementado correctamente.	Desarrollador
Anote el nombre de la AWS Glue base de datos.	La pestaña Salidas de la pila muestra el nombre de	Desarrollador

Tarea	Descripción	Habilidades requeridas
	la AWS Glue base de datos. El nombre de la clave es `GlueDBOutput` .	

Prueba la canalización

Tarea	Descripción	Habilidades requeridas
Inicie el proceso de ETL.	1. Navegue hasta la carpeta de origen (`source` o el nombre de carpeta que haya establecido en el archivo `parameter.json`) en el bucket de Amazon S3. 2. Cargue un archivo CSV de muestra en esta carpeta. (El repositorio de código proporciona un archivo de muestra llamado `Sample_Bank_Transaction_Raw_Dataset.csv` para su uso). Al cargar el archivo, se iniciará el proceso de ETL a través de Step Functions. 3. En la consola de Step Functions, compruebe el estado del proceso de ETL.	Desarrollador
Compruebe el conjunto de datos particionado.	Cuando se complete el proceso de ETL, compruebe que el conjunto de datos particionado esté disponibl	Desarrollador

Tarea	Descripción	Habilidades requeridas
	e en la carpeta de transform ación de Amazon S3 (`transform` , o el nombre de carpeta que haya estableci do en el archivo `parameter .json`).	
Comprueba la base de AWS Glue datos particionada.	1. En la AWS Glue consola, selecciona la AWS Glue base de datos creada por la pila (esta es la base de datos que mencionaste en la epopeya anterior). 2. Compruebe que la tabla particionada esté disponibl e en el AWS Glue Data Catalog.	Desarrollador
Ejecutar consultas.	(Opcional) Use Amazon Athena para ejecutar consultas ad hoc en la base de datos particionada y transformada. Para obtener instrucciones, consulte Ejecutar consultas SQL en Amazon Athena en la AWS documentación.	Análisis de la base de datos

Resolución de problemas

Problema	Solución
AWS Identity and Access Management (IAM) para el AWS Glue trabajo y el rastreador	Si sigue personalizando el AWS Glue trabajo o el rastreador, asegúrese de conceder los

Problema	Solución
	permisos de IAM adecuados en la función de IAM utilizada por el AWS Glue trabajo o de proporcionarle permisos de datos. AWS Lake Formation Para obtener más información, consulte la Documentación de AWS.

Recursos relacionados

Servicio de AWS documentación

- AWS Step Functions
- AWS Glue
- AWS Lambda
- Amazon S3
- Amazon SNS

Información adicional

El siguiente diagrama muestra el AWS Step Functions flujo de trabajo para una canalización de ETL exitosa, desde el panel del AWS Step Functions Inspector.

El siguiente diagrama muestra el AWS Step Functions flujo de trabajo de una canalización de ETL que falla debido a un error de validación de entrada, desde el panel Step Functions Inspector.

Realizar análisis avanzados mediante Amazon Redshift ML

Po Hong y Chyanna Antonio, Amazon Web Services

Resumen

En la nube de Amazon Web Services (AWS), puede utilizar el machine learning de Amazon Redshift (Amazon Redshift ML) para realizar análisis de ML de los datos almacenados en un clúster de Amazon Redshift o en Amazon Simple Storage Service (Amazon S3). Amazon Redshift ML admite el aprendizaje supervisado, que se suele utilizar para análisis avanzados. Los casos de uso de Amazon Redshift ML incluyen la previsión de ingresos, la detección de fraudes con tarjetas de crédito y las predicciones del valor de por vida del cliente (CLV) o la pérdida de clientes.

Amazon Redshift ML facilita a los usuarios de bases de datos crear, entrenar e implementar modelos de machine learning mediante comandos SQL estándar. Amazon Redshift ML utiliza Amazon SageMaker Autopilot para entrenar y ajustar automáticamente los mejores modelos de aprendizaje automático para su clasificación o regresión en función de sus datos, sin perder el control y la visibilidad.

Todas las interacciones entre Amazon Redshift, Amazon S3 y Amazon SageMaker se resumen y automatizan. Una vez entrenado e implementado el modelo de ML, pasa a estar disponible como función definida por el usuario (UDF) en Amazon Redshift y se puede usar en consultas de SQL.

Este patrón complementa el tutorial Crear, entrenar e implementar modelos de aprendizaje automático en Amazon Redshift mediante SQL con Amazon Redshift ML del blog de AWS, y el tutorial Crear, entrenar e implementar un modelo de aprendizaje automático con SageMaker Amazon del Centro de recursos de introducción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Datos existentes en una tabla de Amazon Redshift

Habilidades

- Familiaridad con los términos y conceptos que utiliza Amazon Redshift ML, incluidos machine learning, entrenamiento y predicción.. Para obtener más información, consulte Training ML models

(Entrenar modelos de machine learning) en la documentación de Amazon Machine Learning (Amazon ML).

- Experiencia en la configuración de usuarios, la administración de acceso y la sintaxis SQL estándar de Amazon Redshift. Para obtener más información, consulte Introducción a Amazon Redshift en la documentación de Amazon Redshift.
- Conocimiento y experiencia en Amazon S3 y AWS Identity and Access Management (IAM).
- La experiencia en ejecución de comandos de la interfaz de la línea de comandos de AWS (AWS CLI) también es beneficiosa, pero no obligatoria.

Limitaciones

- El clúster de Amazon Redshift y el bucket de Amazon S3 deben estar en la misma región de AWS.
- El enfoque de este patrón solo admite modelos de aprendizaje supervisado, como la regresión, la clasificación binaria y la clasificación multiclase.

Arquitectura

En los siguientes pasos se explica cómo funciona Amazon Redshift ML SageMaker para crear, entrenar e implementar un modelo de aprendizaje automático:

1. Amazon Redshift exporta los datos de entrenamiento a un bucket de S3.
2. SageMaker El piloto automático preprocesa automáticamente los datos de entrenamiento.
3. Una vez invocada la `CREATE MODEL` declaración, Amazon Redshift ML la utiliza SageMaker para la formación.
4. SageMaker Autopilot busca y recomienda el algoritmo de aprendizaje automático y los hiperparámetros óptimos que optimizan las métricas de evaluación.
5. Amazon Redshift ML registra el modelo de ML de salida como una función SQL en el clúster de Amazon Redshift.
6. La función del modelo ML se puede utilizar en una instrucción SQL.

Pila de tecnología

- Amazon Redshift

- SageMaker
- Amazon S3

Tools (Herramientas)

- Amazon Redshift: Amazon Redshift es un servicio de almacenamiento de datos completamente administrado, de nivel empresarial y de escala de petabytes.
- Amazon Redshift ML: Amazon Redshift machine learning (Amazon Redshift ML) es un servicio robusto basado en la nube que facilita el uso de la tecnología de machine learning a los analistas y científicos de datos con cualquier nivel de habilidades.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet.
- Amazon SageMaker: SageMaker es un servicio de aprendizaje automático totalmente gestionado.
- Amazon SageMaker Autopilot: el SageMaker piloto automático es un conjunto de funciones que automatiza las tareas clave de un proceso de aprendizaje automático (AutoML).

Código

Puede crear un modelo de ML supervisado en Amazon Redshift mediante el siguiente código:

```
"CREATE MODEL customer_churn_auto_model
FROM (SELECT state,
             account_length,
             area_code,
             total_charge/account_length AS average_daily_spend,
             cust_serv_calls/account_length AS average_daily_cases,
             churn
      FROM customer_activity
      WHERE  record_date < '2020-01-01'
     )
TARGET churn
FUNCTION ml_fn_customer_churn_auto
IAM_ROLE 'arn:aws:iam::XXXXXXXXXXXX:role/Redshift-ML'
SETTINGS (
  S3_BUCKET 'your-bucket'
);")
```

> **Note**
>
> Nota: El estado de `SELECT` puede hacer referencia a las tablas normales de Amazon Redshift, a las tablas externas de Amazon Redshift Spectrum o a ambas.

Epics

Preparación de un conjunto de datos para entrenamiento y prueba

Tarea	Descripción	Habilidades requeridas
Prepare un conjunto de datos para entrenamiento y prueba.	Inicie sesión en la consola de administración de AWS y abra la SageMaker consola de Amazon. Siga las instrucciones del tutorial Build, train, and deploy a machine learning model (Crear, entrenar e implementar un modelo de machine learning) para crear un archivo.csv o Apache Parquet con una columna de etiquetas (entrenamiento supervisado) y sin encabezado. **Note** Se recomienda mezclar el conjunto de datos sin procesar y dividirlo en un conjunto de entrenamiento para entrenar el modelo (70 por ciento) y un conjunto	Científico de datos

Tarea	Descripción	Habilidades requeridas
	de prueba para evaluar el rendimien to del modelo (30 por ciento).	

Preparación y configuración de la pila de tecnología

Tarea	Descripción	Habilidades requeridas
Cree y configure un clúster de Amazon Redshift.	En la consola de Amazon Redshift, cree un clúster de acuerdo con sus requisitos. Para obtener más informaci ón, consulte Create a cluster (Crear un clúster) en la documentación de Amazon Redshift. **Important** Los nuevos clústeres de Amazon Redshift deben crearse con la pista de mantenimi ento `SQL_PREVIEW` . Para obtener más información acerca de las pistas de de previsualización, consulte Choosing cluster maintenance tracks (Seleccionar pistas de mantenimi ento del clúster) en	Administrador de base de datos, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	la documentación de Amazon Redshift.	
Cree un bucket de S3 para almacenar los datos de entrenamiento y los artefactos del modelo.	En la consola de Amazon S3, cree un bucket de S3 para los datos de entrenamiento y prueba. Para obtener más información acerca de la creación de un bucket de S3, consulte Creación de un bucket de S3 en Inicios rápidos de AWS. **Important** Asegúrese de que el clúster de Amazon Redshift y el bucket de Amazon S3 se encuentren en la misma región.	Administrador de base de datos, arquitecto de la nube
Cree y asocie una política de IAM al clúster de Amazon Redshift.	Cree una política de IAM para permitir que el clúster de Amazon Redshift SageMaker acceda a Amazon S3. Para las instrucciones y los pasos a seguir, consulte Cluster setup for using Amazon Redshift ML (Configuración del clúster para usar Amazon Redshift ML) en la documentación de Amazon Redshift.	Administrador de base de datos, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Permita que los usuarios y grupos de Amazon Redshift accedan a esquemas y tablas.	Otorgue permisos para permitir que los usuarios y grupos de Amazon Redshift accedan a tablas y esquemas internos y externos. Para ver los pasos e instrucciones, consulte Managing permissions and ownership (Administrar los permisos y la propiedad) en la documentación de Amazon Redshift.	Administrador de base de datos

Creación y entrenamiento del modelo de ML en Amazon Redshift

Tarea	Descripción	Habilidades requeridas
Cree y entrene el modelo de ML en Amazon Redshift.	Cree y entrene el modelo de ML en Amazon Redshift ML. Para obtener más información, consulte la instrucción `CREATE MODEL` en la documentación de Amazon Redshift.	Desarrollador, científico de datos

Cómo realizar inferencias y predicciones por lotes en Amazon Redshift

Tarea	Descripción	Habilidades requeridas
Realice una inferencia mediante la función del modelo de ML generado.	Para obtener más información sobre cómo realizar inferencias mediante la función del modelo de ML generado, consulte Prediction (Predicci	Científico de datos, usuario de inteligencia empresarial

Tarea	Descripción	Habilidades requeridas
	ón) en la documentación de Amazon Redshift.	

Recursos relacionados

Preparación de un conjunto de datos para entrenamiento y prueba

- Creación, formación e implementación de un modelo de aprendizaje automático con Amazon SageMaker

Preparación y configuración de la pila de tecnología

- Creación de un clúster de Amazon Redshift
- Choosing Amazon Redshift cluster maintenance tracks (Seleccionar las pistas de mantenimiento de clústeres de Amazon Redshift)
- Creating an S3 bucket (Crear un bucket de S3)
- Setting up an Amazon Redshift cluster for using Amazon Redshift ML (Configurar un clúster de Amazon Redshift para utilizar Amazon Redshift ML)
- Managing permissions and ownership in Amazon Redshift (Administrar permisos y propiedad en Amazon Redshift)

Creación y entrenamiento del modelo de ML en Amazon Redshift

- CREATE MODEL statement in Amazon Redshift (La instrucción CREATE MODEL en Amazon Redshift)

Cómo realizar inferencias y predicciones por lotes en Amazon Redshift)

- Prediction in Amazon Redshift (Predicción en Amazon Redshift)

Otros recursos

- Getting started with Amazon Redshift ML (Introducción a Amazon Redshift ML)
- Creating, training, and deploying ML models in Amazon Redshift using SQL with Amazon Redshift ML (Crear, entrenar e implementar modelos de ML en Amazon Redshift mediante SQL con Amazon Redshift ML)
- Amazon Redshift partners (Socios de Amazon Redshift.)
- AWS machine learning competency partners (Socios con competencias en machine learning de AWS)

Consulta de las tablas de Amazon DynamoDB con SQL mediante Amazon Athena

Gavin Perrie, Ajit Ambike y Brad Yates, Amazon Web Services

Resumen

Si sus datos incluyen orígenes distintos de Amazon Simple Storage Service (Amazon S3), puede utilizar consultas federadas para acceder a esos orígenes de datos relacionales, no relacionales, de objetos o personalizados. Este patrón muestra cómo configurar el acceso a consultas federadas de Amazon Athena a Amazon DynamoDB mediante un conector de origen de datos SQL.

Con este patrón, puede hacer lo siguiente:

- Consultar tablas de DynamoDB mediante SQL.
- Hacer consultas SQL federadas en Athena y combinar tablas de DynamoDB con otros orígenes de datos compatibles.

Requisitos previos y limitaciones

Requisitos previos

- Una tabla de DynamoDB.
- Un grupo de trabajo de Athena configurado para utilizar el la versión 2 del motor Athena. Para obtener instrucciones, consulte la documentación de Athena.
- Un depósito de S3 donde la `AthenaDynamoDBConnector` AWS Lambda función puede filtrar los datos. La función de Lambda debe estar en la misma región de AWS que el bucket de S3.

Si es la primera vez que accede a Athena, necesitará un bucket de S3 adicional para usarlo como ubicación de los resultados de la consulta. Para obtener instrucciones, consulte la documentación de Athena.

Limitaciones

- No se admiten operaciones de escritura como INSERT INTO.

Versiones de producto

- Athena Query Federation se publica el GitHub

Arquitectura

Arquitectura de destino

El siguiente diagrama muestra el flujo de conexión después de establecer el patrón. El usuario se conecta a Amazon Athena para realizar la consulta. Athena pasa la consulta y el destino a la función de Lambda del conector del origen de datos de DynamoDB, que recupera y devuelve los datos a Athena. Si se devuelven grandes cantidades de datos, Athena almacena los resultados temporales en el bucket de desbordamiento antes de empaquetar y devolver el conjunto de datos completo.

Tools (Herramientas)

Servicios de AWS

- Amazon Athena es un servicio interactivo de consultas que le permite analizar datos directamente en Amazon Simple Storage Service (Amazon S3) usando SQL estándar. Este patrón utiliza Amazon Athena DynamoDB Connector, una herramienta creada con el SDK de Amazon Athena Query Federation e instalada como una aplicación a través del. AWS Lambda AWS Serverless Application Repository
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Repositorio de código

El código de este patrón está disponible en el repositorio de GitHub Athena Query Federation.

Epics

Configuración del conector de origen de datos de DynamoDB y pruebas

Tarea	Descripción	Habilidades requeridas
Implemente la AthenaDynamo DBConnector aplicación.	Para AthenaDynamo DBConnecter implementarla, haga lo siguiente: 1. Inicie sesión en y elija la Consola de administración de AWS Región de AWS que está utilizando para la tabla de DynamoDB y el depósito de residuos. 2. Abra el Serverless Applicati on Repository https://c onsole.aws.amazon.com/ serverlessrepo/ en. 3. En el panel de navegación, elija Aplicaciones disponibl es. 4. Para acceder a AWS Identity and Access Management (IAM), en la barra de búsqueda, active la casilla Mostrar aplicacio nes que creen políticas de recursos o funciones de IAM personalizadas. 5. Busque AthenaDyn amoDBConnector, seleccione y asegúrese de que el autor que aparece en	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	la lista es Amazon Athena Federation. 6. En Configuración de la aplicación, ingrese los siguientes valores: • SpillBucket– Ubicación en la que la función puede transferir datos. • AthenaCatalogName– El nombre de la función Lambda que se va a crear. El nombre también se utilizará como nombre del origen de datos en Athena. 7. Seleccione la casilla de verificación para confirmar la creación de roles y políticas de IAM. 8. Elija Implementar.	

Tarea	Descripción	Habilidades requeridas
Cree un origen de datos para Athena.	Para crear un origen de datos, haga lo siguiente: 1. Abra la consola de Athena en https://console.aws.amazon.com/athena/. 2. Amplíe el panel de navegación y elija Orígenes de datos. 3. Elija Crear origen de datos. 4. Elija Amazon DynamoDB. 5. Ingrese el nombre del origen de datos. 6. Seleccione la función de Lambda que creó. 7. Revise los detalles y seleccione Crear origen de datos.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Utilice Athena para consultar la tabla de DynamoDB.	Para consultar la tabla de DynamoDB, haga lo siguiente: 1. En la consola de Athena, amplíe el panel de navegación y elija Editor de consultas. 2. En la lista desplegable Origen de datos, seleccione el origen de datos que creó. 3. Confirme que las tablas de DynamoDB aparecen en Tablas. 4. Ejecute la consulta.	Desarrollador de aplicaciones

Resolución de problemas

Problema	Solución
La consulta devuelve el error `GENERIC_INTERNAL_ERROR: The bucket is in this region: <region>`.	Asegúrese de que el bucket de desbordamiento de Athena y la función de Lambda estén creadas en la misma Región de AWS.
El origen de datos recién creado no está visible en la consola de Athena.	Los catálogos de datos de Athena son regionales. Asegúrese de que `AthenaDynamoDBConnector` se haya implementado en la región en la que está intentando utilizar Athena.
No puede poner en marcha la consulta en el origen de datos recién creado.	Compruebe que se haya definido Ubicación del resultado de la consulta.

Recursos relacionados

- Conector Amazon Athena DynamoDB
- Consultas federadas de Amazon Athena

Acceder, consultar y unirse a las tablas de Amazon DynamoDB con Athena

Moinul Al-Mamun, Amazon Web Services

Resumen

Este patrón muestra cómo configurar una conexión entre Amazon Athena y Amazon DynamoDB mediante el conector DynamoDB de Amazon Athena. El conector utiliza una función de AWS Lambda para consultar los datos en DynamoDB. No es necesario escribir ningún código para configurar la conexión. Una vez establecida la conexión, puede acceder y analizar rápidamente las tablas de DynamoDB mediante la Consulta federada de Athena para ejecutar comandos SQL desde Athena. También puede unir una o más tablas de DynamoDB entre sí o con otros orígenes de datos, como Amazon Redshift o Amazon Aurora.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa con permisos para gestionar tablas de DynamoDB, los orígenes de datos de Athena, Lambda y roles de (IAM) de AWS Identity and Access Management
- Un bucket de Amazon Simple Storage Service (Amazon S3) en el que Athena puede almacenar resultados de consultas
- Un bucket de S3 en el que el conector DynamoDB de Athena puede guardar los datos a corto plazo
- Una región de AWS compatible con la versión 2 del motor Athena
- Permisos de IAM para acceder a Athena y a los buckets de S3 necesarios
- Conector Amazon Athena DynamoDB, instalado

Limitaciones

La consulta de las tablas de DynamoDB conlleva un costo. Los tamaños de tabla que superen unos pocos gigabytes (GBs) pueden suponer un coste elevado. Le recomendamos que considere el costo antes de realizar cualquier operación de escaneo de una tabla completa. Para obtener más información, consulte los precios de Amazon DynamoDB. Para reducir los costos y lograr un alto rendimiento, le recomendamos que utilice siempre LIMIT en la consulta (por ejemplo, `SELECT * FROM table1 LIMIT 10`). Además, antes de realizar una consulta JOIN (unirse a) o GROUP BY

(agrupar por) en un entorno de producción, tenga en cuenta el tamaño de sus tablas. Si sus tablas son demasiado grandes, considere opciones alternativas, como migrar la tabla a Amazon S3.

Arquitectura

En el siguiente diagrama se muestra la forma en que un usuario puede ejecutar una consulta SQL en una tabla de DynamoDB desde Athena.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Para consultar una tabla de DynamoDB, el usuario ejecuta una consulta SQL desde Athena.
2. Athena inicia una función de Lambda.
3. La función de Lambda consulta los datos solicitados en la tabla de DynamoDB.
4. DynamoDB regresa los datos solicitados a la función de Lambda. A continuación, la función transfiere los resultados de la consulta al usuario a través de Athena.
5. La función de Lambda almacena los datos en el bucket de S3.

Pila de tecnología

- Amazon Athena
- Amazon DynamoDB
- Amazon S3
- AWS Lambda

Tools (Herramientas)

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.
- El Conector de DynamoDB de Amazon Athena es una herramienta de AWS que permite a Athena conectarse con DynamoDB y acceder a sus tablas mediante consultas SQL.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la

capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

Epics

Crear tablas de DynamoDB de muestra

Tarea	Descripción	Habilidades requeridas
Cree la primera tabla de muestra.	1. Inicie sesión en la consola de administración de AWS y abra la consola de DynamoDB. 2. Seleccione Create table (Creación de tabla). 3. En Nombre de tabla, introduzca dydbtable1. 4. En Clave de partición, escriba. PK1 5. Para Clave de clasificación, ingrese SK1. 6. En la sección Configuración de la tabla, elija Personali zar configuración. 7. En la sección Clase de tabla, seleccione DynamoDB Standard. 8. En la sección de Configura ción de capacidad de lectura/escritura, en el Modo capacidad, seleccion e Bajo demanda. 9. En la sección Cifrado en reposo, seleccione	Desarrollador

Tarea	Descripción	Habilidades requeridas
	Propiedad de Amazon DynamoDB. 10. Seleccione Create table (Creación de tabla).	

Tarea	Descripción	Habilidades requeridas

Inserte datos de muestra en la primera tabla.	1. Abra la consola de DynamoDB.
	2. En el panel de navegación, seleccione Tabla y, a continuación, seleccione su tabla en la columna Nombre.
	3. Elija Acciones y, a continuación, seleccione Crear elemento.
	4. Seleccione Vista JSON.
	5. En la barra de título del editor de Atributos, desactive Ver DynamoDB JSON.
	6. En el editor de Atributos, introduzca los siguientes datos de muestra uno por uno:
	
	`{ "PK1": "1234", "SK1": "info", "Salary": "5000" }`
	
	`{ "PK1": "1235", "SK1": "info", "Salary": "5200" }`
		Desarrollador

Tarea	Descripción	Habilidades requeridas
Cree la segunda tabla de muestra.	1. Abra la consola de DynamoDB. 2. Seleccione Create table (Creación de tabla). 3. En Nombre de tabla, introduzca dydbtable2. 4. En Partition key (Clave de partición), ingrese PK2. 5. Para Clave de clasificación, ingrese SK2. 6. En la sección Configuración de la tabla, elija Personalizar configuración. 7. En la sección Clase de tabla, seleccione DynamoDB Standard. 8. En la sección de Configuración de capacidad de lectura/escritura, en el Modo capacidad, seleccione Bajo demanda. 9. En la sección Cifrado en reposo, seleccione Propiedad de Amazon DynamoDB. 10. Seleccione Create table (Creación de tabla).	Desarrollador

Tarea	Descripción	Habilidades requeridas

Inserte datos de muestra en la segunda tabla.	1. Abra la consola de DynamoDB.
	2. En el panel de navegación, seleccione Tabla y, a continuación, seleccione su tabla en la columna Nombre.
	3. Elija Acciones y, a continuación, seleccione Crear elemento.
	4. En la barra de título del editor de Atributos, desactive Ver DynamoDB JSON.
	5. En el editor de Atributos, introduzca los siguientes datos de muestra uno por uno:
	
	`{ "PK2": "1234", "SK2": "bonus", "Bonus": "500" }`
	
	`{ "PK2": "1235", "SK2": "bonus", "Bonus": "1000" }`
		Desarrollador

Crear un origen de datos en Athena para DynamoDB

Tarea	Descripción	Habilidades requeridas
Configure el conector del origen de datos.	Cree un origen de datos para DynamoDB y, a continuación, cree una función de Lambda para conectarse a ese origen de datos. 1. Inicie sesión en la consola de administración de AWS y abra la consola de Athena. 2. En el panel de navegación, seleccione Origen de datos y, a continuación, seleccione Crear origen de datos. 3. Seleccione el origen de datos de Amazon DynamoDB y, a continuación, seleccione Siguiente. 4. En la sección de Detalles del origen de datos, en Nombre del origen de datos, introduzca TestDynamoDB. 5. En la sección Detalles de conexión, seleccione una función de Lambda que ya esté implementada o seleccione Crear función de Lambda si no tiene una función de Lambda para usar en este patrón. Nota: Para obtener más informaci	Desarrollador

Tarea	Descripción	Habilidades requeridas
	ón acerca de cómo crear una función de Lambda, consulte Introducción a AWS Lambda en la Guía para desarrolladores de Lambda. 6. (Opcional) Si elige Crear función Lambda, debe configurar la CloudForm ation plantilla de AWS que incluye la aplicación Java antes de implement ar esa pila. La plantilla incluye ApplicationName SpillBucket AthenaCat alogName, y otros ajustes de la aplicación. Nota: Tras implementar esta aplicación basada en Java, la pila crea una función de Lambda que permite a Athena comunicarse con DynamoDB. Esto hace que sus tablas sean accesible s mediante comandos de SQL. 7. Implementación de la función de Lambda. 8. Elija Siguiente.	

Tarea	Descripción	Habilidades requeridas
Compruebe que la función de Lambda pueda acceder al bucket para derrames de S3.	1. Abra la consola de Lambda. 2. En el panel de navegación, seleccione Funciones y, a continuación, elija la función que creó anteriormente. 3. Elija la pestaña Configura ción. 4. En el panel izquierdo, seleccione Variables de entorno y, a continuación, confirme que el valor de la clave es `spill_bucket` . 5. En el panel izquierdo, seleccione Permisos y, a continuación, en la sección Función de ejecución, seleccione el rol de IAM asociado. Nota: Se le redirige al rol de IAM asociado a su función de Lambda en la consola de IAM. 6. Confirme que tiene permiso de escritura en el bucket `spill_bucket` . Si se producen errores, consulte la sección de Información adicional de este patrón como guía.	Desarrollador

Acceso a las tablas de DynamoDB desde Athena

Tarea	Descripción	Habilidades requeridas
Consultar las tablas de DynamoDB.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Athena. 2. En el panel de navegación, seleccione Origen de datos y, a continuación, seleccione Crear origen de datos. 3. En el panel de navegación, seleccione Query Editor (Editor de consultas). 4. En la pestaña Editor, en la sección Datos, en Origen de datos, seleccione su origen de datos como Origen de datos. 5. En Database (Base de datos), elija la base de datos. 6. Para la consulta 1, introduzca la siguiente consulta: `SELECT * FROM dydbtable1 t1;` 7. Seleccione Ejecutar y, a continuación, verifique el resultado de la tabla. 8. Para la consulta 2, introduzca la siguiente consulta: `SELECT * FROM dydbtable2 t2;`	Desarrollador

Tarea	Descripción	Habilidades requeridas
	9. Seleccione Ejecutar y, a continuación, verifique el resultado de la tabla.	
Unir las dos tablas de DynamoDB.	DynamoDB es un almacén de datos NoSQL y no admite la operación de unión de SQL. En consecuencia, debe realizar una operación de unión en dos tablas de DynamoDB: 1. Elija el icono de signo más para crear otra consulta. 2. Para la consulta 3, introduzca la siguiente consulta: `SELECT pk1, salary, bonus FROM dydbtable1 t1 JOIN dydbtable2 t2 ON t1.pk1 = t2.pk2;`	Desarrollador

Recursos relacionados

- Conector para DynamoDB de Amazon Athena (Laboratorios de AWS)
- Consulte cualquier origen de datos con la nueva consulta federada de Amazon Athena (blog sobre macrodatos de AWS)
- Referencia de la versión del motor Athena (Guía del usuario de Athena)
- Simplifique la extracción y el análisis de datos de Amazon DynamoDB con AWS Glue y Amazon Athena (blog sobre bases de datos de AWS)

Información adicional

Si ejecuta una consulta en Athena con `spill_bucket` en formato `{bucket_name}/folder_name/`, puede recibir el siguiente mensaje de error:

```
"GENERIC_USER_ERROR: Encountered an exception[java.lang.RuntimeException] from your
 LambdaFunction[arn:aws:lambda:us-east-1:xxxxxx:function:testdynamodb] executed in
 context[retrieving meta-data] with message[You do NOT own the spill bucket with the
 name: s3://amzn-s3-demo-bucket/athena_dynamodb_spill_data/]
This query ran against the "default" database, unless qualified by the query. Please
 post the error message on our forum  or contact customer support with Query Id:
 [query-id]"
```

Para resolver este error, actualice la variable de entorno de la función de Lambda de `spill_bucket` a `{bucket_name_only}` y, a continuación, actualice la siguiente política de IAM de Lambda para el acceso de escritura al bucket:

```
{
            "Action": [
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:GetObjectVersion",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::spill_bucket",
                "arn:aws:s3:::spill_bucket/*"
            ],
            "Effect": "Allow"
        }
```

Como alternativa, puede quitar el conector de origen de datos de Athena que creó anteriormente y volver a crearlo utilizando solo `{bucket_name}` para `spill_bucket`.

Configure la clasificación por idioma para los resultados de las consultas de Amazon Redshift mediante una UDF escalar de Python

Ethan Stark, Amazon Web Services

Resumen

Este patrón proporciona los pasos y un código de ejemplo para usar una UDF (función definida por el usuario) de Python escalar para configurar una clasificación lingüística que no distinga entre mayúsculas y minúsculas para los resultados de las consultas de Amazon Redshift. Es necesario utilizar una UDF de Python escalar porque Amazon Redshift devuelve los resultados en función del orden binario de UTF-8 y no admite la clasificación por idiomas específicos. Una UDF de Python es un código de procesamiento que no es de SQL que se basa en un programa de Python y se ejecuta en un almacén de datos. Puede ejecutar código UDF de Python con una instrucción SQL en una sola consulta. Para obtener más información, consulte la entrada del blog Introducción a Python UDFs en Amazon Redshift AWS Big Data.

Los datos de muestra de este patrón se basan en el alfabeto turco con fines de demostración. La UDF escalar de Python de este patrón está diseñada para que los resultados de las consultas predeterminados de Amazon Redshift se ajusten al orden lingüístico de los caracteres del idioma turco. Para obtener más información, consulte Ejemplo de lengua turca en la sección Información adicional de este patrón. Puede modificar la UDF escalar de Python en este patrón para otros lenguajes.

Requisitos previos y limitaciones

Requisitos previos

- Clúster de Amazon Redshift con base de datos, esquema y tablas
- Usuario de Amazon Redshift con permisos `CREATE TABLE` y `CREATE FUNCTION`.
- Python 2.7 o posterior

Limitaciones

La clasificación lingüística utilizada por las consultas en este patrón no distingue entre mayúsculas y minúsculas.

Tools (Herramientas)

Servicios de AWS

- Amazon Redshift es un servicio de almacén de datos administrado que opera a escala de petabytes en la Nube de AWS. Amazon Redshift está integrado en el lago de datos, lo que permite usar los datos para adquirir nueva información para su empresa y sus clientes.

Otras herramientas

- Las funciones definidas por el usuario de Python (UDFs) son funciones que puede escribir en Python y, a continuación, invocar sentencias SQL.

Epics

Desarrolle código para ordenar los resultados de las consultas en orden lingüístico

Tarea	Descripción	Habilidades requeridas

Cree una tabla para los datos de su muestra.	Para crear una tabla en Amazon Redshift e insertar los datos de muestra en la tabla, utilice las siguientes instrucciones SQL:
	`CREATE TABLE my_table (first_name varchar(30));`
	`INSERT INTO my_table (first_name) VALUES ('ali'), ('Ali'), ('ırmak'), ('IRMAK'), ('irem'), ('İREM'), ('oğuz'),`
		Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	('OĞUZ'), ('ömer'), ('ÖMER'), ('sedat'), ('SEDAT'), ('şule'), **Note** Los primeros nombres de los datos de muestra incluyen caracteres especiales del alfabeto turco. Para obtener más información sobre las consideraciones relativas al idioma turco en este ejemplo, consulte Ejemplo de lengua turca en la sección Información adicional de este patrón.	

Tarea	Descripción	Habilidades requeridas

Compruebe la clasificación predeterminada de los datos de la muestra.	Para ver la clasificación predeterminada de los datos de muestra en Amazon Redshift, ejecute la siguiente consulta:
	`SELECT first_name FROM my_table ORDER BY first_name;`
	La consulta devuelve la lista de nombres de la tabla que creó anteriormente:
	`first_name`
	`---------------`
	`Ali`
	`IRMAK`
	`OĞUZ`
	`SEDAT`
	`ali`
	`irem`
	`oğuz`
	`sedat`
	`ÖMER`
	`ömer`
	`İREM`
	`ırmak`
	`ŞULE`
	`şule`
	Los resultados de la consulta no están en el orden correcto porque el orden binario predeterminado en UTF-8 no se adapta al orden lingüístico
		Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	de los caracteres especiales turcos.	

Tarea	Descripción	Habilidades requeridas
Creación de una UDF de Python escalar.	Para crear una UDF de Python escalar, utilice el siguiente código SQL: `CREATE OR REPLACE FUNCTION collate_sort (value varchar) RETURNS varchar IMMUTABLE AS $$ def sort_str(val): import string dictionary = { 'I': 'ı', 'ı': 'h~', 'İ': 'i', 'Ş': 's~', 'ş': 's~', 'Ğ': 'g~', 'ğ': 'g~', 'Ü': 'u~', 'ü': 'u~', 'Ö': 'o~', 'ö': 'o~', 'Ç': 'c~', 'ç': 'c~' } for key, value in dictionary.items(): val = val.replace(key, value) return val.lower()`	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas

	`    return sort_str(value)`
	
	`$$ LANGUAGE plpythonu;`	

Consulta del ejemplo de datos.	Para consultar del ejemplo de datos mediante la UDF de Python, ejecute la siguiente consulta SQL:
	
	`SELECT first_name FROM my_table ORDER BY collate_sort(first_name);`
	
	La consulta ahora devuelve los datos de la muestra en orden lingüístico turco:
	
	`first_name`
	`---------------`
	`ali`
	`Ali`
	`ırmak`
	`IRMAK`
	`irem`
	`İREM`
	`oğuz`
	`OĞUZ`
	`ömer`
	`Ömer`
	`sedat`
	`SEDAT`
	`şule`
	`ŞULE`
		Ingeniero de datos

Recursos relacionados

- Cláusula ORDER BY (documentación de Amazon Redshift)
- Creación de una UDF de Python escalar (documentación de Amazon Redshift)

Información adicional

Ejemplo de idioma turco

Amazon Redshift devuelve los resultados de las consultas en función de la ordenación binaria de UTF-8, no de una ordenación específica del idioma. Esto significa que si consulta una tabla de Amazon Redshift que contenga caracteres turcos, los resultados de la consulta no se ordenarán según el orden lingüístico del idioma turco. El idioma turco contiene seis caracteres especiales (ç, ı, ğ, ö, ş y ü) que no aparecen en el alfabeto latino. Estos caracteres especiales se colocan al final de un conjunto de resultados ordenados según el orden binario UTF-8, como se muestra en la siguiente tabla.

Orden binario en UTF-8	Ordenamiento lingüístico turco
a	a
b	b
c	c
d	ç (*)
e	d
f	e
g	f
h	g
i	ğ (*)
j	h
k	ı (*)

l	i
m	j
n	k
o	l
p	m
r	n
s	o
t	ö (*)
u	p
v	r
y	s
z	ş (*)
ç (*)	t
ğ (*)	u
ı (*)	ü (*)
ö (*)	v
ş (*)	y
ü (*)	z

> **Note**
>
> El asterisco (*) indica un carácter especial en el idioma turco.

Como se muestra en la tabla anterior, el carácter especial ç se encuentra entre la c y la d en el orden lingüístico turco, pero aparece después de la z en el orden binario UTF-8. La UDF de Python escalar de este patrón utiliza el siguiente diccionario de reemplazo de caracteres para reemplazar los caracteres especiales turcos por los correspondientes caracteres equivalentes en latín.

Carácter especial turco	Carácter equivalente en latín
ç	c~
ı	h~
ğ	g~
ö	o~
ş	s~
ü	u~

> **Note**
>
> Se agrega un carácter de tilde (~) al final de los caracteres latinos que sustituyen a sus correspondientes caracteres especiales turcos.

Cómo modificar una función UDF de Python escalar

Para modificar la función UDF de Python escalar a partir de este patrón para que la función acepte un parámetro de localización y admita un diccionario de transacciones múltiples, utilice el siguiente código SQL:

```
CREATE OR REPLACE FUNCTION collate_sort (value varchar, locale varchar)
RETURNS varchar
IMMUTABLE
AS
$$
    def sort_str(val):
       import string
       # Turkish Dictionary
       if locale == 'tr-TR':
```

```
            dictionary = {
               'I': 'ı',
               'ı': 'h~',
               'İ': 'i',
               'Ş': 's~',
               'ş': 's~',
               'Ğ': 'g~',
               'ğ': 'g~',
               'Ü': 'u~',
               'ü': 'u~',
               'Ö': 'o~',
               'ö': 'o~',
               'Ç': 'c~',
               'ç': 'c~'
        }
        # German Dictionary
        if locale == 'de-DE':
            dictionary = {
               ....
               ....
        }

        for key, value in dictionary.items():
            val = val.replace(key, value)

        return val.lower()

    return sort_str(value)

$$ LANGUAGE plpythonu;
```

En el siguiente ejemplo de código se muestra cómo se consulta del UDF de Python modificado:

```
SELECT first_name FROM my_table ORDER BY collate_order(first_name, 'tr-TR');
```

Suscripción de una función de Lambda a las notificaciones de eventos de buckets de S3 en diferentes regiones de AWS

Suresh Konathala, Amazon Web Services

Andrew Preston y Arindom Sarkar, ninguno

Resumen

Notificaciones de eventos de Amazon Simple Storage Service (Amazon S3) publica notificaciones de determinados eventos en su bucket de S3 (por ejemplo, eventos creados por objetos, eventos de eliminación de objetos o eventos de restauración de objetos). Puede usar una función de AWS Lambda para procesar estas notificaciones de acuerdo con los requisitos de su aplicación. Sin embargo, la función de Lambda no puede suscribirse directamente a las notificaciones de los buckets de S3 alojados en distintas regiones de AWS.

El enfoque de este patrón implementa un escenario de distribución ramificada para procesar las notificaciones de Amazon S3 procedentes de buckets de S3 entre regiones mediante un tema del Amazon Simple Notification Service (Amazon SNS) para cada región. Estos temas de SNS regional envían las notificaciones de eventos de Amazon S3 a una cola de Amazon Simple Queue Service (Amazon SQS) en una región central que también contiene la función de Lambda. La función de Lambda se suscribe a esta cola de SQS y procesa las notificaciones de eventos de acuerdo con los requisitos de su organización.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Buckets de S3 existentes en varias regiones, incluida una región central para alojar la cola de Amazon SQS y la función de Lambda.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada. Para obtener más información, consulte Instalar, actualizar y desinstalar la CLI de AWS en la documentación de la CLI de AWS.
- Familiaridad con el escenario de distribución ramificada en Amazon SNS. Para obtener más información al respecto, consulte Escenarios comunes de Amazon SNS en la documentación de Amazon SNS.

Arquitectura

El siguiente diagrama muestra la arquitectura para el enfoque de este patrón.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Amazon S3 envía notificaciones de eventos sobre buckets de S3 (por ejemplo, objetos creados, objetos retirados o objetos restaurados) a un tema de SNS de la misma región.
2. El tema de SNS publica el evento en una cola de SQS en la región central.
3. La cola SQS está configurada como el origen de eventos de la función de Lambda y almacena en búfer los mensajes de eventos de la función de Lambda.
4. La función de Lambda sondea la cola de SQS en busca de mensajes y procesa las notificaciones de eventos de Amazon S3 según los requisitos de la aplicación.

Pila de tecnología

- Lambda
- Amazon SNS
- Amazon SQS
- Amazon S3

Tools (Herramientas)

- AWS CLI: la interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto para interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos. Con una configuración mínima, puede ejecutar comandos de la CLI de AWS que implementan una funcionalidad equivalente a la proporcionada por la consola de administración de AWS basada en navegador desde un símbolo del sistema.
- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Puede administrar y aprovisionar pilas en varias cuentas y regiones de AWS.

- AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.
- Amazon SQS: Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos. Amazon SQS admite tanto las colas estándar como las colas FIFO.

Epics

Crear la cola SQS y la función de Lambda en su región central

Tarea	Descripción	Habilidades requeridas
Cree una cola de SQS con un desencadenador Lambda.	Inicie sesión en la consola de administración de AWS y siga las instrucciones del tutorial Uso de Lambda con Amazon SQS de la documentación de AWS Lambda para crear los siguientes recursos en su región central: • Un rol de ejecución de Lambda • Una función de Lambda para procesar los eventos de Amazon S3 • Una cola de SQS	AWS DevOps, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	Note Asegúrese de configurar la cola de SQS como origen de eventos de la función de Lambda.	

Cree un tema de SNS y configure las notificaciones de eventos para los buckets de S3 de cada región requerida

Tarea	Descripción	Habilidades requeridas
Cree un tema de SNS para recibir notificaciones de eventos de Amazon S3.	Cree un tema de SNS en una región de la que desee recibir notificaciones de eventos de Amazon S3. Para obtener más información al respecto, consulte Creación de un tema SNS en la documentación de Amazon SNS. **Important** Asegúrese de registrar el nombre de recurso de Amazon (ARN) de su tema de SNS.	AWS DevOps, arquitecto de nube
Suscriba el tema SNS a la cola SQS central.	Suscriba su tema de SNS a la cola de SQS alojada en su región central. Para obtener más información al respecto, consulte Suscripción a un	AWS DevOps, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	tema SNS en la documentación de Amazon SNS.	

Tarea	Descripción	Habilidades requeridas
Actualice la política de acceso del tema SNS.	1. Abra la consola de Amazon SNS, seleccione Temas y, a continuación, elija el tema SNS que creó anteriorm ente. 2. Seleccione Editar y, a continuación, amplíe la sección Política de acceso (opcional). 3. Adjunte la siguiente política de acceso a su tema de SNS para conceder permisos de `sns:publi sh` a Amazon S3 y, a continuación, seleccione Guardar: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "0", "Effect": "Allow", "Principal": { "Service": "s3.amazonaws.com" }, "Action": "sns:Publish", "Resource": "arn:aws:sns:us-west-2::s3Events-SNSTopic-us-west-2" } ]`	AWS DevOps, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	`}`	
Configure las notificaciones para cada bucket de S3 de la región.	Configure las notificaciones de eventos para cada bucket de S3 de la región. Para obtener más información al respecto, consulte Activación y configuración de las notificaciones de eventos mediante la consola de Amazon S3 en la documentación de Amazon S3. **Note** En la sección Destino, elija el tema de SNS y especifique el ARN del tema de SNS que creó anteriormente.	AWS DevOps, arquitecto de nube
Repita esta épica en todas las regiones requeridas.	**Important** Repita las tareas de esta epic para cada región de la que quiere recibir notificaciones de eventos de Amazon S3, lo que incluye la región central.	AWS DevOps, arquitecto de nube

Recursos relacionados

- Configuración de una política de acceso (documentación de Amazon SQS)
- Configuración de una cola de SQS como fuente de eventos (documentación de AWS Lambda)
- Configuración de una cola de SQS para iniciar una función de Lambda (documentación de Amazon SQS)
- AWS::Lambda::Function recurso (CloudFormation documentación de AWS)

Tres tipos de trabajos de AWS Glue ETL para convertir datos a Apache Parquet

Adnan Alvee, Nith Govindasivan y Karthikeyan Ramachandran, Amazon Web Services

Resumen

En la nube de Amazon Web Services (AWS), AWS Glue es un servicio de extracción, transformación y carga (ETL) totalmente administrado. Con AWS Glue puede categorizar datos, limpiarlos, enriquecerlos y trasladarlos de manera fiable entre distintos almacenes y flujos de datos de manera rentable.

Este patrón proporciona diferentes tipos de trabajos en AWS Glue y utiliza tres scripts diferentes para demostrar la creación de trabajos de ETL.

Puede usar AWS Glue para escribir trabajos de ETL en un entorno de intérprete de comandos de Python. También puede crear trabajos ETL por lotes o en streaming mediante Python (PySpark) o Scala en un entorno Apache Spark gestionado. Para empezar a crear trabajos de ETL, este patrón se centra en los trabajos de ETL por lotes utilizando Python shell y Scala. PySpark Los trabajos de intérprete de comandos de Python están pensados para cargas de trabajo que requieren menos potencia de cálculo. El entorno gestionado de Apache Spark está diseñado para cargas de trabajo que requieren una gran potencia de cálculo.

Apache Parquet está diseñado para admitir esquemas de compresión y codificación eficientes. Puede acelerar sus cargas de trabajo de análisis porque almacena los datos en forma de columnas. La conversión de datos a Parquet puede ahorrarle espacio de almacenamiento, costos y tiempo a largo plazo. Para obtener más información sobre Parquet, consulte la entrada del blog Apache Parquet: cómo ser un héroe con el formato de datos en columnas de código abierto.

Requisitos previos y limitaciones

Requisitos previos

- Rol de AWS Identity and Access Management (IAM) (si no tiene un rol, consulte la sección de Información adicional).

Arquitectura

Pila de tecnología de destino

- AWS Glue
- Amazon Simple Storage Service (Amazon S3)
- Apache Parquet

Automatizar y escalar

- Los flujos de trabajo de AWS Glue admiten la automatización total de una canalización de ETL.
- Puede cambiar el número de unidades de procesamiento de datos (DPUs), o los tipos de trabajadores, para escalar horizontal y verticalmente.

Tools (Herramientas)

Servicios de AWS

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Glue es un servicio de ETL totalmente gestionado que le ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.

Otras herramientas

- Apache Parquet es un formato de archivo de datos de código abierto orientado por columnas diseñado para el almacenamiento y la recuperación.

Configuración

Utilice los siguientes ajustes para configurar la potencia de procesamiento de AWS Glue ETL. Para reducir los costos, utilice la configuración mínima cuando ejecute la carga de trabajo que se proporciona en este patrón.

- Intérprete de comandos de Python: puede usar 1 DPU para utilizar 16 GB de memoria o 0,0625 DPU para utilizar 1 GB de memoria. Este patrón usa 0,0625 DPU, que es el valor predeterminado en la consola de AWS Glue.
- Python o Scala para Spark: si elige los tipos de trabajo relacionados con Spark en la consola, AWS Glue utiliza de forma predeterminada 10 trabajadores y el tipo de trabajador G.1X. Este patrón

utiliza dos trabajadores, que es el número mínimo permitido, y el tipo de trabajador estándar es suficiente y rentable.

En la siguiente tabla se muestran los distintos tipos de trabajadores de AWS Glue para el entorno Apache Spark. Como un trabajo de intérprete de comandos de Python no utiliza el entorno Apache Spark para ejecutar Python, no se incluye en la tabla.

	Standard	G.1 X	G.2X
vCPU	4	4	8
Memoria	16 GB	16 GB	32 GB
Espacio en disco	50 GB	64 GB	128 GB
Ejecutor por trabajo	2.	1	1

Código

Para ver el código que se utiliza en este patrón, incluida la configuración del rol de IAM y los parámetros de IAM, consulte la sección de Información adicional.

Epics

Carga de datos

Tarea	Descripción	Habilidades requeridas
Cargue los datos en un bucket de S3 nuevo o en un bucket de S3 ya existente.	Cree utilice un bucket de S3 existente en su cuenta. Cargue el archivo sample_data.csv de la sección de Adjuntos y anote el bucket de S3 y la ubicación del prefijo.	AWS general

Cree y ejecute el trabajo de AWS Glue

Tarea	Descripción	Habilidades requeridas
Cree el trabajo de AWS Glue	En la sección ETL de la consola de AWS Glue, añada un trabajo de AWS Glue. Seleccione el tipo de trabajo adecuado, la versión de AWS Glue y el DPU/Worker tipo y número de trabajadores correspondientes. Para más información, consulte la sección Configuración.	Desarrollador, nube o datos
Cambie las ubicaciones de entrada y salida.	Copie el código correspondiente a su trabajo de AWS Glue y cambie la ubicación de entrada y salida que indicó en la descripción de la épica Cargar los datos.	Desarrollador, nube o datos
Configure los parámetros.	Puede utilizar los fragmentos que se proporcionan en la sección de Additional information (Información adicional) para establecer los parámetros de su trabajo de ETL. AWS Glue utiliza cuatro nombres de argumentos internamente: • `--conf` • `--debug` • `--mode` • `--JOB_NAME`	Desarrollador, nube o datos

Tarea	Descripción	Habilidades requeridas
	El parámetro `--JOB_NAME` debe introducirse de forma explícita en la consola de AWS Glue. Elija Trabajos, Edit Job (Editar trabajo), Security configuration, script libraries, and job parameter s (optional) (Configuración de seguridad, bibliotecas de scripts y parámetros de trabajo (opcional)). Introduzc a `--JOB_NAME` como clave y proporcione un valor. También puede utilizar la Interfaz de la línea de comandos de AWS (AWS CLI) o la API de AWS Glue para configurar este parámetro. Spark usa el parámetro `--JOB_NAME` y no es necesario en un trabajo de entorno de intérprete de comandos de Python. Debe añadir `--` antes del nombre de cada parámetro ; de lo contrario, el código no funcionará. Por ejemplo, en el caso de los fragmento s de código, los parámetros de ubicación deben invocarse mediante `--input_loc` y `--output_loc` .	

Tarea	Descripción	Habilidades requeridas
Ejecute el trabajo de ETL.	Ejecute su trabajo y compruebe el resultado. Observe cuánto espacio se ha reducido con respecto al archivo original.	Desarrollador, nube o datos

Recursos relacionados

Referencias

- Apache Spark
- AWS Glue: cómo funciona
- Precios de AWS Glue

Tutoriales y videos

- ¿Qué es AWS Glue?

Información adicional

Rol de IAM

Al crear los trabajos de AWS Glue, puede usar un rol de IAM existente que tenga los permisos que se muestran en el siguiente fragmento de código o un rol nuevo.

Para crear un nuevo rol, utilice el siguiente código YAML.

```
# (c) 2022 Amazon Web Services, Inc. or its affiliates. All Rights Reserved. This AWS
 Content is provided subject to the terms of the AWS Customer
# Agreement available at https://aws.amazon.com/agreement/ or other written agreement
 between Customer and Amazon Web Services, Inc.

AWSTemplateFormatVersion: "2010-09-09"

Description: This template will setup IAM role for AWS Glue service.
```

```
Resources:
  rGlueRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              Service:
                - "glue.amazonaws.com"
            Action:
              - "sts:AssumeRole"
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole
      Policies:
        - PolicyName: !Sub "${AWS::StackName}-s3-limited-read-write-inline-policy"
          PolicyDocument:
            Version: "2012-10-17"
            Statement:
              - Effect: Allow
                Action:
                  - "s3:PutObject"
                  - "s3:GetObject"
                Resource: "arn:aws:s3:::*/*"
      Tags:
        - Key  : "Name"
          Value : !Sub "${AWS::StackName}"

Outputs:
  oGlueRoleName:
    Description: AWS Glue IAM role
    Value:
      Ref: rGlueRole
    Export:
      Name: !Join [ ":", [ !Ref "AWS::StackName", rGlueRole ] ]
```

AWS Glue (intérprete de comandos de Python)

El código Python usa los Pandas y PyArrow las bibliotecas para convertir los datos a Parquet. La biblioteca Pandas ya está disponible. La PyArrow biblioteca se descarga al ejecutar el patrón, ya que se ejecuta una sola vez. Puede usar archivos de rueda PyArrow para convertirlos en una biblioteca

y proporcionar el archivo como un paquete de biblioteca. Para obtener más información, consulte Proporcionar su propia biblioteca de Python

Parámetros del intérprete de comandos de Python de AWS Glue

```
from awsglue.utils import getResolvedOptions

args = getResolvedOptions(sys.argv, ["input_loc", "output_loc"])
```

Código del intérprete de comandos para Python de AWS Glue

```
from io import BytesIO
import pandas as pd
import boto3
import os
import io
import site
from importlib import reload
from setuptools.command import easy_install
install_path = os.environ['GLUE_INSTALLATION']
easy_install.main( ["--install-dir", install_path, "pyarrow"] )
reload(site)
import pyarrow


input_loc = "s3://bucket-name/prefix/sample_data.csv"
output_loc = "s3://bucket-name/prefix/"


input_bucket = input_loc.split('/', 1)[0]
object_key = input_loc.split('/', 1)[1]


output_loc_bucket = output_loc.split('/', 1)[0]
output_loc_prefix = output_loc.split('/', 1)[1]


s3 = boto3.client('s3')
obj = s3.get_object(Bucket=input_bucket, Key=object_key)
df = pd.read_csv(io.BytesIO(obj['Body'].read()))


parquet_buffer = BytesIO()
```

```
s3_resource = boto3.resource('s3')
df.to_parquet(parquet_buffer, index=False)
s3_resource.Object(output_loc_bucket, output_loc_prefix +  'data' +
 '.parquet').put(Body=parquet_buffer.getvalue())
```

Trabajo de AWS Glue Spark con Python

Para usar un tipo de trabajo de AWS Glue Spark con Python, elija Spark como tipo de trabajo. Elija Spark 3.1, Python 3 con un tiempo de inicio de trabajo mejorado (Glue versión 3.0) como versión AWS Glue.

Parámetros de Python de AWS Glue

```
from awsglue.utils import getResolvedOptions

args = getResolvedOptions(sys.argv, ["JOB_NAME", "input_loc", "output_loc"])
```

Trabajo de AWS Glue Spark con el código de Python

```
import sys
from pyspark.context import SparkContext
from awsglue.context import GlueContext
from awsglue.transforms import *
from awsglue.dynamicframe import DynamicFrame
from awsglue.utils import getResolvedOptions
from awsglue.job import Job


sc = SparkContext()
glueContext = GlueContext(sc)
spark = glueContext.spark_session
job = Job(glueContext)

input_loc = "s3://bucket-name/prefix/sample_data.csv"
output_loc = "s3://bucket-name/prefix/"

inputDyf = glueContext.create_dynamic_frame_from_options(\
    connection_type = "s3", \
    connection_options = {
        "paths": [input_loc]}, \
    format = "csv",
    format_options={
```

```
        "withHeader": True,
        "separator": ","
    })


outputDF = glueContext.write_dynamic_frame.from_options(\
    frame = inputDyf, \
    connection_type = "s3", \
    connection_options = {"path": output_loc \
        }, format = "parquet")
```

En el caso de un gran número de archivos comprimidos de gran tamaño (por ejemplo, 1000 archivos de aproximadamente 3 MB cada uno), utilice el parámetro `compressionType` junto con el parámetro `recurse` para leer todos los archivos disponibles en el prefijo, tal y como se muestra en el código siguiente.

```
input_loc = "bucket-name/prefix/"
output_loc = "bucket-name/prefix/"

inputDyf = glueContext.create_dynamic_frame_from_options(
                    connection_type = "s3",
                    connection_options = {"paths": [input_loc],
                                          "compressionType":"gzip","recurse" :"True",
                                          },
                    format = "csv",
                    format_options={"withHeader": True,"separator": ","}
                    )
```

Para un gran número de archivos pequeños comprimidos (por ejemplo, 1000 archivos de aproximadamente 133 KB cada uno), utilice el parámetro`groupFiles` junto con los parámetros `compressionType` y `recurse`. El parámetro `groupFiles` agrupa los archivos pequeños en varios archivos grandes y el parámetro `groupSize` controla la agrupación según el tamaño especificado en bytes (por ejemplo, 1 MB). El siguiente fragmento de código proporciona un ejemplo del uso de estos parámetros en el código.

```
input_loc = "bucket-name/prefix/"
output_loc = "bucket-name/prefix/"

inputDyf = glueContext.create_dynamic_frame_from_options(
                    connection_type = "s3",
                    connection_options = {"paths": [input_loc],
```

```
                                          "compressionType":"gzip","recurse" :"True",
                                           "groupFiles" :"inPartition",
 "groupSize" :"1048576",
                                          },
                    format = "csv",
                    format_options={"withHeader": True,"separator": ","}
                    )
```

Sin ningún cambio en los nodos de trabajo, esta configuración permite que el trabajo de AWS Glue lea varios archivos (grandes o pequeños, con o sin compresión) y los escriba en el destino en formato Parquet.

Trabajo de AWS Glue Spark con Scala

Para usar un tipo de trabajo de AWS Glue Spark con Scala, elija Spark como tipo de trabajo y un Language (Idioma) como Scala. Elija Spark 3.1, Scala 2 con un tiempo de inicio de trabajo mejorado (Glue versión 3.0) como versión de AWS Glue. Para ahorrar espacio de almacenamiento, en el siguiente ejemplo de AWS Glue with Scala también se utiliza la característica `applyMapping` para convertir tipos de datos.

Parámetros de AWS Glue Scala

```
import com.amazonaws.services.glue.util.GlueArgParser val args =
 GlueArgParser.getResolvedOptions(sysArgs, Seq("JOB_NAME", "inputLoc",
 "outputLoc").toArray)
```

Trabajo de AWS Glue Spark con código Scala

```
import com.amazonaws.services.glue.GlueContext
import com.amazonaws.services.glue.MappingSpec
import com.amazonaws.services.glue.DynamicFrame
import com.amazonaws.services.glue.errors.CallSite
import com.amazonaws.services.glue.util.GlueArgParser
import com.amazonaws.services.glue.util.Job
import com.amazonaws.services.glue.util.JsonOptions
import org.apache.spark.SparkContext
import scala.collection.JavaConverters._


object GlueScalaApp {
  def main(sysArgs: Array[String]) {
```

```
    @transient val spark: SparkContext = SparkContext.getOrCreate()
    val glueContext: GlueContext = new GlueContext(spark)

    val inputLoc = "s3://bucket-name/prefix/sample_data.csv"
    val outputLoc = "s3://bucket-name/prefix/"

    val readCSV = glueContext.getSource("csv", JsonOptions(Map("paths" ->
 Set(inputLoc)))).getDynamicFrame()

    val applyMapping = readCSV.applyMapping(mappings = Seq(("_c0", "string", "date",
 "string"), ("_c1", "string", "sales", "long"),
    ("_c2", "string", "profit", "double")), caseSensitive = false)

    val formatPartition = applyMapping.toDF().coalesce(1)

    val dynamicFrame = DynamicFrame(formatPartition, glueContext)

    val dataSink = glueContext.getSinkWithFormat(
        connectionType = "s3",
        options = JsonOptions(Map("path" -> outputLoc )),
        transformationContext = "dataSink", format =
 "parquet").writeDynamicFrame(dynamicFrame)
  }
}
```

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Visualice los registros de auditoría de Amazon Redshift con Amazon Athena y Amazon QuickSight

Sanket Sirsikar y Gopal Krishna Bhatia, Amazon Web Services

Resumen

La seguridad es una parte integral de las operaciones de base de datos en la nube de Amazon Web Services (AWS). Su organización debe asegurarse de supervisar las actividades y las conexiones de los usuarios de la base de datos para detectar posibles incidentes y riesgos de seguridad. Este patrón ayuda a supervisar las bases de datos con fines de seguridad y solución de problemas, un proceso que suele denominarse auditoría de base de datos.

Este patrón proporciona un script SQL que automatiza la creación de una tabla de Amazon Athena y vistas para un panel de informes en Amazon que le ayuda a auditar los registros de QuickSight Amazon Redshift. Esto garantiza que los usuarios responsables de supervisar las actividades de la base de datos tengan un acceso cómodo a las características de seguridad de los datos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un clúster de Amazon Redshift existente. Para obtener más información, consulte Create an Amazon Redshift cluster (Crear un clúster de Amazon Redshift) en la documentación de Amazon Redshift.
- Acceso a un grupo de trabajo de Athena existente. Para obtener más información, consulte How workgroups work (Cómo funcionan los grupos de trabajo) en la documentación de Amazon Athena.
- Un bucket de origen de Amazon Simple Storage Service (Amazon S3) con los permisos de AWS Identity and Access Management (IAM) requeridos. Para obtener más información, consulte Bucket permissions for Amazon Redshift audit logging (Permisos de bucket para el registro de auditoría de Amazon Redshift) en Database audit logging (Registros de auditoría de bases de datos) de la documentación de Amazon Redshift.

Arquitectura

Pila de tecnología

- Athena
- Amazon Redshift
- Amazon S3
- QuickSight

Tools (Herramientas)

- Amazon Athena : Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.
- Amazon QuickSight: QuickSight es un servicio de inteligencia empresarial (BI) escalable, sin servidor, integrable y basado en el aprendizaje automático.
- Amazon Redshift: Amazon Redshift es un servicio de almacenamiento de datos completamente administrado, de nivel empresarial y de escala de petabytes.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet.

Epics

Configurar el clúster de Amazon Redshift

Tarea	Descripción	Habilidades requeridas
Habilite el registro de auditoría para el clúster de Amazon Redshift.	1. Inicie sesión en la consola de administración de AWS, abra la consola de Amazon Redshift, seleccione CLUSTERS y, a continuación, el clúster para el que desea habilitar el registro. 2. Seleccione la pestaña Properties (Propiedades) y, a continuación, active	Administrador de base de datos, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	la auditoría; para ello, siga las instrucciones de Configuring auditing using the console (Configurar la auditoría mediante la consola) en la documentación de Amazon Redshift.	

Tarea	Descripción	Habilidades requeridas
Habilite el registro en el grupo de parámetros del clúster de Amazon Redshift.	Puede habilitar la auditoría de los registros de conexión, los registros de usuario y los registros de actividad de los usuarios al mismo tiempo mediante la Consola de administración de AWS, la API de referencia de Amazon Redshift o la interfaz de la línea de comandos de AWS (AWS CLI). Para auditar los registros de actividad de los usuarios, también debe habilitar el parámetro `enable_user_activity_logging` de la base de datos. Si habilita solo la característica de registro de auditoría y no el parámetro asociado, los registros de auditoría de la base de datos registrarán únicamente la información de los registros de conexión y de usuario, pero no la del registro de actividad del usuario. El parámetro `enable_user_activity_logging` no está habilitado de forma predeterminada, pero puede activarlo cambiándolo de `false` a `true`.	Administrador de base de datos, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	Important Debe crear un nuevo grupo de parámetros de clúster con el parámetro `user_activity_logging` activado y adjuntarlo a su clúster de Amazon Redshift. Para obtener más información, consulte Modifying a cluster (Cómo modificar un clúster) en la documentación de Amazon Redshift. Para obtener más información sobre esta tarea, consulte Amazon Redshift parameter groups (Grupos de parámetros de Amazon Redshift) y Configuring auditing using the console (Configurar la auditoría mediante la consola) en la documentación de Amazon Redshift.	

Tarea	Descripción	Habilidades requeridas
Configure los permisos del bucket de S3 para el registro de clúster de Amazon Redshift.	Al habilitar el registro, Amazon Redshift recopila la información de los registros y la carga en los archivos de registro almacenados en el bucket de S3. Puede crear un nuevo bucket de S3 o utilizar un bucket existente. **Important** Asegúrese de que Amazon Redshift tenga los permisos de IAM requeridos para tener acceso al bucket de S3. Para obtener más información al respecto, consulte Bucket permissions for Amazon Redshift audit logging (Permisos de bucket para el registro de auditoría de Amazon Redshift) en Database audit logging (Registros de auditoría de bases de datos) de la documentación de Amazon Redshift.	Administrador de base de datos, ingeniero de datos

Crear la tabla y las vistas de Athena

Tarea	Descripción	Habilidades requeridas
Cree la tabla y las vistas de Athena para consultar los datos del registro de auditoría de Amazon Redshift desde el bucket de S3.	Abra la consola de Amazon Athena y utilice la consulta del lenguaje de definición de datos (DDL) del script de SQL `AuditLogging.sql` (adjunto) para crear la tabla y las vistas de los registros de actividad de los usuarios, los registros de usuarios y los registros de conexión. Para obtener más informaci ón e instrucciones, consulte el tutorial Create tables and run queries (Crear tablas y ejecutar consultas) del taller de Amazon Athena.	Ingeniero de datos

Configure la supervisión de registros en el panel de control QuickSight

Tarea	Descripción	Habilidades requeridas
Cree un QuickSight cuadro de mando con Athena como fuente de datos.	Abre la QuickSight consola de Amazon y crea un QuickSigh t panel de control siguiendo las instrucciones del tutorial Visualiza QuickSight con Athena del taller de Amazon Athena.	Administrador de base de datos, ingeniero de datos

Recursos relacionados

- Create tables and run queries in Athena (Crear crear tablas y ejecutar consultas en Athena)
- Visualice QuickSight con Athena

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Visualice los informes de credenciales de IAM para todas las cuentas de AWS mediante Amazon Quick Sight

Parag Nagwekar y Arun Chandapillai, Amazon Web Services

Resumen

> Advertencia: Los usuarios de IAM tienen credenciales de larga duración, lo que supone un riesgo de seguridad. Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten.

Puede utilizar los informes de credenciales de AWS Identity and Access Management (IAM) para ayudarle a cumplir los requisitos de seguridad, auditoría y conformidad de su organización. Los informes de credenciales proporcionan una lista de todos los usuarios de sus cuentas de AWS y muestran el estado de sus credenciales, como las contraseñas, claves de acceso y dispositivos de autenticación multifactor (MFA). Puede usar informes de credenciales para varias cuentas de AWS administradas por AWS Organizations.

Este patrón incluye pasos y código para ayudarle a crear y compartir informes de credenciales de IAM para todas las cuentas de AWS de su organización mediante los paneles de Amazon Quick Sight. Puede compartir los paneles con las partes interesadas de su organización. Los informes pueden ayudar a su organización a lograr los siguientes resultados empresariales previstos:

- Identifique los incidentes de seguridad relacionados con los usuarios de IAM
- Realice un seguimiento de la migración en tiempo real de los usuarios de IAM a la autenticación de inicio de sesión único (SSO)
- Realice un seguimiento de las regiones de AWS a las que acceden los usuarios de IAM
- Manténgase en conformidad
- Comparta información con otras partes interesadas

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Las cuentas miembro de una organización
- Un rol de IAM con permisos para acceder a las cuentas de Organizations
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2, instalada y configurada
- Una suscripción a la edición Amazon Quick Enterprise

Arquitectura

Pila de tecnología

- Amazon Athena
- Amazon EventBridge
- Amazon Quick Suite
- Amazon Simple Storage Service (Amazon S3)
- AWS Glue
- AWS Identity y Access Management (IAM)
- AWS Lambda
- AWS Organizations

Arquitectura de destino

El siguiente diagrama muestra una arquitectura para configurar un flujo de trabajo que captura los datos de los informes de credenciales de IAM de varias cuentas de AWS.

1. EventBridge invoca una función Lambda a diario.
2. La función de Lambda asume un rol de IAM en todas las cuentas de AWS de la organización. A continuación, la función crea el informe de credenciales de IAM y almacena los datos del informe en un bucket de S3 centralizado. Debe habilitar el cifrado y desactivar el acceso público en el bucket de S3.
3. Un rastreador de AWS Glue rastrea el depósito de S3 a diario y actualiza la tabla de Athena en consecuencia.
4. Quick Sight importa y analiza los datos del informe de credenciales y crea un panel que las partes interesadas pueden visualizar y compartir con ellas.

Tools (Herramientas)

Servicios de AWS

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, funciones de Lambda, puntos de conexión de invocación HTTP que utilizan destinos API o buses de eventos en otras cuentas de AWS.
- Amazon QuickSight es un servicio de inteligencia empresarial (BI) a escala de la nube que lo ayuda a visualizar, analizar y generar informes de sus datos en un único panel. Quick Sight es un componente central de Amazon Quick, que proporciona visualización interactiva de datos, análisis en memoria de SPICE, análisis integrados y uso compartido de paneles.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

Código

El código de este patrón está disponible en el GitHub getiamcredsreport-allaccounts-orgrepositorio. Puede usar el código de este repositorio para crear informes de credenciales de IAM en todas las cuentas de AWS en Organizations y almacenarlos en una ubicación central.

Epics

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Configura la edición Amazon Quick Enterprise.	1. Active la edición Amazon Quick Enterprise en su cuenta de AWS. Para obtener más información,	Administrador de AWS DevOps, administrador de la nube, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	consulta Administrar el acceso de los usuarios dentro de Amazon Quick en la documentación de Quick. 2. Para conceder permisos al panel de control, obtenga el nombre de recurso de Amazon (ARN) de los usuarios de Quick Sight.	
Integre Amazon Quick Sight con Amazon S3 y Athena.	Debe autorizar a Quick Sight a utilizar Amazon S3 y Athena antes de implementar la pila de AWS CloudFormation .	Administrador de AWS DevOps, administrador de la nube, arquitecto de la nube

Implementación de la infraestructura

Tarea	Descripción	Habilidades requeridas
Clona el GitHub repositorio.	1. Clone el GitHub getiamcredsreport-allaccounts-orgrepositorio en su máquina local ejecutando el siguiente comando: `git clone https://github.com/aws-samples/getiamcredsreport-allaccounts-org`	Administrador de AWS
Implemente la infraestructura.	1. Inicie sesión en la consola de administración de AWS y abra la consola de CloudFormation .	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	2. En el panel de navegación, seleccione Crear pila y, a continuación, seleccione Con nuevos recursos (estándar). 3. En la página Identificar recursos, seleccione Siguiente. 4. En la página Especificar plantilla, en Origen de la plantilla, seleccione Cargar un archivo de plantilla. 5. Elija Elegir archivo, seleccione el `Cloudformation-createcredrepo.yaml` archivo del GitHub repositorio clonado y, a continuación, elija Siguiente. 6. En Parámetros, actualice `IAMRoleName` con su rol de IAM. Esta debe ser el rol de IAM que desea que Lambda asuma en todas las cuentas de la organización. Esta función crea el informe de credenciales. Nota: No es necesario que el rol esté presente en todas las cuentas en este paso de la creación de la pila. 7. En Parámetros, actualice `S3BucketName` con el	

Tarea	Descripción	Habilidades requeridas
	nombre del bucket de S3 donde Lambda puede almacenar las credenciales de todas las cuentas. 8. En Nombre de la pila, introduzca el nombre de la pila. 9. Seleccione Enviar. 10 Anote el nombre del rol de la función de Lambda.	
Cree una política de permisos de IAM.	Cree una política de IAM para cada cuenta de AWS de su organización con los siguientes permisos: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "iam:GenerateCredentialReport", "iam:GetCredentialReport" ], "Resource": "*" } ] }`	AWS DevOps, administrador de nube, arquitecto de nube, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
Cree un rol de IAM con una política de confianza.	1. Cree un rol de IAM para las cuentas de AWS y adjunte la política de permisos que creó en el paso anterior. 2. Adjunte la siguiente política de confianza al rol de IAM: `{ "Version": "2012-10-17", "Statement":[ { "Effect": "Allow", "Principal":{ "AWS":[ "arn:aws:iam::<MasterAccountID>:role/<LambdaRole>" ] }, "Action": "sts:AssumeRole" } ] }` **Important** Sustituya `arn:aws:iam::<MasterAccountID>:role/<LambdaRole>` por el ARN de la función	Administrador de la nube, arquitecto de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	de Lambda que indicó anteriormente. **Note** Las organizaciones suelen utilizar la automatización para crear funciones de IAM para sus cuentas de AWS. Le recomendamos que utilice esta automatización, si está disponible. Como alternativa, puede utilizar el `CreateRoleforOrg.py` script del repositorio de código . El script requiere una función administrativa existente o cualquier otro rol de IAM que tenga permiso para crear una política y un rol de IAM en cada cuenta de AWS.	

Tarea	Descripción	Habilidades requeridas
Configure Amazon Quick Sight para visualizar los datos.	1. Inicie sesión en Quick con sus credenciales. 2. Cree un conjunto de datos con Athena (con la base de datos `iamcredreportdb` y la tabla `"cfn_iamcredreport"`) y, a continuación, actualice automáticamente el conjunto de datos. 3. Cree un análisis en Quick Sight. 4. Cree un panel de Quick Sight.	AWS DevOps, administrador de nube, arquitecto de nube, ingeniero de datos

Información adicional

Consideraciones adicionales

Considere lo siguiente:

- Después de implementar la infraestructura, puede esperar a que Athena cree los informes en Amazon S3 y los analice hasta que Lambda y AWS Glue se ejecuten según lo programado. CloudFormation Como alternativa, puede ejecutar Lambda manualmente para obtener los informes en Amazon S3 y, a continuación, ejecutar el rastreador AWS Glue para obtener la tabla Athena que se crea a partir de los datos.
- Quick es una poderosa herramienta para analizar y visualizar datos en función de los requisitos de su empresa. Puedes usar los parámetros de Quick para controlar los datos de los widgets en función de los campos de datos que elijas. Además, puedes usar un análisis rápido para crear parámetros (por ejemplo, campos de cuenta, fecha y usuario, por ejemplo, y `partition_0partition_1`, `user` respectivamente) a partir de tu conjunto de datos para añadir controles a los parámetros de cuenta, fecha y usuario.
- Para crear sus propios paneles de Quick Sight, consulte Quick Workshops en el sitio web de AWS Workshop Studio.

- Para ver ejemplos de cuadros de mando de Quick Sight, consulte el repositorio de GitHub getiamcredsreport-allaccounts-orgcódigos.

Resultados empresariales específicos

Puede utilizar esta guía para lograr los siguientes resultados empresariales:

- Identifique los incidentes de seguridad relacionados con los usuarios de IAM: investigue a todos los usuarios de todas las cuentas de AWS de su organización mediante un único panel de control. Puede realizar un seguimiento de la tendencia de las regiones de AWS individuales a las que accedió más recientemente un usuario de IAM y de los servicios que utilizó.
- Realice un seguimiento de la migración en tiempo real de los usuarios de IAM a la autenticación de SSO: mediante el SSO, los usuarios pueden iniciar sesión una vez con una sola credencial y acceder a varias cuentas y aplicaciones de AWS. Si planea migrar sus usuarios de IAM al SSO, este patrón puede ayudarlo a realizar la transición al SSO y a realizar un seguimiento del uso de todas las credenciales de los usuarios de IAM (como el acceso a la consola de administración de AWS o el uso de claves de acceso) en todas las cuentas de AWS.
- Realice un seguimiento de las regiones de AWS a las que acceden los usuarios de IAM: puede controlar el acceso de los usuarios de IAM a las regiones con diversos fines, como la soberanía de los datos y el control de costos. También puede realizar un seguimiento del uso de las regiones por parte de cualquier usuario de IAM.
- Cumpla con las normas: si sigue el principio de privilegios mínimos, solo puede conceder los permisos de IAM específicos necesarios para realizar una tarea específica. Además, puede realizar un seguimiento del acceso a los servicios de AWS, a la consola de administración de AWS y al uso prolongado de las credenciales.
- Comparta información con otras partes interesadas: puede compartir paneles seleccionados con otras partes interesadas, sin darles acceso a los informes de credenciales de IAM ni a las cuentas de AWS.

Más patrones

- Autentique a los usuarios de la aplicación React mediante las interfaces de usuario de Amazon Cognito y AWS Amplify
- Extraer contenido de archivos PDF automáticamente con Amazon Textract
- Cree un modelo de previsión de arranque en frío utilizando DeepAR para series temporales en SageMaker Amazon AI Studio Lab
- Crear informes detallados de costos y uso para los clústeres de Amazon EMR mediante el explorador de costos de AWS.
- Crear informes detallados de costos y uso para Amazon RDS y Amazon Aurora
- Crear informes detallados de costos y uso para los trabajos de AWS Glue con el explorador de costos de AWS
- Entregue registros de DynamoDB a Amazon S3 mediante Kinesis Data Streams y Firehose con AWS CDK
- Implemente un trabajo de AWS Glue con una canalización de CodePipeline CI/CD de AWS
- Incorpore componentes visuales de Amazon Quick Sight en aplicaciones web mediante Amazon Cognito y la automatización iAC
- Costos de almacenamiento estimados para una tabla de Amazon DynamoDB
- Ejecución de consultas SQL en Amazon Redshift mediante Terraform
- Extraer y consultar atributos de AWS IoT SiteWise metadatos en un lago de datos
- Genere información de datos mediante AWS Mainframe Modernization Amazon Q en Quick Sight
- Genere información sobre z/OS datos de Db2 mediante AWS Mainframe Modernization Amazon Q en Quick Sight
- Otorgue a las instancias de SageMaker notebook acceso temporal a un CodeCommit repositorio de otra cuenta de AWS
- Identifique y avise cuando los recursos de Amazon Data Firehose no estén cifrados con una clave AWS KMS
- Importe la biblioteca psycopg2 para interactuar con su base de AWS Lambda datos PostgreSQL
- Ingesta y análisis de registros de seguridad de AWS en Microsoft Sentinel
- Migración de Amazon RDS para Oracle a Amazon RDS para PostgreSQL en modo SSL mediante AWS DMS
- Migre una base de datos Oracle a Amazon RDS for Oracle mediante adaptadores de archivos planos de GoldenGate Oracle

- Migración de una base de datos de Oracle a Amazon Redshift con AWS DMS y AWS SCT
- Migre datos de un entorno Hadoop local a Amazon S3 con DistCp AWS PrivateLink para Amazon S3
- Migración de Couchbase Server a Couchbase Capella en AWS
- Migración de cargas de trabajo de Cloudera en las instalaciones a la plataforma de datos de Cloudera en AWS
- Administración de la conmutación por error de multi-AZ para clústeres de EMR mediante el Controlador de recuperación de aplicaciones
- Automatice blue/green las implementaciones de las bases de datos globales de Amazon Aurora mediante los principios de la IaC
- AWS Service Catalog Aprovisione productos en función de AWS CloudFormation plantillas mediante GitHub acciones
- Ejecute pruebas unitarias para trabajos ETL de Python AWS Glue utilizando el marco pytest
- Configurar un panel de monitoreo de Grafana para AWS ParallelCluster
- Descarga de datos de un clúster de Amazon Redshift entre las cuentas a Amazon S3
- Visualice los resultados del AI/ML modelo con Flask y AWS Elastic Beanstalk

Computación

Temas

- Contenedores y microservicios
- Sin servidor
- Red
- Entrega de contenido

Contenedores y microservicios

Temas

- Acceso a una base de datos de Amazon Neptune desde un contenedor de Amazon EKS
- Acceda a las aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS PrivateLink y un Network Load Balancer
- Acceda a las aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS Fargate PrivateLink, AWS y un Network Load Balancer
- Acceda a aplicaciones de contenedores de forma privada en Amazon EKS mediante AWS PrivateLink y un Network Load Balancer
- Automatizar las copias de seguridad de las instancias de base de datos de Amazon RDS para PostgreSQL mediante AWS Batch
- Automatice la implementación del controlador de terminación de nodos en Amazon EKS mediante una CI/CD canalización
- Cree e implemente automáticamente una aplicación Java en Amazon EKS mediante una CI/CD canalización
- Copie imágenes de contenedores de Amazon ECR en y Cuentas de AWS Regiones de AWS
- Cree una definición de tareas de Amazon ECS y monte un sistema de archivos en EC2 las instancias mediante Amazon EFS
- Implementar funciones de Lambda con imágenes de contenedor
- Implementar microservicios de Java en Amazon ECS con AWS Fargate
- Implementar recursos y paquetes de Kubernetes con Amazon EKS y un repositorio de gráficos de Helm en Amazon S3
- Implemente un clúster de CockroachDB en Amazon EKS mediante Terraform
- Implemente un microservicio Java de muestra en Amazon EKS y exponga el microservicio mediante un Equilibrador de carga de aplicación
- Implemente una aplicación basada en gRPC en un clúster de Amazon EKS y acceda a ella con un Equilibrador de carga de aplicación
- Implemente aplicaciones en contenedores si se AWS IoT Greengrass V2 ejecutan como un contenedor Docker
- Implementar contenedores mediante Elastic Beanstalk
- Habilite el modo automático de Amazon EKS en todos los clústeres de EKS mediante GitHub acciones

- Genere una dirección IP saliente estática mediante una función de Lambda, Amazon VPC y una arquitectura sin servidor
- Identificación automática de las imágenes de contenedor duplicadas al migrar a un repositorio de Amazon ECR
- Instalación del agente SSM en los nodos de trabajo de Amazon EKS mediante Kubernetes DaemonSet
- Instale el agente SSM y el CloudWatch agente en los nodos de trabajo de Amazon EKS mediante preBootstrapCommands
- Migración de los controladores de entrada NGINX al activar el Modo automático de Amazon EKS
- Migre sus cargas de trabajo de contenedores de Azure Red Hat OpenShift (ARO) a Red Hat OpenShift Service en AWS (ROSA)
- Ejecute tareas de Amazon ECS en Amazon WorkSpaces con Amazon ECS Anywhere
- Ejecute un contenedor Docker de la API web de ASP.NET Core en una instancia de Amazon Linux EC2
- Ejecutar cargas de trabajo con estado y almacenamiento de datos persistente mediante Amazon EFS en Amazon EKS con AWS Fargate
- Configuración del escalado automático basado en eventos en Amazon EKS mediante Amazon EKS Pod Identity y KEDA
- Simplificación de las implementaciones de PostgreSQL en Amazon EKS mediante PGO
- Simplificación de la autenticación de aplicaciones con TLS mutuo en Amazon ECS mediante el equilibrador de carga de aplicación
- Más patrones

Acceso a una base de datos de Amazon Neptune desde un contenedor de Amazon EKS

Ramakrishnan Palaninathan, Amazon Web Services

Resumen

Este patrón establece una conexión entre Amazon Neptune, que es una base de datos de gráficos totalmente gestionada, y Amazon Elastic Kubernetes Service (Amazon EKS), un servicio de orquestación de contenedores, para acceder a una base de datos de Neptune. Los clústeres de la base de datos de Neptune están confinados dentro de una nube privada virtual (VPC) en AWS. Por este motivo, el acceso a Neptune requiere una configuración cuidadosa de la VPC para permitir la conectividad.

A diferencia de Amazon Relational Database Service (Amazon RDS) para PostgreSQL, Neptune no depende de las credenciales de acceso a bases de datos típicas. En su lugar, utiliza funciones AWS Identity and Access Management (IAM) para la autenticación. Por lo tanto, conectarse a Neptune desde Amazon EKS implica configurar un rol de IAM con los permisos necesarios para acceder a Neptune.

Además, solo se puede acceder a los puntos de conexión de Neptune dentro de la VPC en la que se encuentra el clúster. Esto significa que debe configurar los ajustes de red para facilitar la comunicación entre Amazon EKS y Neptune. Según sus requisitos específicos y sus preferencias de red, existen varios enfoques para configurar la VPC a fin de permitir una conectividad fluida entre Neptune y Amazon EKS. Cada método ofrece ventajas y opciones distintas, que proporcionan flexibilidad a la hora de diseñar la arquitectura de la base de datos para adaptarla a las necesidades de la aplicación.

Requisitos previos y limitaciones

Requisitos previos

- Instale la última versión de kubectl (consulte las instrucciones). Para comprobar la versión, ejecute:

```
kubectl version --short
```

- Instale la última versión de eksctl (consulte las instrucciones). Para comprobar la versión, ejecute:

```
eksctl info
```

- Instale la última versión de la AWS Command Line Interface (AWS CLI) versión 2 (consulte las instrucciones). Para comprobar la versión, ejecute:

```
aws --version
```

- Cree un clúster de base de datos de Neptune (consulte las instrucciones). Asegúrese de establecer las comunicaciones entre la VPC del clúster y Amazon EKS mediante el emparejamiento de VPC, AWS Transit Gateway, u otro método. Asegúrese también de que el estado del clúster esté como Disponible y de que tenga una regla de entrada en el puerto 8182 para el grupo de seguridad.
- Configure un proveedor de IAM OpenID Connect (OIDC) en un clúster de Amazon EKS existente (consulte las instrucciones).

Versiones de producto

- Amazon EKS 1.27
- Versión 1.3.0.0 del motor de Amazon Neptune (2023-11-15)

Arquitectura

En el siguiente diagrama se muestra la conexión entre los pods de Kubernetes de un clúster de Amazon EKS y Neptuno para proporcionar acceso a una base de datos de Neptune.

Automatización y escala

Puede usar el escalador automático de pods horizontales para escalar esta solución.

Tools (Herramientas)

Servicios

- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar AWS Kubernetes sin necesidad de instalar o mantener su propio plano de control o nodos de Kubernetes.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- Amazon Neptune es un servicio de base de datos de gráficos que le permite crear y ejecutar aplicaciones que funcionen con conjuntos de datos altamente conectados.

Prácticas recomendadas

Para obtener información sobre las prácticas recomendadas, consulte Identity and Access Management en las guías de prácticas recomendadas de Amazon EKS.

Epics

Configuración de las variables de entorno

Tarea	Descripción	Habilidades requeridas
Verifique el contexto del clúster.	Antes de interactuar con su clúster de Amazon EKS mediante Helm u otras herramientas de línea de comandos, debe definir las variables de entorno que encapsulen los detalles del clúster. Estas variables se utilizan en los comandos posteriores para garantizar que se dirijan al clúster y los recursos correctos. En primer lugar, confirme que está trabajando en el contexto de clúster correcto. Esto garantiza que cualquier comando posterior se envíe al clúster de Kubernetes deseado. Para comprobar el contexto actual, ejecute el siguiente comando. `kubectl config current-context`	Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
Defina la variable `CLUSTER_NAME` .	Establezca la variable de entorno `CLUSTER_NAME` para el clúster de Amazon EKS. En el siguiente comando, sustituya el valor `us-west-2` de muestra por el correcto Región de AWS para su clúster. Reemplace el valor de muestra `eks-workshop` por el nombre de su clúster existente. `export CLUSTER_NAME=$(aws eks describe-cluster --region us-west-2 --name eks-workshop --query "cluster.name" --output text)`	Administrador de la nube, administrador de AWS
Valide la salida.	Para comprobar que las variables se hayan configurado correctamente, ejecute el siguiente comando. `echo $CLUSTER_NAME` Compruebe que el resultado de este comando coincida con la entrada que especificó en el paso anterior.	Administrador de la nube, administrador de AWS

Cree un rol de IAM y asócielo con Kubernetes

Tarea	Descripción	Habilidades requeridas
Cree una cuenta de servicio de .	Utilice roles de IAM para cuentas de servicio y así poder asignar sus cuentas de servicio de Kubernetes a roles de IAM para habilitar una administración de permisos detallada en las aplicaciones que se ejecutan en Amazon EKS. Puede usar eksctl para crear y asociar un rol de IAM a una cuenta de servicio de Kubernetes específica dentro de su clúster de Amazon EKS. La política AWS administr ada `NeptuneFullAccess` permite el acceso de escritura y lectura al clúster de Neptune especificado. **Important** Debe tener un punto de conexión OIDC asociado a su clúster antes de ejecutar estos comandos. Cree una cuenta de servicio que desee asociar a una política AWS administrada denominada`NeptuneFu llAccess` .	Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas

	`eksctl create iamserviceaccount --name eks-neptune-sa --namespace default --cluster $CLUSTER_NAME --attach-policy-arn arn:aws:iam::aws:policy/NeptuneFullAccess --approve --override-existing-serviceaccounts`
	
	`eks-neptune-sa` será el nombre de la cuenta de servicio que quiera crear.
	
	Al finalizar, el comando muestra la siguiente respuesta:
	
	`2024-02-07 01:12:39 [#] created serviceaccount "default/eks-neptune-sa"`	

Tarea	Descripción	Habilidades requeridas

Compruebe que la cuenta esté configurada correctamente.	Asegúrese de que la cuenta de servicio de `eks-neptune-sa` esté configurada correctamente en el espacio de nombres predeterminado del clúster.
	
	`kubectl get sa eks-neptune-sa -o yaml`
	
	La salida debe tener el siguiente aspecto:
	
	`apiVersion: v1`
	`kind: ServiceAccount`
	`metadata:`
	`  annotations:`
	`  eks.amazonaws.com/role-arn: arn:aws:iam::123456789123:role/eksctl-eks-workshop-addon-iamserviceaccount-d-Role1-Q35yKgdQOlmM`
	`  creationTimestamp: "2024-02-07T01:12:39Z"`
	`  labels:`
	`  app.kubernetes.io/managed-by: eksctl`
	`  name: eks-neptune-sa`
	`  namespace: default`
	`  resourceVersion: "5174750"`
	`  uid: cd6ba2f7-a0f5-40e1-a6f4-4081e0042316`
		Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas

Compruebe la conectividad.	Implemente un pod de muestra llamado `pod-util` y compruebe la conectividad con Neptune.
	
	`apiVersion: v1`
	`kind: Pod`
	`metadata:`
	`  name: pod-util`
	`  namespace: default`
	`spec:`
	`  serviceAccountName:`
	` eks-neptune-sa`
	`  containers:`
	`  - name: pod-util`
	`  image: public.ec`
	`r.aws/patrickc/tro`
	`ubleshoot-util`
	`  command:`
	`  - sleep`
	`  - "3600"`
	`  imagePullPolicy:`
	` IfNotPresent`
	
	`kubectl apply -f pod-`
	`util.yaml`
	
	`kubectl exec --stdin --`
	`tty pod-util -- /bin/`
	`bash`
	`bash-5.1# curl -X POST`
	` -d '{"gremlin":"g.V()`
	`.limit(1)"}' https://`
	`db-neptune-1.cluste`
	`r-xxxxxxxxxxx.us-`
	`west-2.neptune.ama`
	`zonaws.com:8182/gr`
	`emlin`
		Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	{"requestId":"a4964f2d-12b1-4ed3-8a14-eff511431a0e","status":{"message":"","code":200,"attributes":{"@type":"g:Map","@value":[]},"result":{"data":{"@type":"g:List","@value":[]},"meta":{"@type":"g:Map","@value":[]}}} bash-5.1# exit exit	

Comprobar la actividad de la conexión

Tarea	Descripción	Habilidades requeridas
Habilite la autenticación de bases de datos de IAM	De forma predeterminada, la autenticación de bases de datos de IAM está deshabilitada al crear un clúster de Neptune DB. Puede habilitar o deshabilitar la autenticación de la base de datos IAM mediante Consola de administración de AWS. Siga los pasos de la AWS documentación para habilitar la autenticación de bases de datos de IAM en Neptune.	Administrador de la nube, administrador de AWS
Compruebe las conexiones.	En este paso, interactuará con el contenedor de `pod-util`, que ya está en ejecución, para	Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas

	instalar awscurl y comprobar la conexión.
	
	1. Ejecute el comando siguiente para buscar el pod.
	
	`kubectl get pods`
	
	La salida debe tener el siguiente aspecto:
	
	`NAME READY STATUS RESTARTS AGE pod-util 1/1 Running 0 50m`
	
	2. Ejecute el siguiente comando para instalar awscurl.
	
	`kubectl exec --stdin --tty pod-util -- /bin/bash bash-5.1# pip3 install awscurl Installing collected packages: idna, configparser, configargparse, charset-normalizer, certifi, requests, awscurl Successfully installed awscurl-0.32 certifi-2024.2.2 charset-normalizer-3.3.2 configargparse-1.7 configparser-6.0.0 idna-3.6 requests-2.31.0`	

Tarea	Descripción	Habilidades requeridas
	bash-5.1# awscurl https://db-neptune-1.cluster-xxxxxxxxxxxx.us-west-2.neptune.amazonaws.com:8182/status --region us-west-2 --service neptune-db {"status":"healthy","startTime":"Thu Feb 08 01:22:14 UTC 2024","dbEngineVersion":"1.3.0.0.R1","role":"writer","dfeQueryEngine":"viaQueryHint","gremlin":{"version":"tinkerpop-3.6.4"},"sparql":{"version":"sparql-1.1"},"opencypher":{"version":"Neptune-9.0.20190305-1.0"},"labMode":{"ObjectIndex":"disabled","ReadWriteConflictDetection":"enabled"},"features":{"SlowQueryLogs":"disabled","ResultCache":{"status":"disabled"},"IAMAuthentication":"enabled","Streams":"disabled","AuditLog":"disabled"},"settings":{"clusterQueryTimeoutInMs":"120000","SlowQueryLogsThreshold":"5000"}}	

Resolución de problemas

Problema	Solución
No se puede acceder a la base de datos de Neptune.	Revise la política de IAM adjunta a la cuenta de servicio. Asegúrese de que permite realizar las acciones necesarias (por ejemplo, `neptune:Connec,neptune:DescribeDBInstances`) para las operaciones que desee ejecutar.

Recursos relacionados

- Otorgue a las cargas de trabajo de Kubernetes acceso al AWS uso de cuentas de servicio de Kubernetes (documentación de Amazon EKS)
- Roles de IAM para cuentas de servicio (documentación de Amazon EKS)
- Creación de un nuevo clúster de base de datos de Neptune (documentación de Amazon Neptune)

Acceda a las aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS PrivateLink y un Network Load Balancer

Kirankumar Chandrashekar, Amazon Web Services

Resumen

Este patrón describe cómo alojar de forma privada una aplicación contenedora de Docker en Amazon Elastic Container Service (Amazon ECS) detrás de un Network Load Balancer y cómo acceder a la aplicación mediante AWS. PrivateLink A continuación, puede utilizar una red privada para acceder de forma segura a los servicios de la nube de Amazon Web Services (AWS). Amazon Relational Database Service (Amazon RDS) aloja la base de datos relacional para la aplicación que se ejecuta en Amazon ECS con alta disponibilidad (HA). Se usa Amazon Elastic File System (Amazon EFS) si la aplicación necesita almacenamiento persistente.

El servicio Amazon ECS que ejecuta las aplicaciones de Docker, con un Network Load Balancer en la interfaz, se puede asociar a un punto final de nube privada virtual (VPC) para acceder a él a través de AWS. PrivateLink Luego, este servicio de punto final de VPC se puede compartir con otros VPCs mediante sus puntos de enlace de VPC.

También puede usar AWS Fargate en lugar de un grupo de Amazon EC2 Auto Scaling. Para obtener más información, consulte Acceda a aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS Fargate PrivateLink, AWS y un Network Load Balancer.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2, instalada y configurada en Linux, macOS o Windows
- Docker, instalado y configurado en Linux, macOS o Windows
- Una aplicación que se ejecuta en Docker

Arquitectura

Pila de tecnología

- Amazon CloudWatch
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon EC2 Auto Scaling
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon ECS
- Amazon RDS
- Amazon Simple Storage Service (Amazon S3)
- AWS Lambda
- AWS PrivateLink
- AWS Secrets Manager
- Equilibrador de carga de aplicación
- Equilibrador de carga de red
- VPC

Automatización y escala

- Puede usar AWS CloudFormation para crear este patrón mediante Infrastructure as Code.

Tools (Herramientas)

- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS.
- Amazon EC2 Auto Scaling: Amazon EC2 Auto Scaling le ayuda a garantizar que dispone del número correcto de EC2 instancias de Amazon disponibles para gestionar la carga de su aplicación.
- Amazon ECS: Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores altamente escalable y rápido que facilita la tarea de ejecutar, detener y administrar contenedores en un clúster.
- Amazon ECR: Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor de AWS administrado que es seguro, escalable y fiable.
- Amazon EFS: Amazon Elastic File System (Amazon EFS) ofrece un sistema de archivos NFS sencillo, escalable, elástico y completamente administrado que se utiliza con servicios de nube de AWS y recursos en las instalaciones.

- AWS Lambda: AWS Lambda es un servicio informático para ejecutar código sin aprovisionar ni administrar servidores.
- Amazon RDS: Amazon Relational Database Service (Amazon RDS) es un servicio web que facilita la configuración, el funcionamiento y el escalado de una base de datos relacional en la nube de AWS.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet. Está diseñado para facilitar a los desarrolladores recursos de computación escalables basados en Web.
- AWS Secrets Manager: Secrets Manager permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, proponiendo una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- Amazon VPC: Amazon Virtual Private Cloud (Amazon VPC) permite lanzar recursos de AWS en una red virtual previamente definida.
- Elastic Load Balancing: Elastic Load Balancing distribuye el tráfico entrante de aplicaciones o redes entre varios destinos, como EC2 instancias de Amazon, contenedores y direcciones IP, en varias zonas de disponibilidad.
- Docker: Docker ayuda a los desarrolladores a empaquetar, enviar y ejecutar cualquier aplicación como un contenedor ligero, portátil y autosuficiente.

Epics

Creación de componentes de redes

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon VPC. Seleccione Crear VPC y, a continuación, VPC y más. 2. Especifique un nombre para su VPC y seleccione un rango de bloques CIDR adecuado.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	3. Especifique dos zonas de disponibilidad, dos subredes públicas y cuatro subredes privadas. Dos subredes privadas son para las tareas de Amazon ECS y otras dos subredes privadas son para las bases de datos de Amazon RDS. 4. Especifique una puerta de enlace NAT para cada zona de disponibilidad. 5. Seleccione Creación de VPC.	

Crear el equilibrador de carga

Tarea	Descripción	Habilidades requeridas
Crear un equilibrador de carga de red.	1. Abre la EC2 consola de Amazon y elige la región de AWS que contiene tu VPC. 2. En Equilibrio de carga seleccione Equilibradores de carga y Crear equilibra dor de carga. 3. Seleccione Equilibrador de carga de red y luego Crear. 4. En la página Configurar el equilibrador de carga, configure el equilibrador de carga de red y el oyente. Importante: Asegúrese	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	de elegir el esquema del equilibrador de carga de red como Interno. 5. Seleccione los ajustes de seguridad aplicable s, configure un grupo de seguridad y un grupo de destino. Seleccione Instancia o IP como Tipo de destino en la sección Configurar enrutamiento. Asegúrese de no registrar un destino. 6. Una vez haya configurado todos los ajustes, seleccion e Siguiente: Revisar y, a continuación, seleccione Crear.	

Tarea	Descripción	Habilidades requeridas
Cree un Equilibrador de carga de aplicación.	1. En la EC2 consola de Amazon, elige la misma región que contiene tu VPC. 2. En Equilibrio de carga seleccione Equilibradores de carga y Crear equilibrador de carga. 3. Seleccione Application Load Balancer (Equilibrador de carga de aplicación) y, a continuación, Create. 4. **Important** Configure el equilibrador de carga de aplicación y el oyente. Asegúrese de elegir el esquema del equilibrador de carga de aplicación como interno. 5. Seleccione los ajustes de seguridad aplicables, configure un grupo de seguridad y un grupo de destino. Seleccione Instancia o IP como Tipo de destino en la sección Configurar enrutamiento. Asegúrese de no registrar un destino.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	6. Una vez haya configurado todos los ajustes, seleccione Siguiente: Revisar y, a continuación, seleccione Crear.	

Crear un sistema de archivos de Amazon EFS

Tarea	Descripción	Habilidades requeridas
Crear un sistema de archivos de Amazon EFS.	1. Abra la consola de Amazon EFS y seleccione Crear sistema de archivos. 2. En el cuadro de diálogo Crear sistema de archivos, especifique un nombre para su sistema de archivos y seleccione su VPC. 3. Seleccione Crear para crear el sistema de archivos. 4. Instale y configure su sistema de archivos de Amazon EFS.	Administrador de la nube
Defina el montaje de los destinos para las subredes.	1. Regrese a la consola de Amazon EFS y seleccione Sistemas de archivos. La página Sistemas de archivos muestra los sistemas de archivos Amazon EFS de su cuenta. 2. Seleccione el sistema de archivos que creó y seleccione Administrar	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	para mostrar las Zonas de disponibilidad. Para añadir un destino de montaje, seleccione Añadir destino de montaje y añada las cuatro subredes privadas que creó.	
Compruebe que las subredes estén montadas como destinos.	1. En la consola de Amazon EFS, seleccione Sistemas de archivos. 2. Para ver la lista de objetivos de montaje existentes, seleccione Red. Asegúrese de que las cuatro subredes que creó estén incluidas.	Administrador de la nube

Creación de un bucket de S3

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Si es necesario, abra la consola de Amazon S3 y cree un bucket de S3 para almacenar los activos estáticos de la aplicación.	Administrador de la nube

Crear un secreto en Secrets Manager

Tarea	Descripción	Habilidades requeridas
Para cifrar el secreto de Secrets Manager, cree una clave de AWS KMS.	Abra la consola de AWS Key Management Service (AWS KMS) y cree una clave KMS.	Administrador de la nube
Cree un secreto de Secrets Manager para almacenar la contraseña de Amazon RDS.	1. Abra la consola de AWS Secrets Manager y cree un secreto nuevo. Para hacerlo, seleccione Almacenar un nuevo secreto. 2. Seleccione la clave de KMS que creó y guarde su nuevo secreto.	Administrador de la nube

Crear una instancia de Amazon RDS

Tarea	Descripción	Habilidades requeridas
Creación de un grupo de subredes de base de datos.	1. Abra la consola de Amazon RDS y seleccione Grupos de subred. 2. Seleccione Crear un grupo de subred de base de datos, e introduzca un nombre y una descripción para su grupo de subred de base de datos. 3. Seleccione la VPC que creó anteriormente y, a continuación, seleccione las zonas de disponibilidad y	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	las subredes. A continuación, seleccione Crear.	
Cree una instancia de Amazon RDS.	Cree y configure una instancia de Amazon RDS dentro de las subredes privadas. Asegúrese de que Multi-AZ esté activado para una alta disponibilidad.	Administrador de la nube
Cargue los datos en la instancia de Amazon RDS.	Cargue los datos relacionales que necesita la aplicación en la instancia de Amazon RDS. Este proceso variará según las necesidades de la aplicación y la forma en que se defina y diseñe el esquema de la base de datos.	Administrador de la nube, administrador de bases de datos

Crear los componentes de Amazon ECS

Tarea	Descripción	Habilidades requeridas
Cree un clúster de ECS.	1. Abra la consola de Amazon ECS y seleccione Clústeres. 2. Seleccione Crear clústeres y configure un clúster de ECS de acuerdo con las especificaciones requeridas.	Administrador de la nube
Cree las imágenes de Docker.	Cree las imágenes de Docker según las instrucciones de la sección Recursos relacionados.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Crear repositorios de Amazon ECR.	1. En la consola de Amazon ECR, seleccione Repositorios. 2. Seleccione Create repository (Crear repositorio) y especifique un nombre exclusivo para el repositorio. 3. Configure el repositorio de acuerdo con sus especificaciones, incluyendo el cifrado de AWS KMS si es necesario.	Administrador de nube, ingeniero DevOps
Autenticar su cliente Docker para el repositorio de Amazon ECR.	Para autenticar su cliente de Docker para el repositorio de Amazon ECR, ejecute el comando `aws ecr get-login-password` en la CLI de AWS.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Pase las imágenes de Docker al repositorio de Amazon ECR.	1. Identifique la imagen de Docker que quiere insertar y ejecute el comando `docker images` en la CLI de AWS. 2. Etiquete su imagen con la combinación de registro, repositorio y etiqueta de imagen opcional de Amazon ECR. 3. Ejecute el comando `docker push` para enviar la imagen de Docker. 4. Repita estos pasos para todas las imágenes requeridas.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree una definición de tarea de Amazon ECS.	Para ejecutar contenedores Docker en Amazon ECS, se requiere una definición de tareas. 1. Regrese a la consola de Amazon ECS, seleccione Definiciones de tareas y, a continuación, seleccione Crear nueva definición de tarea. 2. En la página Selección de compatibilidades, seleccione el tipo de lanzamiento que su tarea debe usar y, a continuación, seleccione Siguiente paso. **Important** Para obtener ayuda sobre la configuración de la definición de la tarea, consulte “Creación de una definición de tarea” en la sección Recursos relacionados. Asegúrese de proporcionar las imágenes de Docker que envió a Amazon ECR.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Creación de un servicio de Amazon ECS.	Cree un servicio de Amazon ECS mediante el clúster de ECS que creó anteriormente. Asegúrese de elegir Amazon EC2 como tipo de lanzamien to y de elegir la definición de tarea creada en el paso anterior, así como el grupo objetivo del Application Load Balancer.	Administrador de la nube

Crear un grupo de Amazon EC2 Auto Scaling

Tarea	Descripción	Habilidades requeridas
Cree una configuración de lanzamiento.	Abre la EC2 consola de Amazon y crea una configura ción de lanzamiento. Asegúrese de que los datos del usuario tengan el código que permita que las EC2 instancias se unan al clúster de ECS deseado. Para ver un ejemplo del código necesario , consulte la sección Recursos relacionados.	Administrador de la nube
Cree un grupo de Amazon EC2 Auto Scaling.	Regrese a la EC2 consola de Amazon y, en Auto Scaling, elija grupos de Auto Scaling. Configure un grupo de Amazon EC2 Auto Scaling. Asegúrese de elegir las subredes privadas y la	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	configuración de lanzamiento que creó anteriormente.	

Configurar AWS PrivateLink

Tarea	Descripción	Habilidades requeridas
Configure el PrivateLink punto de conexión de AWS.	1. En la consola de Amazon VPC, cree un punto de conexión de AWS PrivateLink . 2. Asocie este punto de conexión con el equilibrador de carga de red, lo que hará que la aplicación alojada en Amazon ECS esté disponible para los clientes de forma privada. Para obtener más información, consulte la sección Recursos relacionados.	Administrador de la nube

Crear un punto de conexión de VPC

Tarea	Descripción	Habilidades requeridas
Cree un punto de conexión de VPC.	Cree un punto de enlace de VPC para el punto de PrivateLink enlace de AWS que creó anteriormente. El nombre de dominio completo (FQDN) del punto final de la	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	VPC apuntará al FQDN del punto final de AWS PrivateLi nk . Esto crea una interfaz de red elástica para el servicio de puntos de conexión de VPC a la que pueden acceder los puntos de conexión de DNS.	

Crear la función de Lambda

Tarea	Descripción	Habilidades requeridas
Crear la función de Lambda.	En la consola de AWS Lambda, cree una función de Lambda para actualizar las direcciones IP del equilibra dor de carga de aplicación como destinos del equilibra dor de carga de red. Para más información sobre este tema, consulte la entrada en el blog Using AWS Lambda to enable static IP addresses for Application Load Balancers.	Desarrollador de aplicaciones

Recursos relacionados

Crear los equilibradores de carga:

- Utilice un Network Load Balancer para Amazon ECS
- Crear un equilibrador de carga de red
- Utilice un balanceador de carga de aplicaciones para Amazon ECS
- Creación de un equilibrador de carga de aplicación

Crear un sistema de archivos de Amazon EFS:

- Crear un sistema de archivos de Amazon EFS
- Crear destinos de montaje en Amazon EFS

Creación de un bucket de S3:

- Creación de un bucket de S3

Crear un secreto en Secrets Manager:

- Crear claves en AWS KMS
- Crear un secreto en AWS Secrets Manager

Crear una instancia de Amazon RDS:

- Crear una instancia de base de datos de Amazon RDS

Crear los componentes de Amazon ECS:

- Crear un clúster de Amazon ECS
- Crear una imagen de Docker
- Crear un repositorio de Amazon ECR
- Autenticar Docker con el repositorio de Amazon ECR
- Pasar una imagen a un repositorio de Amazon ECR
- Crear una definición de tarea de Amazon ECS
- Creación de un servicio de Amazon ECS

Cree un grupo de Amazon EC2 Auto Scaling:

- Crear una configuración de lanzamiento
- Crear un grupo de escalado automático mediante una configuración de lanzamiento
- Instancias de contenedores Bootstrap con datos de EC2 usuario de Amazon

Configure AWS PrivateLink:

- Servicios de puntos finales de VPC (AWS) PrivateLink

Crear un punto de conexión de VPC:

- Puntos de enlace de interfaz de VPC (AWS) PrivateLink

Crear la función de Lambda:

- Crear una función de Lambda

Otros recursos:

- Uso de direcciones IP estáticas para los equilibradores de carga de aplicación
- Acceso seguro a los servicios a través de AWS PrivateLink

Acceda a las aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS Fargate PrivateLink, AWS y un Network Load Balancer

Kirankumar Chandrashekar, Amazon Web Services

Resumen

Este patrón describe cómo alojar de forma privada una aplicación contenedora de Docker en la nube de Amazon Web Services (AWS) mediante Amazon Elastic Container Service (Amazon ECS) con un tipo de lanzamiento de AWS Fargate, detrás de un Network Load Balancer, y cómo acceder a la aplicación mediante AWS. PrivateLink Amazon Relational Database Service (Amazon RDS) aloja la base de datos relacional para la aplicación que se ejecuta en Amazon ECS con alta disponibilidad (HA). Puede utilizar Amazon Elastic File System (Amazon EFS) si la aplicación requiere almacenamiento permanente.

Este patrón utiliza un tipo de lanzamiento de Fargate para el servicio de Amazon ECS que ejecuta las aplicaciones de Docker, con un equilibrador de carga de red en el frontend. Luego, se puede asociar a un punto final de nube privada virtual (VPC) para acceder a través de AWS. PrivateLink Luego, este servicio de punto final de VPC se puede compartir con otros VPCs mediante sus puntos de enlace de VPC.

Puede usar Fargate con Amazon ECS para ejecutar contenedores sin tener que administrar servidores o clústeres de instancias de Amazon Elastic Compute Cloud EC2 (Amazon). También puede usar un grupo de Amazon EC2 Auto Scaling en lugar de Fargate. Para obtener más información, consulte Acceda a aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS PrivateLink y un Network Load Balancer.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2, instalada y configurada en Linux, macOS o Windows
- Docker, instalado y configurado en Linux, macOS o Windows
- Una aplicación que se ejecuta en Docker

Arquitectura

Pila de tecnología

- Amazon CloudWatch
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon ECS
- Amazon EFS
- Amazon RDS
- Amazon Simple Storage Service (Amazon S3)
- AWS Fargate
- AWS PrivateLink
- AWS Secrets Manager
- Equilibrador de carga de aplicación
- Equilibrador de carga de red
- VPC

Automatización y escala

- Puede usar AWS CloudFormation para crear este patrón mediante Infrastructure as Code.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor de AWS administrado que es seguro, escalable y fiable.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores altamente escalable y rápido que facilita la tarea de ejecutar, detener y administrar contenedores de Docker en un clúster.
- Amazon Elastic File System (Amazon EFS) ofrece un sistema de archivos NFS sencillo, escalable, elástico y completamente administrado que se utiliza con servicios de nube de AWS y recursos en las instalaciones.

- AWS Fargatees una tecnología que puede utilizar con Amazon ECS para ejecutar contenedores sin tener que gestionar servidores o clústeres de EC2 instancias de Amazon.
- Amazon Relational Database Service (Amazon RDS) es un servicio web que facilita la configuración, la operación y la escala de una base de datos relacional en Nube de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet. Está diseñado para facilitar a los desarrolladores recursos de computación escalables basados en Web.
- AWS Secrets Manager lo ayuda a reemplazar las credenciales codificadas en su código, incluidas contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido.
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos, como EC2 instancias, contenedores y direcciones IP, en varias zonas de disponibilidad.

Otras herramientas

- Docker facilita a los desarrolladores el proceso de empaquetar, enviar y ejecutar cualquier aplicación como un contenedor ligero, portátil y autosuficiente.

Epics

Creación de componentes de redes

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon VPC. Seleccione Crear VPC y, a continuac ión, VPC y más. 2. Especifique un nombre para su VPC y seleccione un	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	rango de bloques CIDR adecuado. 3. Especifique dos zonas de disponibilidad, dos subredes públicas y cuatro subredes privadas. Dos subredes privadas son para las tareas de Amazon ECS y otras dos subredes privadas son para las bases de datos de Amazon RDS. 4. Especifique una puerta de enlace NAT para cada zona de disponibilidad. 5. Seleccione Creación de VPC.	

Crear el equilibrador de carga

Tarea	Descripción	Habilidades requeridas
Crear un equilibrador de carga de red.	1. Abra la EC2 consola de Amazon y elija la región de AWS que contiene la VPC. 2. En Equilibrio de carga seleccione Equilibradores de carga y Crear equilibra dor de carga. 3. Seleccione Equilibrador de carga de red y luego Crear. 4. En la página Configurar el equilibrador de carga, configure el equilibrador de	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	carga de red y el oyente. Importante: Asegúrese de elegir el esquema del equilibrador de carga de red como interno. 5. Seleccione los ajustes de seguridad aplicable s, configure un grupo de seguridad y un grupo de destino. Seleccion e IP como Target type (Tipo de destino) en la sección Configure routing (Configurar enrutamiento). Asegúrese de no registrar un destino. 6. Una vez haya configurado todos los ajustes, seleccion e Siguiente: Revisar y, a continuación, seleccione Crear. Para obtener ayuda con esta y otras explicaciones, consulte la sección Recursos relaciona dos.	

Tarea	Descripción	Habilidades requeridas
Cree un Equilibrador de carga de aplicación.	1. En la EC2 consola de Amazon, elige la misma región que contiene tu VPC. 2. En Equilibrio de carga seleccione Equilibradores de carga y Crear equilibrador de carga. 3. Seleccione Application Load Balancer (Equilibrador de carga de aplicación) y, a continuación, Create. 4. **Important** Configure el equilibrador de carga de aplicación y el oyente. Asegúrese de elegir el esquema del equilibrador de carga de aplicación como interno. 5. Seleccione los ajustes de seguridad aplicables, configure un grupo de seguridad y un grupo de destino. Seleccione IP como Target type (Tipo de destino) en la sección Configure routing (Configurar enrutamiento).	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	Asegúrese de no registrar un destino. 6. Una vez haya configurado todos los ajustes, seleccione Siguiente: Revisar y, a continuación, seleccione Crear.	

Crear un sistema de archivos de Amazon EFS

Tarea	Descripción	Habilidades requeridas
Crear un sistema de archivos de Amazon EFS.	1. Abra la consola de Amazon EFS y seleccione Crear sistema de archivos. 2. En el cuadro de diálogo Crear sistema de archivos, especifique un nombre para su sistema de archivos y seleccione su VPC. 3. Seleccione Crear para crear el sistema de archivos. 4. Instale y configure su sistema de archivos de Amazon EFS.	Administrador de la nube
Defina el montaje de los destinos para las subredes.	1. Regrese a la consola de Amazon EFS y seleccione Sistemas de archivos. La página Sistemas de archivos muestra los sistemas de archivos Amazon EFS de su cuenta.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	2. Seleccione el sistema de archivos que creó y, a continuación, seleccione Manage (Administrar) para mostrar la zona de disponibilidad. 3. Para añadir un destino de montaje, seleccione Añadir destino de montaje y añada las cuatro subredes privadas que creó.	
Compruebe que las subredes estén montadas como destinos.	1. En la consola de Amazon EFS, seleccione Sistemas de archivos. 2. Para ver la lista de objetivos de montaje existentes, seleccione Red. Asegúrese de que las cuatro subredes que creó estén incluidas.	Administrador de la nube

Creación de un bucket de S3

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Si es necesario, abra la consola de Amazon S3 y cree un bucket de S3 para almacenar los activos estáticos de la aplicación.	Administrador de la nube

Crear un secreto en Secrets Manager

Tarea	Descripción	Habilidades requeridas
Para cifrar el secreto de Secrets Manager, cree una clave de AWS KMS.	Abra la consola de AWS Key Management Service (AWS KMS) y cree una clave KMS.	Administrador de la nube
Cree un secreto de Secrets Manager para almacenar la contraseña de Amazon RDS.	1. Abra la consola de AWS Secrets Manager y cree un secreto nuevo. Para hacerlo, seleccione Almacenar un nuevo secreto. 2. Seleccione la clave de KMS que creó y guarde su nuevo secreto.	Administrador de la nube

Crear una instancia de Amazon RDS

Tarea	Descripción	Habilidades requeridas
Creación de un grupo de subredes de base de datos.	1. Abra la consola de Amazon RDS y seleccione Subnet groups (Grupos de subred). 2. Seleccione Crear un grupo de subred de base de datos, e introduzca un nombre y una descripción para su grupo de subred de base de datos. 3. Seleccione la VPC que creó anteriormente y, a continuación, seleccione las zonas de disponibilidad y	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	las subredes. A continuación, seleccione Crear.	
Cree una instancia de Amazon RDS.	Cree y configure una instancia de Amazon RDS dentro de las subredes privadas. Asegúrese de que Multi-AZ esté activado, para una alta disponibilidad (HA).	Administrador de la nube
Cargue los datos en la instancia de Amazon RDS.	Cargue los datos relacionales que necesita la aplicación en la instancia de Amazon RDS. Este proceso variará según las necesidades de la aplicación y la forma en que se defina y diseñe el esquema de la base de datos.	Administrador de base de datos

Crear los componentes de Amazon ECS

Tarea	Descripción	Habilidades requeridas
Cree un clúster de ECS.	1. Abra la consola de Amazon ECS y seleccione Clústeres. 2. Seleccione Crear clústeres y configure un clúster de ECS de acuerdo con las especificaciones requeridas.	Administrador de la nube
Cree las imágenes de Docker.	Cree las imágenes de Docker siguiendo las instrucciones de la documentación de AWS.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree un repositorio de Amazon ECR.	1. Abra la consola de Amazon ECR y seleccione Repositories. 2. Seleccione Create repository (Crear repositorio) y especifique un nombre exclusivo para el repositorio. 3. Configure el repositorio de acuerdo con sus especificaciones, incluyendo el cifrado de AWS KMS si es necesario.	Administrador de nube, ingeniero DevOps
Pase las imágenes de Docker al repositorio de Amazon ECR.	1. Identifique la imagen de Docker que desea insertar y ejecute el comando `docker images` en la AWS CLI. 2. Etiquete su imagen con la combinación de registro, repositorio y etiqueta de imagen opcional de Amazon ECR. 3. Ejecute el comando `docker push` para enviar la imagen de Docker. 4. Repita estos pasos para todas las imágenes requeridas.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree una definición de tarea de Amazon ECS.	Para ejecutar contenedores Docker en Amazon ECS, se requiere una definición de tareas. 1. Regrese a la consola de Amazon ECS, seleccione Definiciones de tareas y, a continuación, seleccione Crear nueva definición de tarea. 2. En la página Selección de compatibilidades, seleccione el tipo de lanzamiento que su tarea debe usar y, a continuación, seleccione Siguiente paso. **Important** Para obtener ayuda sobre la configuración de la definición de la tarea, consulte “Creación de una definición de tarea” en la sección Recursos relacionados. Asegúrese de proporcionar las imágenes de Docker que envió a Amazon ECR.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree un servicio ECS y seleccione Fargate como tipo de lanzamiento.	1. Cree un servicio de Amazon ECS mediante el clúster de ECS que creó anteriormente. Asegúrese de seleccionar Fargate como tipo de lanzamiento. 2. Seleccione la definición de tarea creada en el paso anterior y, a continuación, el grupo objetivo del equilibra dor de carga de aplicación.	Administrador de la nube

Configuración de AWS PrivateLink

Tarea	Descripción	Habilidades requeridas
Configure el PrivateLink punto de conexión de AWS.	1. Abra la consola de Amazon VPC y cree un AWS PrivateLink punto final. 2. Asocie este punto de conexión con el equilibra dor de carga de red, lo que hará que la aplicació n alojada en Amazon ECS esté disponible para los clientes de forma privada.	Administrador de la nube

Crear un punto de conexión de VPC

Tarea	Descripción	Habilidades requeridas
Cree un punto de conexión de VPC.	Cree un punto de enlace de VPC para el punto de	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	PrivateLink enlace de AWS que creó anteriormente. El nombre de dominio completo (FQDN) del punto final de la VPC apuntará al FQDN del punto final de AWS PrivateLink . Esto crea una interfaz de red elástica para el servicio de punto de conexión de VPC a la que pueden acceder los puntos de conexión del servicio de nombres de dominio.	

Establecimiento del destino

Tarea	Descripción	Habilidades requeridas
Agregue el equilibrador de carga de aplicación como destino.	Para agregar el equilibrador de carga de aplicación como destino para el equilibrador de carga de red, siga las instrucciones de la documentación de AWS.	Desarrollador de aplicaciones

Recursos relacionados

Crear los equilibradores de carga:

- Utilice un Network Load Balancer para Amazon ECS
- Crear un equilibrador de carga de red
- Utilice un balanceador de carga de aplicaciones para Amazon ECS
- Creación de un equilibrador de carga de aplicación

Crear un sistema de archivos de Amazon EFS:

- Crear un sistema de archivos de Amazon EFS
- Crear destinos de montaje en Amazon EFS

Crear un secreto en Secrets Manager:

- Crear claves en AWS KMS
- Crear un secreto en AWS Secrets Manager

Crear una instancia de Amazon RDS:

- Crear una instancia de base de datos de Amazon RDS

Crear los componentes de Amazon ECS

- Crear un repositorio de Amazon ECR
- Autenticar Docker con el repositorio de Amazon ECR
- Pasar una imagen a un repositorio de Amazon ECR
- Crear una definición de tarea de Amazon ECS
- Creación de un servicio de Amazon ECS

Otros recursos:

- Acceso seguro a los servicios a través de AWS PrivateLink

Acceda a aplicaciones de contenedores de forma privada en Amazon EKS mediante AWS PrivateLink y un Network Load Balancer

Kirankumar Chandrashekar, Amazon Web Services

Resumen

Este patrón describe cómo alojar de forma privada una aplicación contenedora de Docker en Amazon Elastic Kubernetes Service (Amazon EKS) detrás de un Network Load Balancer y cómo acceder a la aplicación mediante AWS. PrivateLink A continuación, puede utilizar una red privada para acceder de forma segura a los servicios de la nube de Amazon Web Services (AWS).

El clúster de Amazon EKS que ejecuta las aplicaciones de Docker, con un Network Load Balancer en la interfaz, se puede asociar a un punto final de nube privada virtual (VPC) para acceder a él a través de AWS. PrivateLink Luego, este servicio de punto final de VPC se puede compartir con otros VPCs mediante sus puntos de enlace de VPC.

La configuración descrita en este patrón es una forma segura de compartir el acceso a las aplicaciones entre VPCs cuentas de AWS. No requiere configuraciones de enrutamiento ni conectividad especiales, ya que la conexión entre las cuentas del consumidor y del proveedor se encuentra en la red troncal global de AWS y no atraviesa la Internet pública.

Requisitos previos y limitaciones

Requisitos previos

- Docker, instalado y configurado en Linux, macOS o Windows.
- Una aplicación que se ejecuta en Docker.
- Una cuenta de AWS activa.
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2, instalada y configurada en Linux, macOS o Windows.
- Un clúster de Amazon EKS existente con subredes privadas etiquetadas y configurado para alojar aplicaciones. Para obtener más información, consulte Etiquetado de subredes en la documentación de Amazon EKS.
- Kubectl, instalado y configurado para acceder a los recursos de su clúster de Amazon EKS. Para más información, consulte Instalar kubectl en la documentación de Amazon EKS.

Arquitectura

Pila de tecnología

- Amazon EKS
- AWS PrivateLink
- Equilibrador de carga de red

Automatización y escala

- Los manifiestos de Kubernetes se pueden rastrear y administrar en un repositorio basado en Git, y se pueden implementar mediante la integración y entrega continuas (CI/CD) en AWS. CodePipeline
- Puede usar AWS CloudFormation para crear este patrón mediante la infraestructura como código (IaC).

Tools (Herramientas)

- AWS CLI: la interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.
- Elastic Load Balancing: Elastic Load Balancing distribuye el tráfico entrante de aplicaciones o redes entre varios destinos, como instancias, contenedores y direcciones IP de Amazon Elastic Compute Cloud (Amazon EC2), en una o más zonas de disponibilidad.

- Amazon EKS: Amazon Elastic Kubernetes Service (Amazon EKS) es un servicio administrado que puede utilizar para ejecutar Kubernetes en AWS sin necesidad de instalar, operar ni mantener su propio plano de control o nodos de Kubernetes.
- Amazon VPC: Amazon Virtual Private Cloud (Amazon VPC) permite lanzar recursos de AWS en una red virtual previamente definida.
- Kubectl – Kubectl es una utilidad de línea de comandos para ejecutar comandos en clústeres de Kubernetes.

Epics

Implementar los archivos de manifiesto de implementación y servicio de Kubernetes

Tarea	Descripción	Habilidades requeridas

Cree el archivo de manifiesto de implementación de Kubernetes.	Cree un archivo de manifiesto de implementación modificando el siguiente archivo de muestra según sus necesidades.
	
	`apiVersion: apps/v1`
	`kind: Deployment`
	`metadata:`
	`  name: sample-app`
	`spec:`
	`  replicas: 3`
	`  selector:`
	`  matchLabels:`
	`  app: nginx`
	`  template:`
	`  metadata:`
	`  labels:`
	`  app: nginx`
	`  spec:`
	`  containers:`
	`  - name: nginx`
	`  image: public.ecr.aws/z9d2n7e1/nginx:1.19.5`
	`  ports:`
	`  - name: http`
	`  containerPort: 80`
	
	Note
	Esta es una muestra de archivo de configuración de
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	NGINX que se implementa mediante la imagen de Docker de NGINX. Para obtener más información, consulte Cómo usar la imagen de Docker de NGINX en la documentación de Docker.	
Implemente el archivo de manifiesto de implementación de Kubernetes.	Ejecute el siguiente comando para aplicar el archivo de manifiesto de implementación a su clúster de Amazon EKS: `kubectl apply -f <your_deployment_file_name>`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Cree el archivo de manifiesto del servicio de Kubernetes.	Cree un archivo de manifiesto de servicio modificando el siguiente archivo de muestra según sus necesidades.
	
	`apiVersion: v1`
	`kind: Service`
	`metadata:`
	`  name: sample-service`
	`  annotations:`
	`  service.beta.kubernetes.io/aws-load-balancer-type: nlb`
	`  service.beta.kubernetes.io/aws-load-balancer-internal: "true"`
	`spec:`
	`  ports:`
	`  - port: 80`
	`  targetPort: 80`
	`  protocol: TCP`
	`  type: LoadBalancer`
	`  selector:`
	`  app: nginx`
	
	Important
	Asegúrese de incluir las siguientes `annotations` para definir un equilibrador de carga de red interno:
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`service.beta.kubernetes.io/aws-load-balancer-type: nlb` `service.beta.kubernetes.io/aws-load-balancer-internal: "true"`	
Implemente el archivo de manifiesto del servicio de Kubernetes.	Ejecute el siguiente comando para aplicar el archivo de manifiesto de servicio a su clúster de Amazon EKS: `kubectl apply -f <your_service_file_name>`	DevOps ingeniero

Creación de los puntos de conexión

Tarea	Descripción	Habilidades requeridas
Registre el nombre del equilibrador de carga de red.	Ejecute el siguiente comando para recuperar el nombre del equilibrador de carga de red: `kubectl get svc sample-service -o wide` Registre el nombre del balanceador de carga de red, que es necesario para crear un PrivateLink punto de conexión de AWS.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Cree un PrivateLink punto de conexión de AWS.	Inicie sesión en la consola de administración de AWS, abra la consola de Amazon VPC y, a continuación, cree un punto de conexión de AWS PrivateLink . Al asociar este punto de conexión al equilibrador de carga de red, la aplicación estará disponible de forma privada para los clientes. Para obtener más información, consulte los servicios de punto final de VPC PrivateLink (AWS) en la documentación de Amazon VPC. **Important** Si la cuenta del consumidor requiere acceso a la aplicación, el ID de cuenta de AWS de la cuenta del consumidor debe añadirse a la lista de principales permitidos para la configuración del PrivateLink punto de conexión de AWS. Para obtener más información, consulte Cómo añadir y eliminar permisos para el servicio de puntos de conexión en	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	la documentación de Amazon VPC.	
Cree un punto de conexión de VPC.	En la consola de Amazon VPC, elija Endpoint Services y, a continuación, elija Create Endpoint Service. Cree un punto de enlace de VPC para el punto de enlace de AWS PrivateLink . El nombre de dominio completo (FQDN) del punto de enlace de VPC apunta al FQDN del punto de enlace de AWS. PrivateLink Esto crea una interfaz de red elástica para el servicio de puntos de conexión de VPC a la que pueden acceder los puntos de conexión de DNS.	Administrador de la nube

Recursos relacionados

- Uso de la imagen de Docker NGINX oficial
- Equilibrio de carga de red en Amazon EKS
- Creación de servicios de punto final de VPC (AWS) PrivateLink
- Cómo agregar y eliminar permisos para el servicio de punto de conexión

Automatizar las copias de seguridad de las instancias de base de datos de Amazon RDS para PostgreSQL mediante AWS Batch

Kirankumar Chandrashekar, Amazon Web Services

Resumen

Realizar copias de seguridad de las bases de datos de PostgreSQL es una tarea importante que, por lo general, se puede obtener mediante el programa de utilidad pg_dump, que usa el comando COPY de forma predeterminada para crear un esquema y un volcado de datos de una base de datos de PostgreSQL. Sin embargo, este proceso puede resultar repetitivo si necesita copias de seguridad periódicas de varias bases de datos de PostgreSQL. Si las bases de datos PostgreSQL están alojadas en la nube, también puede aprovechar la función automated backup de copia de seguridad automática que ofrece Amazon Relational Database Service (Amazon RDS) para PostgreSQL. Este patrón describe cómo automatizar las copias de seguridad periódicas de las instancias de base de datos de Amazon RDS para PostgreSQL mediante el programa de utilidad pg_dump.

Nota: En las instrucciones se parte del supuesto de que utiliza Amazon RDS. Sin embargo, también puede utilizar este enfoque para bases de datos PostgreSQL alojadas fuera de Amazon RDS. Para realizar copias de seguridad, la función de AWS Lambda debe poder acceder a las bases de datos.

Un evento de Amazon CloudWatch Events basado en el tiempo inicia una función Lambda que busca etiquetas de respaldo específicas aplicadas a los metadatos de las instancias de base de datos de PostgreSQL en Amazon RDS. Si las instancias de base de datos PostgreSQL tienen la etiqueta DBDump bkp:Automated = Active y otras etiquetas de backup obligatorias, la función Lambda envía los trabajos individuales para cada copia de seguridad de la base de datos a AWS Batch.

AWS Batch procesa estos trabajos y carga los datos de copia de seguridad en un bucket de Amazon Simple Storage Service (Amazon S3). En este patrón se utiliza un Dockerfile y un archivo entrypoint.sh para crear una imagen de contenedor de Docker que se usa para realizar copias de seguridad en el trabajo de AWS Batch. Una vez finalizado el proceso de copia de seguridad, AWS Batch registra los detalles de la copia de seguridad en una tabla de inventario de Amazon DynamoDB. Como medida de seguridad adicional, un evento de CloudWatch eventos inicia una notificación de Amazon Simple Notification Service (Amazon SNS) si un trabajo falla en AWS Batch.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.

- Un entorno informático existente, administrado o no administrado. Para obtener más información, consulte Entornos informáticos administrados y no administrados en la documentación de AWS Batch.
- Imagen de Docker de la Interfaz de la línea de comandos (CLI) de AWS, versión 2, instalada y configurada.
- Instancias de base de datos de Amazon RDS para PostgreSQL existentes.
- Un bucket de S3 existente.
- Docker, instalado y configurado en Linux, macOS o Windows.
- Familiaridad con la codificación en Lambda.

Arquitectura

Pila de tecnología

- CloudWatch Eventos de Amazon
- Amazon DynamoDB
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon RDS
- Amazon SNS
- Amazon S3
- AWS Batch
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- AWS Secrets Manager
- Docker

Tools (Herramientas)

- Amazon CloudWatch Events — CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS.
- Amazon DynamoDB: DynamoDB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido y predecible, así como una perfecta escalabilidad.

- Amazon ECR: Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor de AWS administrado que es seguro, escalable y fiable.
- Amazon RDS: Amazon Relational Database Service (Amazon RDS) es un servicio web que facilita la configuración, el funcionamiento y el escalado de una base de datos relacional en la nube de AWS.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio administrado que proporciona la entrega de mensajes de los publicadores a los suscriptores.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet.
- AWS Batch: AWS Batch facilita poder ejecutar cargas de trabajo informáticas por lotes en la nube de AWS.
- AWS KMS – AWS Key Management Service (AWS KMS) es un servicio administrado que permite crear y controlar fácilmente las claves de cifrado que se utilizan para cifrar datos.
- AWS Lambda: Lambda es un servicio informático que facilita poder ejecutar código sin aprovisionar ni administrar servidores.
- AWS Secrets Manager: Secrets Manager le permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- Docker: Docker facilita a los desarrolladores empaquetar, enviar y ejecutar cualquier aplicación como un contenedor ligero, portátil y autosuficiente.

Las instancias de base de datos de PostgreSQL en Amazon RDS deben tener etiquetas aplicadas a sus metadatos. La función de Lambda busca etiquetas para identificar las instancias de base de datos de las que se debe hacer una copia de seguridad y, por lo general, se utilizan las siguientes etiquetas.

Etiqueta	Description (Descripción)
BKP: Automatizado = Activo DBDump	Identifica una instancia de base de datos de Amazon RDS como candidata para realizar copia de seguridad.
bkp: = AutomatedBackupSecret <secret_name>	Identifica el secreto de Secrets Manager que contiene las credenciales de inicio de sesión de Amazon RDS.

BKP: Cubeta S3 DBDump automatizada = <s3_bucket_name>	Identifica el bucket de S3 al que se enviarán las copias de seguridad.
BKP: DBDump Frecuencia automatizada BKP: Tiempo DBDump automatizado	Identifica la frecuencia y las horas en las que se deben hacer copias de seguridad de las bases de datos.
bkp:pgdumpcommand = <pgdump_command>	Identifica las bases de datos para las que se deben realizar las copias de seguridad.

Epics

Crear una tabla de inventario en DynamoDB

Tarea	Descripción	Habilidades requeridas
Cree una tabla en DynamoDB.	Inicie sesión en la Consola de administración de AWS, abra la consola de Amazon DynamoDB y cree una tabla. Para obtener ayuda con esta y otras explicaciones, consulte la sección Recursos relacionados.	Administrador de la nube, administrador de bases de datos
Confirme que se creó la tabla.	Ejecute el comando `aws dynamodb describe-table --table-name <table-name> | grep TableStatus` . Si la tabla existe, el comando devolverá el resultado `"TableStatus": "ACTIVE",` .	Administrador de la nube, administrador de bases de datos

Creación de un tema de SNS para los eventos de trabajo con errores en AWS Batch

Tarea	Descripción	Habilidades requeridas
Cree un tema de SNS.	Abra la consola de Amazon SNS, seleccione Topics (Temas) y cree un tema de SNS con el nombre `JobFailedAlert` . Suscríbase al tema con una dirección de correo electrónico activa y compruebe su bandeja de entrada para confirmar que llegue el correo electrónico de suscripción a SNS de AWS Notifications.	Administrador de la nube
Cree una regla de eventos de trabajo con errores para AWS Batch.	Abre la CloudWatch consola de Amazon, selecciona Eventos y, a continuación, selecciona Crear regla. Seleccione Show advanced options (Mostrar opciones avanzadas) y, a continuación, Edit (Editar). En Build a pattern that selects events for processing by your targets (Crear un patrón que seleccione eventos para procesar por los destinos) , sustituya el texto que aparezca con el código Failed job event (Evento de trabajo con errores) de la sección Información adicional. Este código define una regla de CloudWatch eventos que se	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	inicia cuando AWS Batch tiene un `Failed` evento.	
Agregue el destino de la regla del evento.	En Targets (Destinos), seleccione Add target (Agregar destino) y, a continuación, el tema de SNS `JobFailedAlert` . Configure los detalles restantes y cree la regla de eventos de Cloudwatch.	Administrador de la nube

Crear una imagen de Docker y pasarla a un repositorio de Amazon ECR

Tarea	Descripción	Habilidades requeridas
Cree un repositorio de Amazon ECR.	Abra la consola de Amazon ECR y seleccione la región de AWS donde desee crear el repositorio. Seleccione Repositories (Repositorios) y, a continuación, Create repository (Crear repositorio). Configure el repositorio según los requisitos.	Administrador de la nube
Cree un Dockerfile.	Inicie sesión en Docker y utilice Sample Dockerfile (Dockerfile de muestra) y el archivo entrypoint.sh de muestra de la sección de Información adicional para crear un Dockerfile.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Cree una imagen de Docker y pásela a un repositorio de Amazon ECR.	Cree el Dockerfile en una imagen de Docker y pásela a un repositorio de Amazon ECR. Para obtener ayuda con esta y otras explicaciones, consulte la sección Recursos relacionados.	DevOps ingeniero

Crear los componentes de AWS Batch

Tarea	Descripción	Habilidades requeridas
Cree una definición de trabajo de AWS Batch.	Abra la consola de AWS Batch y cree una definició n de trabajo que incluya el identificador uniforme de recursos (URI) del repositor io de Amazon ECR como la propiedad `Image`.	Administrador de la nube
Configure la cola de trabajos de AWS Batch.	En la consola de AWS Batch, seleccione Job queues (Colas de trabajos) y, a continuación, Create queue (Crear cola). Cree una cola de trabajos que almacene los trabajos hasta que AWS Batch los ejecute en los recursos del entorno informático. Important e: Asegúrese de escribir la lógica para que AWS Batch registre los detalles de la copia de seguridad en la tabla de inventario de DynamoDB.	Administrador de la nube

Crear y programar una función de Lambda

Tarea	Descripción	Habilidades requeridas
Cree una función de Lambda para buscar etiquetas.	Cree una función de Lambda que busque etiquetas en las instancias de base de datos de PostgreSQL e identifiq ue los candidatos a copia de seguridad. Asegúrese de que la función de Lambda pueda identificar la etiqueta `bkp:AutomatedDBDum p = Active` y todas las demás etiquetas necesaria s. Importante: La función de Lambda también debe poder agregar trabajos a la cola de trabajo de AWS Batch.	DevOps ingeniero
Crea un evento de CloudWatc h eventos basado en el tiempo.	Abra la CloudWatch consola de Amazon y cree un evento CloudWatch Events que utilice una expresión cron para ejecutar la función Lambda de forma regular. Importante: Todos los eventos programad os utilizan la zona horaria UTC.	Administrador de la nube

Probar la automatización de las copias de seguridad

Tarea	Descripción	Habilidades requeridas
Cree una clave de Amazon KMS.	Abra la consola de Amazon KMS y cree una clave de KMS	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	que pueda usarse para cifrar las credenciales de Amazon RDS almacenadas en AWS Secrets Manager.	
Crear un secreto de AWS Secrets Manager.	Abra la consola de AWS Secrets Manager y guarde en secreto las credenciales de la base de datos de Amazon RDS para PostgreSQL.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Agregue las etiquetas necesarias a las instancias de base de datos de PostgreSQL.	**Important** Abra la consola de Amazon RDS y agregue etiquetas a las instancias de base de datos de PostgreSQL de las que desee hacer una copia de seguridad automática. Puede utilizar las etiquetas de la tabla de la sección Tools (Herramientas). Si necesita copias de seguridad de varias bases de datos de PostgreSQL dentro de la misma instancia de Amazon RDS, utilice `-d test:-d test1` como valor para la etiqueta `bkp:pgdum pcommand .test` y `test1` son los nombres de las bases de datos. Compruebe que no quede ningún espacio después de los dos puntos (:).	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Verifique la automatización de la copia de seguridad.	Para verificar la automatización de la copia de seguridad, puede invocar la función de Lambda o esperar a que comience la programación de la copia de seguridad. Una vez finalizado el proceso de copia de seguridad, compruebe que la tabla de inventario de DynamoDB tenga una entrada de copia de seguridad válida para las instancias de base de datos de PostgreSQL. Si coinciden, el proceso de automatización de la copia de seguridad se ha realizado correctamente.	Administrador de la nube

Recursos relacionados

Crear una tabla de inventario en DynamoDB

- Crear una tabla de Amazon DynamoDB

Creación de un tema de SNS para los eventos de trabajo con errores en AWS Batch

- Crear un tema de Amazon SNS
- Enviar alertas de SNS sobre eventos de trabajo con errores en AWS Batch

Crear una imagen de Docker y pasarla a un repositorio de Amazon ECR

- Crear un repositorio de Amazon ECR
- Escribir un Dockerfile, crear una imagen de Docker y pasarla a Amazon ECR

Crear los componentes de AWS Batch

- Crear una definición de trabajo de AWS Batch
- Configurar el entorno informático y la cola de trabajos de AWS Batch
- Crear una cola de trabajos en AWS Batch

Crear una función de Lambda

- Crear una función de Lambda y escribir código
- Usar Lambda con DynamoDB

Cree un evento de eventos CloudWatch

- Crea un evento de CloudWatch eventos basado en el tiempo
- Utilizar expresiones cron en eventos de Cloudwatch

Probar la automatización de las copias de seguridad

- Crear una clave de Amazon KMS
- Crear un secreto en Secrets Manager
- Agregar etiquetas a una instancia de Amazon RDS

Información adicional

Evento de trabajo con errores:

```
{
  "detail-type": [
    "Batch Job State Change"
  ],
  "source": [
    "aws.batch"
  ],
  "detail": {
    "status": [
      "FAILED"
    ]
  }
}
```

Dockerfile de muestra:

```
FROM alpine:latest
RUN apk --update add py-pip postgresql-client jq bash && \
pip install awscli && \
rm -rf /var/cache/apk/*
ADD entrypoint.sh /usr/bin/
RUN chmod +x /usr/bin/entrypoint.sh
ENTRYPOINT ["entrypoint.sh"]
```

Archivo entrypoint.sh de muestra:

```
 #!/bin/bash
set -e
DATETIME=`date +"%Y-%m-%d_%H_%M"`
FILENAME=RDS_PostGres_dump_${RDS_INSTANCE_NAME}
FILE=${FILENAME}_${DATETIME}

aws configure --profile new-profile set role_arn arn:aws:iam::${TargetAccountId}:role/
${TargetAccountRoleName}
aws configure --profile new-profile set credential_source EcsContainer

echo "Central Account access provider IAM role is: "
aws sts get-caller-identity

echo "Target Customer Account access provider IAM role is: "
aws sts get-caller-identity --profile new-profile
```

```
securestring=$(aws secretsmanager get-secret-value --secret-id $SECRETID --output json
 --query 'SecretString' --region=$REGION --profile new-profile)

if [[ ${securestring} ]]; then
    echo "successfully accessed secrets manager and got the credentials"
    export PGPASSWORD=$(echo $securestring | jq --raw-output | jq -r '.DB_PASSWORD')
    PGSQL_USER=$(echo $securestring | jq --raw-output | jq -r '.DB_USERNAME')
    echo "Executing pg_dump for the PostGres endpoint ${PGSQL_HOST}"
    # pg_dump -h $PGSQL_HOST -U $PGSQL_USER -n dms_sample | gzip -9 -c  | aws s3 cp -
 --region=$REGION  --profile new-profile s3://$BUCKET/$FILE
    # in="-n public:-n private"
    IFS=':' list=($EXECUTE_COMMAND);
    for command in "${list[@]}";
      do
        echo $command;
        pg_dump -h $PGSQL_HOST -U $PGSQL_USER ${command} | gzip -9 -c  | aws s3 cp - --
region=$REGION --profile new-profile s3://${BUCKET}/${FILE}-${command}".sql.gz"
        echo $?;
        if  [[ $? -ne 0 ]]; then
            echo "Error occurred in database backup process. Exiting now....."
            exit 1
        else
            echo "Postgresql dump was successfully taken for the RDS endpoint
 ${PGSQL_HOST} and is uploaded to the following S3 location s3://${BUCKET}/${FILE}-
${command}.sql.gz"
            #write the details into the inventory table in central account
            echo "Writing to DynamoDB inventory table"
            aws dynamodb put-item --table-name ${RDS_POSTGRES_DUMP_INVENTORY_TABLE} --
region=$REGION --item '{ "accountId": { "S": "'"${TargetAccountId}"'" }, "dumpFileUrl":
 {"S": "'"s3://${BUCKET}/${FILE}-${command}.sql.gz"'" }, "DumpAvailableTime": {"S":
 "'"`date +"%Y-%m-%d::%H::%M::%S"` UTC"'"}}'
            echo $?
            if  [[ $? -ne 0 ]]; then
                echo "Error occurred while putting item to DynamoDb Inventory Table.
 Exiting now....."
                exit 1
            else
                echo "Successfully written to DynamoDb Inventory Table
 ${RDS_POSTGRES_DUMP_INVENTORY_TABLE}"
            fi
        fi
      done;
else
    echo "Something went wrong {$?}"
```

```
    exit 1
fi

exec "$@"
```

Automatice la implementación del controlador de terminación de nodos en Amazon EKS mediante una CI/CD canalización

Sandip Gangapadhyay, Sandeep Gawande, Viyoma Sachdeva, Pragtideep Singh y John Vargas, Amazon Web Services

Resumen

Aviso: AWS ya no CodeCommit está disponible para nuevos clientes. Los clientes actuales de AWS CodeCommit pueden seguir utilizando el servicio con normalidad. Más información

En la nube de Amazon Web Services (AWS), puede utilizar AWS Node Termination Handler, un proyecto de código abierto, para gestionar el cierre de instancias de Amazon Elastic Compute Cloud EC2 (Amazon) en Kubernetes sin problemas. El controlador de terminaciones de nodos de AWS ayuda a garantizar que el plano de control de Kubernetes responda adecuadamente a los eventos que pueden provocar que la EC2 instancia deje de estar disponible. Dichos eventos incluyen lo siguiente:

- EC2 mantenimiento programado de la instancia
- Interrupciones de Amazon EC2 Spot Instance
- El grupo de escalado automático se reduce horizontalmente
- Reequilibrio de grupos de escalado automático en todas las zonas de disponibilidad
- EC2 terminación de instancias a través de la API o la consola de administración de AWS

Si no se gestiona un evento, es posible que el código de su aplicación no se detenga correctamente. También puede tardar más en recuperar la disponibilidad total o programar accidentalmente el trabajo en los nodos que están dejando de funcionar. El (NTH) `aws-node-termination-handler` puede funcionar en dos modos diferentes: servicio de metadatos de instancias (IMDS) o procesador de colas. Para obtener más información acerca de los dos modos, consulte el archivo Léame.

Este patrón utiliza AWS CodeCommit y automatiza la implementación de NTH mediante el uso de Queue Processor mediante un proceso de integración y entrega continuas (CI/CD).

> **Note**
>
> Si utiliza grupos de nodos gestionados por EKS, no necesita `aws-node-termination-handler`.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un navegador web compatible para su uso con la consola de administración de AWS. Consulte la lista de los navegadores compatibles.
- AWS Cloud Development Kit (AWS CDK), instalado.
- `kubectl`, la herramienta de línea de comandos de Kubernetes, instalada.
- `eksctl`, la interfaz de la línea de comandos de AWS (AWS CLI) para Amazon Elastic Kubernetes Service (Amazon EKS), instalada.
- Un clúster de EKS en ejecución con la versión 1.20 o posterior.
- Grupo de nodos autogestionados adjunto al clúster de EKS. Para crear un clúster de Amazon EKS con un grupo de nodos autogestionado, ejecute el siguiente comando.

```
eksctl create cluster --managed=false --region <region> --name <cluster_name>
```

  Para obtener más información sobre `eksctl`, consulte la documentación de eksctl.
- Proveedor de OpenID Connect (OIDC) de AWS Identity and Access Management (IAM) para su clúster. Para obtener más información, consulte Creación de un proveedor OIDC de IAM para su clúster.

Limitaciones

- Debe utilizar una región de AWS que sea compatible con el servicio Amazon EKS.

Versiones de producto

- Versión de Kubernetes 1.20 o posterior
- `eksctl` versión 0.107.0 o posterior
- CDK de AWS, versión 2.27.0 o posterior

Arquitectura

Pila de tecnología de destino

- Una nube privada virtual (VPC)
- Un Clúster de EKS
- Amazon Simple Queue Service (Amazon SQS)
- IAM
- Kubernetes

Arquitectura de destino

El siguiente diagrama muestra una vista de alto nivel de los end-to-end pasos que se deben seguir cuando se inicia la terminación del nodo.

El flujo de trabajo que se muestra en el diagrama consta de los siguientes pasos de alto nivel:

1. El evento de finalización de la EC2 instancia de escalado automático se envía a la cola de SQS.
2. El NTH Pod supervisa los mensajes nuevos en la cola de SQS.
3. El NTH Pod recibe el nuevo mensaje y hace lo siguiente:
   - Acordona el nodo para que el nuevo pod no se ejecute en él.
   - Drena el nodo para evacuar el pod existente
   - Envía una señal de enlace de ciclo de vida al grupo de escalado automático para que se pueda terminar el nodo.

Automatizar y escalar

- El código lo administra e implementa AWS CDK, con el respaldo de pilas CloudFormation anidadas de AWS.
- El plano de control de Amazon EKS se ejecuta en varias zonas de disponibilidad para garantizar una alta disponibilidad.
- Para el escalado automático, Amazon EKS admite el escalador automático de clústeres de Kubernetes y Karpenter.

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS le CodePipeline ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.
- Amazon Elastic Kubernetes Service (Amazon EKS) lo ayuda a ejecutar Kubernetes en AWS sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.
- Amazon EC2 Auto Scaling le ayuda a mantener la disponibilidad de las aplicaciones y le permite añadir o eliminar automáticamente EC2 instancias de Amazon según las condiciones que defina.
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.

Otras herramientas

- kubectl: es una herramienta de línea de comandos para la ejecución de comandos en clústeres de Kubernetes. Puede usar kubectl para implementar aplicaciones, inspeccionar y administrar los recursos del clúster y ver los registros.

Código

El código de este patrón está disponible en el deploy-nth-to-eksrepositorio de GitHub .com. El repositorio de código contiene los siguientes archivos y carpetas.

- `nth folder`— El diagrama de Helm, los archivos de valores y los scripts para escanear e implementar la CloudFormation plantilla de AWS para Node Termination Handler.
- `config/config.json`: el archivo de parámetros de configuración de la aplicación. Este archivo contiene todos los parámetros necesarios para implementar el CDK.
- `cdk`: el código fuente del CDK de AWS.
- `setup.sh`— El script utilizado para implementar la aplicación AWS CDK para crear la CI/CD canalización requerida y otros recursos necesarios.

- `uninstall.sh`: el script utilizado para limpiar los recursos.

Para usar el código de muestra, siga las instrucciones en la sección Epics .

Prácticas recomendadas

Para conocer las prácticas recomendadas a la hora de automatizar AWS Node Termination Handler, consulte lo siguiente:

- Guías de prácticas recomendadas de EKS
- Node Termination Handler: configuración

Epics

Configure su entorno

Tarea	Descripción	Habilidades requeridas

Clone el repositorio.	Para clonar el repositorio mediante SSH (Secure Shell), ejecute el siguiente comando.
	`git clone git@github.com:aws-samples/deploy-nth-to-eks.git`
	Para clonar el repositorio mediante HTTPS, ejecute el siguiente comando.
	`git clone https://github.com/aws-samples/deploy-nth-to-eks.git`
	Al clonar el repositorio se crea una carpeta llamada `deploy-nth-to-eks` .
		Desarrollador de aplicaciones, AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Cambie a ese directorio. `cd deploy-nth-to-eks`	
Configure el archivo kubeconfig.	Configure sus credenciales de AWS en su terminal y confirme que tiene derechos para asumir el rol de clúster. Puede utilizar el siguiente código de ejemplo. `aws eks update-kubeconfig --name <Cluster_Name> --region <region>--role-arn <Role_ARN>`	AWS DevOps, DevOps ingeniero, desarrollador de aplicaciones

Implemente la CI/CD canalización

Tarea	Descripción	Habilidades requeridas
Establezca los parámetros.	Configure los siguientes parámetros obligatorios en el archivo `config/config.json` . • `pipelineName` : el nombre de la CI/CD canalización que va a crear AWS CDK (por ejemplo,`deploy-nth-to-eks-pipeline`). AWS CodePipeline creará una canalización con este nombre.	Desarrollador de aplicaciones, AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• `repositoryName` : El CodeCommit repositorio de AWS que se va a crear (por ejemplo,`deploy-nth-to-eks-repo`). AWS CDK creará este repositorio y lo establecerá como la fuente de la canalización. CI/CD **Note** Esta solución creará este CodeCommit repositorio y la rama (proporcionados en el siguiente parámetro de rama). • `branch`: el nombre de rama del repositorio (por ejemplo, `main`). Si se confirma con esta rama, se iniciará la CI/CD canalización. • `cfn_scan_script` : la ruta del script que se utilizará para escanear la CloudFormation plantilla de AWS en busca de NTH (`scan.sh`). Este script existe en `nth` una carpeta que formará parte del CodeCommit repositorio de AWS.	

Tarea	Descripción	Habilidades requeridas
	• `cfn_deploy_scrip t`: la ruta del script que se utilizará para implement ar la CloudFormation plantilla de AWS para NTH (`installApp.sh`). • `stackName` : El nombre de la CloudFormation pila que se va a implementar. • `eksClusterName` : el nombre del clúster de EKS existente. • `eksClusterRole` : el rol de IAM que se utilizará para acceder al clúster de EKS para todas las llamadas a la API de Kubernetes (por ejemplo, `clusterad min`). Por lo general, este rol se agrega en `aws-auth ConfigMap` . • `create_cluster_rol e` : para crear el rol de IAM `eksClusterRole` , escriba sí. Si desea proporcionar un rol de clúster existente en el parámetro `eksCluste rRole` , escriba no. • `create_iam_oidc_pr ovider` : para crear un proveedor de OIDC de IAM para su clúster, escriba sí. Si ya existe un proveedor	

Tarea	Descripción	Habilidades requeridas
	de IAM OIDC, escriba no. Para obtener más información, consulte Creación de un proveedor OIDC de IAM para su clúster. • `AsgGroupName` : una lista separada por comas de los nombres de los grupos de escalado automático que forman parte del clúster de EKS (por ejemplo, `ASG_Group_1,ASG_Group_2`). • `region`: el nombre de la región de AWS donde se encuentra el clúster (por ejemplo, `us-east-2`). • `install_cdk` : si el CDK de AWS no está instalado actualmente en el equipo, escriba sí. Ejecute el comando `cdk --version` para comprobar si la versión del CDK de AWS instalada es 2.27.0 o posterior. En ese caso, escriba no. Si escribe sí, el script setup.sh ejecutará el comando `sudo npm install -g cdk@2.27.0` para instalar el CDK de AWS en el equipo. El script	

Tarea	Descripción	Habilidades requeridas
	requiere permisos sudo, por lo que debe proporcionar la contraseña de la cuenta cuando se le solicite.	
Cree la CI/CD canalización para implementar NTH.	Ejecute el script setup.sh. `./setup.sh` El script implementará la aplicación AWS CDK que creará el CodeCommit repositorio con el código de ejemplo, la canalización y los CodeBuild proyectos en función de los parámetros ingresados por el usuario en `config/config.json` el archivo. Este script solicitará la contraseña cuando instale los paquetes npm con el comando sudo.	Desarrollador de aplicaciones, AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Revise la CI/CD canalización.	Abra la consola de administración de AWS y revise los siguientes recursos creados en la pila. • CodeCommit repositorio con el contenido de la carpeta `nth` • CodeBuild Proyecto AWS`cfn-scan`, que escaneará la CloudFormation plantilla en busca de vulnerabilidades. • CodeBuild proyecto`Nth-Deploy` , que implementará la CloudFormation plantilla de AWS y los gráficos de NTH Helm correspondientes a través de la CodePipeline canalización de AWS. • Una CodePipeline canalización para implementar NTH. Una vez que la canalización se ejecute correctamente, la versión de Helm `aws-node-termination-handler` se instala en el clúster de EKS. Además, se está ejecutando un pod denominado `aws-node-termination-handler` en el espacio	Desarrollador de aplicaciones, AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	de nombres `kube-system` del clúster.	

Pruebe la implementación de NTH

Tarea	Descripción	Habilidades requeridas
Simule un evento de escalado de grupo de escalado automático.	Para simular un evento de reducción horizontal del escalado automático, haga lo siguiente: 1. En la consola de AWS, abra la EC2 consola y elija Auto Scaling Groups. 2. Seleccione el grupo de escalado automático que tenga el mismo nombre que el proporcionado en `config/config.json` y elija Editar. 3. Reduzca la capacidad deseada y mínima en 1. 4. Elija Actualizar.	
Revise los registros.	Durante el evento de escalado, el NTH Pod acordonará y vaciará el nodo de trabajo correspondiente (la EC2 instancia que finalizará como parte del evento de escalado). Para comprobar los registros, utilice el código de la sección Información adicional.	Desarrollador de aplicaciones, AWS DevOps, DevOps ingeniero

Limpieza

Tarea	Descripción	Habilidades requeridas
Limpieza de todos los recursos de AWS.	Para limpiar los recursos creados por este patrón, ejecute el siguiente comando. `./uninstall.sh` Esto limpiará todos los recursos creados en este patrón al eliminar la CloudFormation pila.	DevOps ingeniero

Resolución de problemas

Problema	Solución
El registro npm no está configurado correctamente.	Durante la instalación de esta solución, el script instala npm install para descargar todos los paquetes necesarios. Si, durante la instalación, ve un mensaje que dice “No se puede encontrar el módulo”, es posible que el registro npm no esté configurado correctamente. Para ver la configuración actual del registro, ejecute el siguiente comando. `npm config get registry` Ejecute el siguiente comando para establecer el registro con `https://registry.npmjs.org/` .

Problema	Solución
	`npm config set registry https://registry.npmjs.org`
Retrasar la entrega del mensaje SQS.	Como parte de la solución de problemas, si desea retrasar la entrega de los mensajes de SQS a NTH Pod, puede ajustar el parámetro de retraso de entrega de SQS. Para obtener más información, consulte Colas de retraso de Amazon SQS.

Recursos relacionados

- Código fuente de AWS Node Termination Handler
- EC2 taller
- AWS CodePipeline
- Amazon Elastic Kubernetes Service (Amazon EKS)
- AWS Cloud Development Kit
- AWS CloudFormation

Información adicional

1. Busque el nombre del NTH Pod.

```
kubectl get pods -n kube-system |grep aws-node-termination-handler
aws-node-termination-handler-65445555-kbqc7   1/1     Running   0          26m
kubectl get pods -n kube-system |grep aws-node-termination-handler
aws-node-termination-handler-65445555-kbqc7   1/1     Running   0          26m
```

2. Consulte los registros. Un registro de ejemplo se ve del siguiente modo. Muestra que el nodo ha sido acordonado y drenado antes de enviar la señal de finalización del enlace de ciclo de vida del grupo de escalado automático.

```
kubectl -n kube-system logs aws-node-termination-handler-65445555-kbqc7
```

```
022/07/17 20:20:43 INF Adding new event to the event store
 event={"AutoScalingGroupName":"eksctl-my-cluster-target-nodegroup-
ng-10d99c89-NodeGroup-ZME36IGAP7O1","Description":"ASG Lifecycle Termination
 event received. Instance will be interrupted at 2022-07-17 20:20:42.702
 +0000 UTC \n","EndTime":"0001-01-01T00:00:00Z","EventID":"asg-lifecycle-
term-33383831316538382d353564362d343332362d613931352d383430666165636334333564","InProgress":fal
east-2.compute.internal","NodeProcessed":false,"Pods":null,"ProviderID":"aws:///us-
east-2c/i-0409f2a9d3085b80e","StartTime":"2022-07-17T20:20:42.702Z","State":""}
2022/07/17 20:20:44 INF Requesting instance drain event-id=asg-lifecycle-
term-33383831316538382d353564362d343332362d613931352d383430666165636334333564
 instance-id=i-0409f2a9d3085b80e kind=SQS_TERMINATE node-name=ip-192-168-75-60.us-
east-2.compute.internal provider-id=aws:///us-east-2c/i-0409f2a9d3085b80e
2022/07/17 20:20:44 INF Pods on node node_name=ip-192-168-75-60.us-
east-2.compute.internal pod_names=["aws-node-qchsw","aws-node-termination-
handler-65445555-kbqc7","kube-proxy-mz5x5"]
2022/07/17 20:20:44 INF Draining the node
2022/07/17 20:20:44 ??? WARNING: ignoring DaemonSet-managed Pods: kube-system/aws-node-
qchsw, kube-system/kube-proxy-mz5x5
2022/07/17 20:20:44 INF Node successfully cordoned and drained
 node_name=ip-192-168-75-60.us-east-2.compute.internal reason="ASG Lifecycle
 Termination event received. Instance will be interrupted at 2022-07-17 20:20:42.702
 +0000 UTC \n"
2022/07/17 20:20:44 INF Completed ASG Lifecycle Hook (NTH-K8S-TERM-HOOK) for instance
 i-0409f2a9d3085b80e
```

Cree e implemente automáticamente una aplicación Java en Amazon EKS mediante una CI/CD canalización

MAHESH RAGHUNANDANAN, Jomcy Pappachen y James Radtke, Amazon Web Services

Resumen

Este patrón describe cómo crear una canalización de integración y entrega continuas (CI/CD) que cree e implemente automáticamente una aplicación Java con DevSecOps las prácticas recomendadas en un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) del. Nube de AWS Este patrón utiliza una aplicación de saludo desarrollada con un marco Java Spring Boot y que utiliza Apache Maven.

Puede utilizar el enfoque de este patrón para crear el código de una aplicación Java, empaquetar los artefactos de la aplicación como una imagen de Docker, escanear la imagen por motivos de seguridad y cargarla como un contenedor de carga de trabajo en Amazon EKS. El enfoque de este patrón es útil si desea migrar de una arquitectura monolítica estrechamente acoplada a una arquitectura de microservicios. Este enfoque también le ayuda a supervisar y gestionar todo el ciclo de vida de una aplicación Java, lo que garantiza un mayor nivel de automatización y ayuda a evitar errores o fallos.

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- AWS Command Line Interface (AWS CLI) versión 2, instalada y configurada. Para obtener más información al respecto, consulte Instalación o actualización a la última versión de AWS CLI en la AWS CLI documentación.

  AWS CLI la versión 2 debe configurarse con el mismo rol AWS Identity and Access Management (IAM) que crea el clúster de Amazon EKS, ya que solo ese rol está autorizado a añadir otros roles de IAM al. `aws-auth` `ConfigMap` Para obtener información y los pasos de configuración AWS CLI, consulte Configuración de los ajustes en la AWS CLI documentación.
- Funciones y permisos de IAM con acceso total a AWS CloudFormation. Para obtener más información al respecto, consulte Controlar el acceso con IAM en la CloudFormation documentación.

- Un clúster de Amazon EKS existente, con detalles del nombre del rol de IAM y el nombre de recurso de Amazon (ARN) del rol de IAM de los nodos de trabajo del clúster de EKS.
- Escalador automático de clústeres de Kubernetes instalado y configurado en su clúster de Amazon EKS. Para más información, consulte Escalado de computación en clústeres´con Karpenter y Cluster Autoscaler en la documentación de Amazon EKS.
- Acceso al código del GitHub repositorio.

> **Important**
>
> AWS Security Hub CSPM está habilitado como parte de las CloudFormation plantillas que se incluyen en el código de este patrón. De forma predeterminada, una vez que Security Hub CSPM está activado, viene con una prueba gratuita de 30 días. Una vez finalizada la prueba, se aplicará un costo a Servicio de AWS. Para obtener más información acerca de los precios, consulte Precios de AWS Security Hub CSPM.

Versiones de producto

- Helm versión 3.4.2 o posterior
- Apache Maven versión 3.6.3 o posterior
- BridgeCrew Compruebe la versión 2.2 o posterior
- Aqua Security Trivy versión 0.37 o posterior

Arquitectura

Pila de tecnología

- AWS CodeBuild
- AWS CodeCommit
- Amazon CodeGuru
- AWS CodePipeline
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon EKS
- Amazon EventBridge
- AWS Security Hub CSPM

- Amazon Simple Notification Service (Amazon SNS)

Arquitectura de destino

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El desarrollador actualiza el código de la aplicación Java en la rama base del CodeCommit repositorio, lo que crea una solicitud de extracción (PR).
2. En cuanto se envía el PR, Amazon CodeGuru Reviewer revisa automáticamente el código, lo analiza en función de las prácticas recomendadas para Java y ofrece recomendaciones al desarrollador.
3. Una vez que el PR se fusiona con la rama base, se crea un EventBridge evento de Amazon.
4. El EventBridge evento inicia la CodePipeline canalización, que comienza.
5. CodePipeline ejecuta la etapa de CodeSecurity escaneo (seguridad continua).
6. AWS CodeBuild inicia el proceso de análisis de seguridad, en el que los archivos Helm de implementación de Dockerfile y Kubernetes se escanean mediante Checkov, y el código fuente de la aplicación se escanea en función de los cambios incrementales en el código. El escaneo del código fuente de la aplicación lo realiza el contenedor de interfaz de línea de comandos (CLI) de CodeGuru Reviewer.

   > **Note**
   >
   > A partir del 7 de noviembre de 2025, no podrá crear nuevas asociaciones de repositorios en Amazon CodeGuru Reviewer. Para obtener información sobre los servicios con capacidades similares a las de CodeGuru Reviewer, consulte el cambio de disponibilidad de Amazon CodeGuru Reviewer en la documentación de CodeGuru Reviewer.

7. Si la etapa de escaneo de seguridad es exitosa, se inicia la etapa de compilación (integración continua).
8. En la etapa de compilación, CodeBuild crea el artefacto, empaqueta el artefacto en una imagen de Docker, escanea la imagen en busca de vulnerabilidades de seguridad mediante Aqua Security Trivy y almacena la imagen en Amazon ECR.
9. Las vulnerabilidades detectadas en el paso 8 se cargan en Security Hub CSPM para que los desarrolladores o ingenieros las analicen más a fondo. Security Hub CSPM proporciona una descripción general y recomendaciones para corregir las vulnerabilidades.

10. Las notificaciones por correo electrónico de las fases secuenciales de la CodePipeline canalización se envían a través de Amazon SNS.
11. Una vez completadas las fases de integración continua, CodePipeline pasa a la etapa de implementación (entrega continua).
12. La imagen de Docker se implementa en Amazon EKS como una carga de trabajo de contenedor (pod) mediante gráficos de Helm.
13. El pod de la aplicación se configura con el agente Amazon CodeGuru Profiler, que envía los datos de creación de perfiles de la aplicación (CPU, uso del montón y latencia) a CodeGuru Profiler, lo que ayuda a los desarrolladores a comprender el comportamiento de la aplicación.

Tools (Herramientas)

Servicios de AWS

- CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y administrarlos a lo largo de su ciclo de vida en todas las regiones. Cuentas de AWS
- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- AWS CodeCommit es un servicio de control de versiones que permite almacenar y administrar repositorios de Git de forma privada, sin necesidad de administrar su propio sistema de control de origen.
- Amazon CodeGuru Profiler recopila datos de rendimiento en tiempo de ejecución de sus aplicaciones activas y proporciona recomendaciones que pueden ayudarle a ajustar el rendimiento de las aplicaciones.
- AWS CodePipeline permite diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software y automatizar los pasos necesarios para lanzar los cambios en el software de manera continua.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar AWS Kubernetes sin necesidad de instalar o mantener su propio plano de control o nodos de Kubernetes.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes, incluidas AWS Lambda funciones,

puntos de enlace de invocación HTTP que utilizan destinos de API o buses de eventos, entre otros. Cuentas de AWS

- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Security Hub CSPMproporciona una visión completa del estado de su seguridad. AWS También le ayuda a comparar su AWS entorno con los estándares y las mejores prácticas del sector de la seguridad.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otros servicios

- Helm es un administrador de paquetes de código abierto para Kubernetes.
- Apache Maven es una herramienta de software para la comprensión y administración de proyectos.
- BridgeCrew Checkov es una herramienta de análisis de código estático que permite escanear la infraestructura en forma de archivos de código (IaC) para detectar errores de configuración que puedan provocar problemas de seguridad o de conformidad.
- Aqua Security Trivy es un escáner completo para detectar vulnerabilidades en imágenes de contenedores, sistemas de archivos y repositorios de Git, además de problemas de configuración.

Código

El código de este patrón está disponible en el repositorio. GitHub aws-codepipeline-devsecops-amazoneks

Prácticas recomendadas

- Este patrón sigue las prácticas recomendadas de seguridad de IAM para aplicar el principio de privilegios mínimos en las entidades de IAM en todas las fases de la solución. Si desea ampliar la solución con herramientas adicionales Servicios de AWS o de terceros, le recomendamos que consulte la sección sobre la aplicación de permisos con privilegios mínimos de la documentación de IAM.

- Si tiene varias aplicaciones Java, le recomendamos que cree CI/CD canalizaciones independientes para cada aplicación.
- Si tiene una aplicación monolítica, le recomendamos dividirla en microservicios en la medida de lo posible. Los microservicios son más flexibles, facilitan la implementación de aplicaciones como contenedores y proporcionan una mejor visibilidad de la creación y la implementación generales de la aplicación.

Epics

Configuración del entorno

Tarea	Descripción	Habilidades requeridas
Clona el GitHub repositorio.	Para clonar el repositorio, ejecute el siguiente comando. `git clone https://github.com/aws-samples/aws-codepipeline-devsecops-amazoneks`	Desarrollador de aplicaciones, DevOps ingeniero
Cree un bucket de S3 y suba el código.	1. Inicie sesión en Consola de administración de AWS, abra la consola de Amazon S3 y, a continuación, cree un bucket de S3 en el Región de AWS lugar donde planea implementar esta solución. Para obtener más información, consulte Creación de un bucket en la documentación de Amazon S3. 2. En el bucket de S3, cree una carpeta llamada `code`.	AWS DevOps, administrador de la nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	3. Navegue hasta el lugar donde clonó el repositorio. Para crear una versión comprimida de todo el código con la extensión .zip (`cicdstack.zip`) y validar el archivo .zip, ejecute los siguientes comandos en orden.
	`cd aws-codepipeline-devsecops-amazoneks`
	`python -m zipfile -c cicdstack.zip *`
	`python -m zipfile -t cicdstack.zip`
	Note
	Si el comando `python` devuelve un error e indica que no se encontró Python, utilice `python3` en su lugar.
	4. Cargue el archivo `cicdstack.zip` a la carpeta de código que creó previamente en el bucket de S3.	

Tarea	Descripción	Habilidades requeridas
Cree una CloudFormation pila.	1. Abra la consola de CloudFormation y elija Create Stack (Crear pila). 2. En el panel Specify Template (Especificar plantilla), elija Upload a template file (Cargar un archivo de plantilla), elija el archivo `cf_templates/codecommit_ecr.yaml` y, a continuación, elija Next (Siguiente). 3. En Especificar los detalles de la pila, introduzca el nombre de la pila y, a continuación, aporte los siguientes valores de los parámetros de entrada: • `CodeCommitRepositoryBranchName`: el nombre de la rama en la que residirá el código (el nombre predeterminado es `main`) • `CodeCommitRepositoryName`: El nombre del que se va CodeCommitrepository a crear • `CodeCommitRepositoryS3Bucket`: el nombre del bucket de S3 en el que creó la carpeta de códigos	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• `CodeCommitRepositoryS3BucketObjKey` : `code/cicdstack.zip` • `ECRRepositoryName` : el nombre del repositorio de Amazon ECR que se va a crear 4. Elija Siguiente, utilice la configuración predeterminada para las Opciones de configuración de pila y, a continuación, elija Siguiente . 5. En la sección Review (Revisar), verifique los detalles de la plantilla y la pila y, a continuación, seleccione Create stack (Crear pila). A continuación, se crea la pila, que incluye los repositorios CodeCommit y Amazon ECR. 6. Anote los nombres de los repositorios CodeCommit y de Amazon ECR, que serán necesarios para configurar la canalización de Java CI/CD .	

Tarea	Descripción	Habilidades requeridas
Valide el despliegue de la CloudFormation pila.	1. En Stacks, en la CloudFormation consola, verifica el estado de la CloudFormation pila que has implementado. El estado de la pila debe ser CREATE COMPLETE. 2. Desde la consola, compruebe que los repositorios CloudFormation y Amazon ECR se hayan aprovisionado y estén listos.	AWS DevOps, DevOps ingeniero
Elimine el bucket de S3.	Vacíe y borre el bucket de S3 que creó con anterioridad. Para obtener más información, consulte Eliminación de un bucket en la documentación de Amazon S3.	AWS DevOps, DevOps ingeniero

Configure los gráficos de Helm

Tarea	Descripción	Habilidades requeridas
Configure los gráficos de Helm de su aplicación Java.	1. En la ubicación en la que clonó el GitHub repositorio, vaya a la carpeta`helm_charts/aws-proserve-java-greeting` . En esta carpeta, el archivo `values.dev.yaml` contiene información sobre	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	la configuración de los recursos de Kubernetes que puede modificar para las implementaciones de contenedores en Amazon EKS. Actualice el parámetro del repositorio de Docker proporcionando su Cuenta de AWS ID y el Región de AWS nombre del repositorio de Amazon ECR.
	
	`image:`
	`  repository:`
	`  <account-id>.dkr.ecr.<region>.amazonaws.com/<app-ecr-repo-name>`
	
	2. El tipo de servicio del pod de Java está establecido en `LoadBalancer` .
	
	`service:`
	`  type: LoadBalancer`
	`  port: 80`
	`  targetPort: 8080`
	`  path: /hello`
	`  initialDelaySeconds: 60`
	`  periodSeconds: 30`
	
	Para usar un servicio diferente (por ejemplo, `NodePort`), puede cambiar leste parámetro. Para obtener más informaci	

Tarea	Descripción	Habilidades requeridas

	ón, consulte Documentación Kubernetes en la documentación de Kubernetes.
	3. Puede activar el Escalador automático de Kubernetes Horizontal Pod cambiando el parámetro `autoscaling` a `enabled: true`.
	`autoscaling:`
	`  enabled: true`
	`  minReplicas: 1`
	`  maxReplicas: 100`
	`  targetCPUUtilizationPercentage: 80`
	`  # targetMemoryUtilizationPercentage: 80`
	4. Puede habilitar diferentes características para las cargas de trabajo de Kubernetes; para ello, cambie los valores del archivo `values.<ENV>.yaml`, donde `<ENV>` es su entorno de desarrollo, producción, UAT o control de calidad.	

Tarea	Descripción	Habilidades requeridas

Valide los gráficos de Helm para detectar errores de sintaxis.	1. Desde la terminal, compruebe que Helm v3 esté instalado en su estación de trabajo local ejecutando el siguiente comando.
	`helm --version`
	Si Helm v3 no está instalado, instálelo.
	2. En la terminal, navegue hasta el directorio de gráficos de Helm (`helm_charts/aws-proserve-java-greeting`) y ejecute el siguiente comando.
	`helm lint . -f values.dev.yaml`
	Esto comprobará si hay errores de sintaxis en los gráficos de Helm.
		DevOps ingeniero

Configure la CI/CD canalización de Java

Tarea	Descripción	Habilidades requeridas
Crea la CI/CD canalización.	1. Abra la consola de CloudFormation y elija Create Stack (Crear pila).	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	2. En el panel Specify Template (Especificar plantilla), elija Upload a template file (Cargar un archivo de plantilla), elija el archivo `cf_templates/build_deployment.yaml` y, a continuación, elija Next (Siguiente). 3. En Specify stack details (Especificar los detalles de la pila), introduzca el Stack name (Nombre de la pila) y, a continuación, aporte los siguientes valores de los parámetros de entrada: • `CodeBranchName`: Nombre de la rama del CodeCommit repositorio en el que reside tu código • `EKSClusterName`: nombre de su clúster de EKS (no el ID `EKSCluster`) • `EKSCodeBuildAppName`: Nombre de la aplicación del gráfico de Helm (`aws-proserve-java-greeting`) • `EKSWorkerNodeRoleARN`: ARN del rol de IAM asignado a los nodos de trabajo de Amazon EKS	

Tarea	Descripción	Habilidades requeridas
	• `EKSWorkerNodeRoleName` : nombre del rol de IAM asignado a los nodos de trabajo de Amazon EKS • `EcrDockerRepository` : nombre del repositorio de Amazon ECR donde se almacenarán las imágenes de Docker de su código • `EmailRecipient` : dirección de correo electrónico a la que se deben enviar las notificaciones de compilación • `EnvType`: entorno (por ejemplo, desarrollo, pruebas o producción) • `SourceRepoName` : Nombre del CodeCommit repositorio en el que reside tu código 4. Elija Siguiente. Utilice la configuración predeterminada para las Configure stack options (Opciones de configuración de pila) y, a continuación, elija Next (Siguiente). 5. En la sección Revisar, compruebe los detalles de la CloudFormation plantilla	

Tarea	Descripción	Habilidades requeridas
	y la pila y, a continuación, seleccione Siguiente. 6. Seleccione Creación de pila. 7. Durante el despliegue de la CloudFormation pila, el propietario de la dirección de correo electrónico que has indicado en los parámetros recibirá un mensaje para suscribirse a un tema de SNS. Para suscribirse a Amazon SNS, el propietario debe elegir el enlace del mensaje. 8. Una vez creada la pila, abra la pestaña Salidas de la pila y, a continuación, registre el valor ARN de la clave de salida `EksCodeBuildkubeRoleARN` . Este valor de ARN de IAM se requerirá más adelante, cuando otorgue permisos para que CodeBuild la función de IAM implement e cargas de trabajo en el clúster de Amazon EKS.	

Active la integración entre Security Hub CSPM y Aqua Security

Tarea	Descripción	Habilidades requeridas
Active la integración de Aqua Security.	Este paso es necesario para cargar los hallazgos de vulnerabilidad de imágenes de Docker reportados por Trivy a Security Hub CSPM. Como CloudFormation no es compatible con las integraciones CSPM de Security Hub, este proceso debe realizarse manualmente. 1. Abra la consola de AWS Security Hub CSPM y vaya a Integraciones. 2. Busque Aqua Security y seleccione Aqua Security: Aqua Security. 3. Seleccione Aceptar los resultados.	Administrador DevOps e ingeniero de AWS

Configure CodeBuild para ejecutar los comandos Helm o kubectl

Tarea	Descripción	Habilidades requeridas
Permite CodeBuild ejecutar comandos Helm o kubectl en el clúster de Amazon EKS.	CodeBuild Para autenticarse para usar Helm o `kubectl` comandos con el clúster de Amazon EKS, debe añadir las funciones de IAM al. `aws-auth ConfigMap` En este caso, añada el ARN de la función de IAM`EksCodeBu`	DevOps

Tarea	Descripción	Habilidades requeridas
	`ildkubeRoleARN` , que es la función de IAM creada para que el CodeBuild servicio acceda al clúster de Amazon EKS e implemente cargas de trabajo en él. Esta es una actividad que se realiza una vez. **Important** El siguiente procedimiento debe completarse antes de la fase de aprobación de la implementación. CodePipeline 1. Abra el script de intérprete de comandos `cf_templates/kube_aws_auth_configmap_patch.sh` en su entorno Amazon Linux o macOS. 2. Autentifíquese en el clúster de Amazon EKS ejecutando el siguiente comando. `aws eks --region <aws-region> update-kubeconfig --name <eks-cluster-name>` 3. Ejecute el script de intérprete de comandos mediante	

Tarea	Descripción	Habilidades requeridas
	el siguiente comando, sustituyendo `<rolearn-eks-codebuild-kubectl>` por el valor ARN `EksCodeBuildkubeRoleARN` que registró anteriormente. `bash cf_templates/kube_aws_auth_configmap_patch.sh <rolearn-eks-codebuild-kubectl>` `aws_auth ConfigMap` se configura y se concede el acceso.	

Valide la CI/CD canalización

Tarea	Descripción	Habilidades requeridas
Compruebe que la CI/CD canalización se inicie automáticamente.	1. La fase de CodeSecurity análisis del proceso suele fallar si Checkov detecta vulnerabilidades en los gráficos de Dockerfile o Helm. Sin embargo, el objetivo de este ejemplo es establecer un proceso de identificación de posibles vulnerabilidades de seguridad, en lugar de corregirlas de forma	DevOps

Tarea	Descripción	Habilidades requeridas

	gradual, lo que suele ser un proceso. CI/CD DevSecOps En el archivo `buildspec/buildspec_secscan.yaml`, el comando `checkov` usa la marca `--soft-fail` para evitar que la canalización falle.
	
	`- echo -e "\n Running Dockerfile Scan"`
	`- checkov -f code/app/Dockerfile --framework dockerfile --soft-fail --summary-position bottom`
	`- echo -e "\n Running Scan of Helm Chart files"`
	`- cp -pv helm_charts/$EKS_CODEBUILD_APP_NAME/values.dev.yaml helm_charts/$EKS_CODEBUILD_APP_NAME/values.yaml`
	`- checkov -d helm_charts/$EKS_CODEBUILD_APP_NAME --framework helm --soft-fail --summary-position bottom`
	`- rm -rfv helm_charts/$EKS_CODEBUILD_APP_NAME/values.yaml`
	
	Para que la canalización falle cuando se detecten	

Tarea	Descripción	Habilidades requeridas
	vulnerabilidades en los gráficos de Dockerfile y Helm, se debe eliminar la opción `--soft-fail` del comando `checkov`. Luego, los desarrolladores o ingenieros pueden corregir las vulnerabilidades y registrar los cambios en el repositorio de código CodeCommit fuente. 2. Al igual que en CodeSecurity Scan, la etapa de compilación utiliza Aqua Security Trivy para identificar las vulnerabilidades `HIGH` y las imágenes de `CRITICAL` Docker antes de enviar la aplicación a Amazon ECR. `- AWS_REGION=$AWS_DEFAULT_REGION AWS_ACCOUNT_ID=$AWS_ACCOUNT_ID trivy -d image --no-progress --ignore-unfixed --exit-code 0 --severity HIGH,CRITICAL --format template --template "@securityhub/asff.tpl" -o securityhub/report.asff $AWS_ACCOUNT_ID.dkr.ecr.$AWS_DEFAULT_REGION.amazonaws.com/$IMAG`	

Tarea	Descripción	Habilidades requeridas
	`E_REPO_NAME:$CODEB UILD_RESOLVED_SOUR CE_VERSION` En este ejemplo, la canalización no devuelve un error cuando se informa de vulnerabilidades en las imágenes de Docker, ya que el comando `trivy` del archivo `buildspec /buildspec.yml` incluye la marca `--exit-code` con un valor de `0`. Para que la canalización devuelva un error cuando se detecten vulnerabi lidades `HIGH` y `CRTICAL`, cambie el valor de `--exit-code` a `1`. A continuación, los desarroll adores o ingenieros pueden corregir las vulnerabilidades y registrar los cambios en el repositorio de CodeCommit código fuente. 3. Las vulnerabilidades de imagen de Docker reportadas por Aqua Security Trivy se cargan en Security Hub CSPM. En la consola CSPM de Security Hub, vaya a Findings. Filtre los resultados con Registrar Estado= Activo y	

Tarea	Descripción	Habilidades requeridas
	Producto = Aqua Security. Aquí se enumeran las vulnerabilidades de imagen de Docker en Security Hub CSPM. Las vulnerabilidades pueden tardar entre 15 minutos y una hora en aparecer en Security Hub CSPM. Para obtener más información sobre cómo iniciar la canalización mediante el uso CodePipeline, consulte Iniciar una canalización enCodePipeline, Iniciar una canalización manualmente e Iniciar una canalización según un cronograma en la CodePipeline documentación.	

Tarea	Descripción	Habilidades requeridas
Apruebe la implementación.	1. Una vez finalizada la fase de construcción, hay una puerta de aprobación de la implementación. El revisor o el administr ador de versiones deben inspeccionar la compilación y, si se cumplen todos los requisitos, aprobarla. Este es el enfoque recomenda do para los equipos que utilizan la entrega continua para la implementación de aplicaciones. 2. Tras la aprobación, la canalización inicia la fase de implementación. 3. Una vez finalizada la fase de despliegue, el CodeBuild registro de esta fase proporciona la URL de la aplicación. Utilice la URL para validar que la aplicació n esté lista.	DevOps

Tarea	Descripción	Habilidades requeridas
Valide la creación de perfiles de la aplicación.	Una vez finalizada la implementación y desplegado el pod de la aplicación en Amazon EKS, el agente Amazon CodeGuru Profiler que está configurado en la aplicación intentará enviar los datos de creación de perfiles de la aplicación (CPU, resumen del montón, latencia y cuellos de botella) a Profiler. CodeGuru Para la implementación inicial de una aplicación, CodeGuru Profiler tarda unos 15 minutos en visualizar los datos de creación de perfiles.	AWS DevOps

Recursos relacionados

- AWS CodePipeline documentación
- Escanear imágenes con Trivy en una AWS CodePipeline (AWS entrada de blog)
- Mejora de sus aplicaciones Java con Amazon CodeGuru Profiler (AWS entrada del blog)
- AWS Sintaxis del formato de búsqueda de seguridad (ASFF)
- Patrones de EventBridge eventos de Amazon
- Actualización de Helm

Información adicional

- CodeGuru El generador de perfiles no debe confundirse con el AWS X-Ray servicio en términos de funcionalidad. Le recomendamos que utilice CodeGuru Profiler para identificar las líneas de códigos más caras que puedan provocar cuellos de botella o problemas de seguridad, y que las

corrija antes de que se conviertan en un riesgo potencial. El servicio X-Ray sirve para supervisar el rendimiento de las aplicaciones.

- En este patrón, las reglas de eventos se asocian al bus de eventos predeterminado. Si es necesario, puede ampliar el patrón para utilizar un bus de eventos personalizado.
- Este patrón utiliza CodeGuru Reviewer como una herramienta estática de pruebas de seguridad de aplicaciones (SAST) para el código de la aplicación. También puedes usar esta canalización para otras herramientas, como SonarQube Checkmarx. Puede añadir las instrucciones de configuración del escaneo a cualquiera de estas herramientas `buildspec/buildspec_secscan.yaml` para reemplazar las instrucciones de CodeGuru escaneo.

> **Note**
>
> A partir del 7 de noviembre de 2025, no podrá crear nuevas asociaciones de repositorios en Amazon CodeGuru Reviewer. Para obtener información sobre los servicios con capacidades similares a las de CodeGuru Reviewer, consulte el cambio de disponibilidad de Amazon CodeGuru Reviewer en la documentación de CodeGuru Reviewer.

Copie imágenes de contenedores de Amazon ECR en y Cuentas de AWS Regiones de AWS

Faisal Shahdad, Amazon Web Services

Resumen

Este patrón le muestra cómo utilizar un enfoque sin servidor para replicar imágenes etiquetadas de repositorios existentes de Amazon Elastic Container Registry (Amazon ECR) a otros repositorios y. Cuentas de AWS Regiones de AWS La solución se utiliza AWS Step Functions para administrar el flujo de trabajo de replicación y AWS Lambda funciona para copiar imágenes de contenedores de gran tamaño.

Amazon ECR utiliza características nativas de replicación entre regiones y entre cuentas que replican imágenes de contenedor entre regiones y cuentas. Sin embargo, estas características solo replican las imágenes desde el momento en que se activa la replicación. No existe ningún mecanismo para replicar las imágenes existentes en distintas regiones y cuentas.

Este patrón ayuda a los equipos de inteligencia artificial (IA) a distribuir modelos, marcos (por ejemplo PyTorch TensorFlow, y Hugging Face) y dependencias de aprendizaje automático (ML) en contenedores a otras cuentas y regiones. Esto puede ayudarle a superar los límites del servicio y optimizar los recursos de computación de la GPU. También puede replicar selectivamente los repositorios de Amazon ECR desde regiones y cuentas de origen específicas. Para obtener más información, consulte Cross-Region replication in Amazon ECR has landed (La replicación entre regiones en Amazon ECR ya está aquí).

Requisitos previos y limitaciones

Requisitos previos

- Dos o más activas Cuentas de AWS (una cuenta de origen y una cuenta de destino, como mínimo)
- Permisos adecuados AWS Identity and Access Management (IAM) en todas las cuentas
- Docker para crear la imagen del contenedor de Lambda
- AWS Command Line Interface (AWS CLI) configurados para todas las cuentas

Limitaciones

- Exclusión de imágenes sin etiquetar: la solución copia solo las imágenes del contenedor que tienen etiquetas explícitas. Omite las imágenes sin etiquetar que existen con resúmenes de `SHA256`.
- Restricciones de tiempo de espera de ejecución de Lambda: AWS Lambda está limitado a un tiempo de espera de ejecución máximo de 15 minutos, que puede ser insuficiente para copiar repositorios o imágenes de contenedores de gran tamaño.
- Administración manual de imágenes de contenedor: el código `crane-app.py` de Python requiere volver a crear e implementar la imagen de contenedor de Lambda.
- Capacidad de procesamiento paralelo limitada: la configuración de estado de `MaxConcurrency` limita el número de repositorios que puede copiar al mismo tiempo. Sin embargo, puedes modificar esta configuración en la plantilla de la cuenta de origen. AWS CloudFormation Tenga en cuenta que los valores de simultaneidad más altos pueden provocar que supere los límites de tasas de servicio y las cuotas de ejecución de Lambda a nivel de cuenta.

Arquitectura

Pila de destino

El patrón tiene cuatro componentes principales:

- Infraestructura de cuentas de origen: CloudFormation plantilla que crea los componentes de orquestación
- Infraestructura de cuentas de destino: CloudFormation plantilla que crea funciones de acceso entre cuentas
- Función de Lambda: función basada en Python que utiliza Crane para copiar imágenes de forma eficiente.
- Imagen de contenedor: contenedor de Docker que empaqueta la función de Lambda con las herramientas necesarias.

Arquitectura de destino

Flujo de trabajo de Step Functions

La máquina de estados de Step Functions organiza lo siguiente, como se muestra en el siguiente diagrama:

- `PopulateRepositoryList`: analiza los repositorios de Amazon ECR y rellena Amazon DynamoDB.
- `GetRepositoryList`: recupera una lista de repositorios únicos de DynamoDB.
- `DeduplicateRepositories`: garantiza que no haya ningún procesamiento duplicado.
- `CopyRepositories`: gestiona la copia paralela de repositorios.
- `NotifySuccess`/`NotifyFailure`: notificaciones de Amazon Simple Notification Service (Amazon SNS) basadas en el resultado de la ejecución.

Tools (Herramientas)

Herramientas de Amazon

- Amazon le CloudWatch ayuda a supervisar las métricas de sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Step Functionses un servicio de organización sin servidor que le ayuda a combinar funciones de Lambda y otras Servicios de AWS para crear aplicaciones críticas para la empresa.

Otras herramientas

- Crane es una herramienta de orquestación de Docker. Es similar a Docker Compose, pero tiene características adicionales.

- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización a nivel del sistema operativo para entregar software en contenedores.

Repositorio de código

- El código de este patrón está disponible en el repositorio. GitHub sample-ecr-copy Puede usar la CloudFormation plantilla del repositorio para crear los recursos subyacentes.

Prácticas recomendadas

Siga el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Preparación del entorno de

Tarea	Descripción	Habilidades requeridas

Configure AWS CLI los perfiles.	1. Configure el perfil de la cuenta de origen:
	`aws configure --profile source-account`
	`# Enter: Access Key ID, Secret Access Key, Default region, Output format (json)`
	2. Configure el perfil de la cuenta de destino:
	`aws configure --profile destination-account`
	`# Enter: Access Key ID, Secret Access`
		DevOps ingeniero, ingeniero de datos, ingeniero de aprendizaje automático

Tarea	Descripción	Habilidades requeridas

	Key, Default region, Output format (json)
	3. Verifique las configuraciones:
	`aws sts get-caller-identity --profile source-account`
	`aws sts get-caller-identity --profile destination-account`	

Tarea	Descripción	Habilidades requeridas

Reúna la información requerida.	1. Obtenga el ID de la cuenta de origen:
	`export SOURCE_ACCOUNT_ID=$(aws sts get-caller-identity --profile source-account --query Account --output text)`
	`echo "Source Account ID: $SOURCE_ACCOUNT_ID"`
	2. Obtenga el ID de la cuenta de destino:
	`export DEST_ACCOUNT_ID=$(aws sts get-caller-identity --profile destination-account --query Account --output text)`
	`echo "Destination Account ID: $DEST_ACCOUNT_ID"`
	3. Configure el Regiones de AWS. Modifique este comando para su región:
	`export SOURCE_REGION="us-east-1"`
	`export DEST_REGION="us-east-2"`
	4. Enumere los repositorios de Amazon ECR existentes en la cuenta de origen:
		DevOps ingeniero, ingeniero de datos, ingeniero de aprendizaje automático

Tarea	Descripción	Habilidades requeridas
	`aws ecr describe-repositories --profile source-account --region $SOURCE_REGION --query 'repositories[].repositoryName' --output table`	
Clonar el repositorio.	Clone el repositorio del patrón en la estación de trabajo local: `git clone https://github.com/aws-samples/sample-ecr-copy`	DevOps ingeniero, ingeniero de datos, ingeniero de ML

Implementación de infraestructura para la cuenta de destino

Tarea	Descripción	Habilidades requeridas
Valide la plantilla.	Valide la CloudFormation plantilla: `aws cloudformation validate-template \ --template-body file://"Destination Account cf_template.yml" \ --profile destination-account`	DevOps ingeniero, ingeniero de aprendizaje automático, ingeniero de datos
Implemente la infraestructura de destino.	1. Implemente la pila de la cuenta de destino:	Ingeniero de datos, ingeniero de aprendizaje automático, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	``
	aws cloudformation
	 deploy \
	  --template-file
	 "Destination Account
	 cf_template.yml" \
	  --stack-name ecr-
	copy-destination \
	  --parameter-overri
	des \
	  SourceAccountId=
	$SOURCE_ACCOUNT_ID \
	  SourceRol
	eName=ECRContainer
	LambdaRole \
	  --capabilities
	 CAPABILITY_NAMED_I
	AM \
	  --profile destinati
	on-account \
	  --region $DEST_REG
	ION
	``
	2. Espere a que se complete la pila:
	``
	aws cloudformation
	 wait stack-create-
	complete \
	  --stack-name ecr-
	copy-destination \
	  --profile destinati
	on-account \
	  --region $DEST_REG
	ION
	``	

Tarea	Descripción	Habilidades requeridas

Comprobar la implementación.	1. Obtenga salidas de pila:
	`aws cloudformation describe-stacks \ --stack-name ecr-copy-destination \ --profile destination-account \ --region $DEST_REGION \ --query 'Stacks[0].Outputs' \ --output table`
	2. Almacene el rol de IAM entre cuentas:
	`export CROSS_ACCOUNT_ROLE_ARN=$(aws cloudformation describe-stacks \ --stack-name ecr-copy-destination \ --profile destination-account \ --region $DEST_REGION \ --query 'Stacks[0].Outputs[?OutputKey==`CrossAccountRoleArn`].OutputValue' \ --output text)`
	`echo "Cross-Account Role ARN: $CROSS_ACCOUNT_ROLE_ARN"`
		DevOps ingeniero, ingeniero de aprendizaje automático, ingeniero de datos

Creación e implementación de la imagen de contenedor de Lambda

Tarea	Descripción	Habilidades requeridas

Prepare la compilación del contenedor.	1. Compruebe que Docker se esté ejecutando:
	`docker --version`
	`docker info`
	2. Asegúrese de que `crane-app.py` y `Dockerfile` estén en el directorio actual:
	`ls -la crane-app.py Dockerfile`
		Ingeniero de datos, ingeniero de aprendizaje automático, DevOps ingeniero

Compile la imagen de contenedor.	1. Compile la imagen de contenedor de Lamba:
	`docker build -t ecr-copy-lambda . --no-cache`
	2. Compruebe que la imagen se haya creado:
	`docker images ecr-copy-lambda`
	3. (Opcional) Pruebe el contenedor localmente:
	`docker run --rm --entrypoint python ecr-copy-lambda -c "import boto3; print('Container working')"`
		Ingeniero de datos, ingeniero de aprendizaje automático, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Cree un repositorio y cargue la imagen.	1. Cree un repositorio de Amazon ECR en la cuenta de origen:
	`aws ecr create-repository \ --repository-name ecr-copy-lambda \ --profile source-account \ --region $SOURCE_REGION`
	2. Obtenga un token de inicio de sesión de Amazon ECR y autentique Docker:
	`aws ecr get-login-password \ --profile source-account \ --region $SOURCE_REGION | \ docker login --username AWS --password-stdin \ $SOURCE_ACCOUNT_ID.dkr.ecr.$SOURCE_REGION.amazonaws.com`
	3. Etiquete la imagen para Amazon ECR:
	`docker tag ecr-copy-lambda:latest \ $SOURCE_ACCOUNT_ID.dkr.ecr.$SOURCE_REGION.amazonaws.co`
		Ingeniero de datos, ingeniero de aprendizaje automático, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	m/ecr-copy-lambda:latest
	4. Cargue la imagen en Amazon ECR:
	`docker push $SOURCE_ACCOUNT_ID.dkr.ecr.$SOURCE_REGION.amazonaws.com/ecr-copy-lambda:latest`
	5. Almacene el URI de la imagen para su uso posterior:
	`export LAMBDA_IMAGE_URI="$SOURCE_ACCOUNT_ID.dkr.ecr.$SOURCE_REGION.amazonaws.com/ecr-copy-lambda:latest"`
	`echo "Lambda Image URI: $LAMBDA_IMAGE_URI"`	

Tarea	Descripción	Habilidades requeridas

Verifique la imagen.	1. Enumere las imágenes del repositorio:
	`aws ecr list-images \ --repository-name ecr-copy-lambda \ --profile source-account \ --region $SOURCE_REGION`
	2. Obtenga los detalles de la imagen:
	`aws ecr describe-images \ --repository-name ecr-copy-lambda \ --profile source-account \ --region $SOURCE_REGION`
		Ingeniero de datos, ingeniero de aprendizaje automático, DevOps ingeniero

Implementación de la infraestructura de cuenta de origen

Tarea	Descripción	Habilidades requeridas
Prepare los parámetros de implementación.	1. Configure el correo electrónico de notificación: `export NOTIFICATION_EMAIL="your-email@company.com"` 2. Defina los repositorios que desea copiar (separados por comas):	Ingeniero de datos, DevOps ingeniero, ingeniero de aprendizaje automático

Tarea	Descripción	Habilidades requeridas
	`export REPOSITOR Y_LIST="app-fronte nd,app-backend,dat abase-migrations"`	

	3. Configure el entorno:
	`export ENVIRONME NT="dev"`
	
	`echo "Deployment Parameters:" echo "Source Account: $SOURCE_ACCOUNT_ID" echo "Destination Account: $DEST_ACC OUNT_ID" echo "Source Region: $SOURCE_REGION" echo "Destination Region: $DEST_REG ION" echo "Lambda Image: $LAMBDA_IMAGE_URI" echo "Notification Email: $NOTIFICA TION_EMAIL" echo "Repositories: $REPOSITORY_LIST"`	

Tarea	Descripción	Habilidades requeridas
Valide la plantilla de origen.	Valide la CloudFormation plantilla de origen: `aws cloudformation validate-template \ --template-body file://"Source Account Cf template.yml" \ --profile source-account`	Ingeniero de datos, ingeniero de aprendizaje automático, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Implemente la infraestructura de origen.	1. Implemente la pila de la cuenta de origen: `aws cloudformation deploy \ --template-file "Source Account Cf template.yml" \ --stack-name ecr-copy-source \ --parameter-overrides \ SourceAccountId=$SOURCE_ACCOUNT_ID \ DestinationAccountId=$DEST_ACCOUNT_ID \ DestinationRegion=$DEST_REGION \ SourceRegion=$SOURCE_REGION \ NotificationEmail=$NOTIFICATION_EMAIL \ RepositoryList="$REPOSITORY_LIST" \ LambdaImageUri=$LAMBDA_IMAGE_URI \ Environment=$ENVIRONMENT \ --capabilities CAPABILITY_NAMED_IAM \ --profile source-account \ --region $SOURCE_REGION`	Ingeniero de datos, ingeniero de aprendizaje automático, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	2. Espere a que se complete la pila (esta acción puede tardar hasta 10 minutos): `aws cloudformation wait stack-create-complete \ --stack-name ecr-copy-source \ --profile source-account \ --region $SOURCE_REGION`	

Tarea	Descripción	Habilidades requeridas

Verifique la implementación y recopile los resultados.	1. Obtenga las salidas de la pila:
	`aws cloudformation describe-stacks \ --stack-name ecr-copy-source \ --profile source-account \ --region $SOURCE_REGION \ --query 'Stacks[0].Outputs' \ --output table`
	2. Guarde los nombres de recursos de Amazon (ARNs) para la máquina de estado y el tema SNS:
	`export STATE_MACHINE_ARN=$(aws cloudformation describe-stacks \ --stack-name ecr-copy-source \ --profile source-account \ --region $SOURCE_REGION \ --query 'Stacks[0].Outputs[?OutputKey==`StateMachineArn`].OutputValue' \ --output text)`
	`export SNS_TOPIC_ARN=$(aws cloudformation describe-stacks \`
		DevOps ingeniero, ingeniero de aprendizaje automático, ingeniero de datos

Tarea	Descripción	Habilidades requeridas

	<pre> --stack-name ecr-copy-source \
	  --profile source-account \
	  --region $SOURCE_REGION \
	  --query 'Stacks[0].Outputs[?OutputKey==`SNSTopicArn`].OutputValue' \
	  --output text)
	
	echo "State Machine ARN: $STATE_MACHINE_ARN"
	echo "SNS Topic ARN: $SNS_TOPIC_ARN"</pre>	

Confirme la suscripción de correo electrónico.	1. Compruebe su correo electrónico para confirmar su suscripción a SNS.
	2. Seleccione el enlace de confirmación en el correo electrónico.
	3. Verifique el estado de la suscripción.
	<pre>aws sns list-subscriptions-by-topic \
	  --topic-arn $SNS_TOPIC_ARN \
	  --profile source-account \
	  --region $SOURCE_REGION</pre>
		Ingeniero de datos, ingeniero de aprendizaje automático, DevOps ingeniero

Ejecución y supervisión del proceso de copia

Tarea	Descripción	Habilidades requeridas
Ejecute y supervise el proceso de copia.	1. Inicie sesión en la Consola de administración de AWSconsola Step Functions y ábrala. 2. Localice la máquina de estado. 3. Seleccione Iniciar ejecución . Cuando finalice, los resultados se muestran en la pestaña de entrada y salida de la ejecución. 4. (Opcional) Si quieres seguir ejecutando Step Functions mediante el AWS CLI, sigue los pasos restantes de esta epopeya.	DevOps ingeniero, ingeniero de aprendizaje automático, ingeniero de datos

Ejecute Step Functions.	1. Genere un nombre único:
	
	`export EXECUTION_NAME="ecr-copy-$(date +%Y%m%d-%H%M%S)"`
	
	2. Ejecute Step Functions.
	
	`export EXECUTION_ARN=$(aws stepfunctions start-execution \ --state-machine-arn $STATE_MACHINE_ARN \`
		DevOps ingeniero, ingeniero de aprendizaje automático, ingeniero de datos

Tarea	Descripción	Habilidades requeridas

	<pre> --name $EXECUTIO
	N_NAME \
	  --profile source-ac
	count \
	  --region $SOURCE_R
	EGION \
	  --query 'executio
	nArn' \
	  --output text)
	
	echo "Execution
	 started: $EXECUTIO
	N_ARN"
	echo "Execution
	 Name: $EXECUTIO
	N_NAME"</pre>	

Tarea	Descripción	Habilidades requeridas

Supervise el progreso.	1. Compruebe el estado:
	`aws stepfunctions describe-execution \ --execution-arn $EXECUTION_ARN \ --profile source-account \ --region $SOURCE_REGION \ --query '{Status:status,StartDate:startDate,StopDate:stopDate}' \ --output table`
	2. Obtenga el historial:
	`aws stepfunctions get-execution-history \ --execution-arn $EXECUTION_ARN \ --profile source-account \ --region $SOURCE_REGION \ --query 'events[?type==`TaskStateEntered` || type==`TaskSucceeded` || type==`TaskFailed`].{Type:type,Timestamp:timestamp,Details:stateEnteredEventDetails.name}' \ --output table`
		DevOps ingeniero, ingeniero de aprendizaje automático, ingeniero de datos

Tarea	Descripción	Habilidades requeridas

Compruebe los resultados.	Espere a que se complete el proceso (se actualiza cada 30 segundos):
	
	`while true; do`
	`  STATUS=$(aws`
	` stepfunctions`
	` describe-execution \`
	`  --execution-arn`
	` $EXECUTION_ARN \`
	`  --profile source-ac`
	`count \`
	`  --region $SOURCE_R`
	`EGION \`
	`  --query 'status' \`
	`  --output text)`
	
	`  echo "Current status:`
	` $STATUS"`
	
	`  if [[ "$STATUS"`
	` == "SUCCEEDED"`
	` || "$STATUS" ==`
	` "FAILED" || "$STATUS"`
	` == "TIMED_OUT"`
	` || "$STATUS" ==`
	` "ABORTED" ]]; then`
	`  break`
	`  fi`
	
	`  sleep 30`
	`done`
	
	`echo "Final execution`
	` status: $STATUS"`
		DevOps ingeniero, ingeniero de aprendizaje automático, ingeniero de datos

Tarea	Descripción	Habilidades requeridas

Verifique las imágenes.	1. Enumere los repositorios de la cuenta de destino:
	`aws ecr describe-repositories \ --profile destination-account \ --region $DEST_REGION \ --query 'repositories[].repositoryName' \ --output table`
	2. Compruebe las imágenes del repositorio:
	`for repo in $(echo $REPOSITORY_LIST | tr ',' ' '); do echo "\nImages in repository: $repo" aws ecr list-images \ --repository-name $repo \ --profile destination-account \ --region $DEST_REGION \ --query 'imageIds[].imageTag' \ --output table 2>/dev/null || echo "Repository $repo not found or no images" done`
		DevOps ingeniero, ingeniero de datos, ingeniero de ML

Resolución de problemas

Problema	Solución

No se ha podido ejecutar Step Functions.	1. Para recuperar los eventos de error detallados del historial, ejecute el siguiente AWS CLI comando:
	`if [[ "$STATUS" == "FAILED" ]]; then`
	`  echo "Getting failure details..."`
	`  aws stepfunctions get-execution-history \`
	`  --execution-arn $EXECUTION_ARN \`
	`  --profile source-account \`
	`  --region $SOURCE_REGION \`
	`  --query 'events[?type==`TaskFailed`]' \`
	`  --output json`
	`fi`
	2. Para recuperar los registros de las funciones de Lambda fallidas, ejecute el siguiente comando: AWS CLI
	`# Check Lambda function logs`
	`echo "\nLambda function logs:"`
	`aws logs describe-log-groups \`
	`  --log-group-name-prefix "/aws/lambda/ecr-copy-source" \`
	`  --profile source-account \`
	`  --region $SOURCE_REGION \`
	`  --query 'logGroups[].logGroupName' \`
	`  --output table`

Recursos relacionados

- Documentación de Crane

- ¿Qué es Amazon Elastic Container Registry?
- ¿Qué es AWS Lambda?
- ¿Qué es Step Functions?

Información adicional

Parámetros de configuración

Parámetro	Description (Descripción)	Ejemplo
`SourceAccountId`	Cuenta de AWS ID de la fuente	`11111111111`
`DestinationAccountId`	Cuenta de AWS ID de destino	`22222222222`
`DestinationRegion`	Objetivo Región de AWS	`us-east-2`
`SourceRegion`	Fuente Región de AWS	`us-east-1`
`NotificationEmail`	Correo electrónico para las notificaciones	`abc@xyz.com`
`RepositoryList`	Repositorios que se van a copiar	`repo1,repo2,repo3`
`LambdaImageUri`	URI de la imagen de contenedor de Lambda	`${ACCOUNT}.dkr.ecr.${REGION}.amazonaws.com/ecr-copy-lambda:latest`

Cree una definición de tareas de Amazon ECS y monte un sistema de archivos en EC2 las instancias mediante Amazon EFS

Durga Prasad Cheepuri, Amazon Web Services

Resumen

Este patrón proporciona ejemplos de código y pasos para crear una definición de tarea de Amazon Elastic Container Service (Amazon ECS) que se ejecute en instancias de Amazon Elastic Compute Cloud (EC2Amazon) en la nube de Amazon Web Services (AWS), mientras se utiliza Amazon Elastic File System (Amazon EFS) para montar un sistema de archivos en EC2 esas instancias. Las tareas de Amazon ECS que utilizan Amazon EFS montan automáticamente los sistemas de archivos que especifique en la definición de la tarea y ponen estos sistemas de archivos a disposición de los contenedores de la tarea en todas las zonas de disponibilidad de una región de AWS.

Para cumplir sus requisitos de almacenamiento persistente y almacenamiento compartido, puede utilizar Amazon ECS y Amazon EFS juntos. Por ejemplo, puede usar Amazon EFS para almacenar datos persistentes de usuarios y datos de aplicaciones para sus aplicaciones con pares de contenedores ECS activos y en espera que se ejecuten en diferentes zonas de disponibilidad para lograr una alta disponibilidad. También puede usar Amazon EFS para almacenar datos compartidos a los que se puede acceder en paralelo mediante contenedores de ECS y cargas de trabajo distribuidas.

Para utilizar Amazon EFS con Amazon ECS, puede añadir una o más definiciones de volumen a una definición de tarea. Una definición de volumen incluye un ID de sistema de archivos de Amazon EFS, un ID de punto de acceso y una configuración para la autorización de AWS Identity and Access Management (IAM) o el cifrado en tránsito de la seguridad de la capa de transporte (TLS). Puede usar definiciones de contenedores dentro de las definiciones de tareas para especificar los volúmenes de definición de tareas que se montan cuando se ejecuta el contenedor. Cuando se ejecuta una tarea que utiliza un sistema de archivos Amazon EFS, Amazon ECS se asegura de que el sistema de archivos esté montado y disponible para los contenedores que necesitan acceder a él.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una nube privada virtual (VPC) con un punto de conexión de red privada virtual (VPN) (VPN) o un router

- (Recomendado) El Agente contenedor Amazon ECS 1.38.0 o posterior para garantizar la compatibilidad con los puntos de acceso de Amazon EFS y las características de autorización de IAM (para obtener más información, consulte la entrada del blog de AWS Nuevo para Amazon EFS – Autorización y puntos de acceso de IAM).

Limitaciones

- Las versiones del agente contenedor de Amazon ECS anteriores a la 1.35.0 no admiten los sistemas de archivos de Amazon EFS para las tareas que utilizan el tipo de EC2 lanzamiento.

Arquitectura

El siguiente diagrama muestra un ejemplo de una aplicación que utiliza Amazon ECS para crear una definición de tarea y montar un sistema de archivos Amazon EFS en EC2 instancias de contenedores de ECS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Crear un sistema de archivos de Amazon EFS.
2. Cree una definición de tarea con un contenedor.
3. Configure las instancias de contenedor para montar el sistema de archivos de Amazon EFS. La definición de la tarea hace referencia a los montajes de volumen, para que la instancia de contenedor pueda utilizar el sistema de archivos Amazon EFS. Las tareas de ECS tienen acceso al mismo sistema de archivos de Amazon EFS, independientemente de la instancia de contenedor en la que se creen esas tareas.
4. Cree un servicio de Amazon ECS con tres instancias de la definición de tarea.

Pila de tecnología

- Amazon EC2
- Amazon ECS
- Amazon EFS

Tools (Herramientas)

- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede utilizar Amazon EC2 para lanzar tantos o tan pocos servidores virtuales como necesite, y puede ampliarlos de forma horizontal o horizontal.
- Amazon ECS: Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores altamente escalable y rápido que permite ejecutar, detener y administrar contenedores en un clúster. Las tareas y los servicios se pueden ejecutar en una infraestructura sin servidor administrada por AWS Fargate. Como alternativa, para tener más control sobre su infraestructura, puede ejecutar sus tareas y servicios en un clúster de EC2 instancias que administre.
- Amazon EFS: Amazon Elastic File System (Amazon EFS) ofrece un sistema de archivos NFS sencillo, escalable, elástico y completamente administrado que se utiliza con servicios de nube de AWS y recursos en las instalaciones.
- AWS CLI: la interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto para interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos. Con una configuración mínima, puede ejecutar comandos de la CLI de AWS que implementan una funcionalidad equivalente a la proporcionada por la consola de administración de AWS basada en navegador desde un símbolo del sistema.

Epics

Crear un sistema de archivos de Amazon EFS

Tarea	Descripción	Habilidades requeridas
Crear un sistema de archivos de Amazon EFS mediante la consola de administración de AWS.	1. **Note** Cree un sistema de archivos Amazon EFS y seleccione la VPC que incluye sus contenedores. : Si utiliza una VPC diferente, configure una conexión de	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	emparejamiento de VPC. 2. Anote el ID del sistema de archivos.	

Cree una definición de tarea de Amazon ECS mediante un sistema de archivos de Amazon EFS o la CLI de AWS.

Tarea	Descripción	Habilidades requeridas
Cree una definición de tarea mediante un sistema de archivos de Amazon EFS.	Cree una definición de tarea mediante la nueva consola Amazon ECS o la consola Amazon ECS clásica con las siguientes configuraciones: • Si utilizas la nueva consola, elige Amazon EC2 instances for App Environment. Si usa la consola clásica, elija EC2el tipo de lanzamiento. • Añada un volumen. Introduzca un nombre para el volumen, seleccione EFS como tipo de volumen y, a continuación, seleccione el ID del sistema de archivos que indicó anteriormente. Para el directorio raíz, seleccione la ruta del sistema de archivos Amazon EFS que	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	desee alojar en el host de contenedores de Amazon ECS.	

Tarea	Descripción	Habilidades requeridas

Cree una definición de tarea utilizando la CLI de AWS.	1. Para crear una plantilla de JSON con marcadores de posición de parámetros de entrada para la definició n de tareas, ejecute el siguiente comando:
	`aws ecs register-task-definition --generate-cli-skeleton`
	2. Para crear la definición de tareas con la plantilla de JSON, ejecute el siguiente comando:
	`aws ecs register-task-definition --cli-input-json file://<path_to_your_json_file>`
	3. **Note**
	Introduzca los parámetros de entrada en su plantilla JSON en función del archivo `task_definition_parameters.json` (adjunto). : Para obtener más información sobre los parámetros de
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	entrada, consulte Parámetros de definición de tareas (documentación de Amazon ECS) y register-task-definition(Referencia de comandos de la CLI de AWS).	

Recursos relacionados

- Definiciones de tareas de Amazon ECS
- Volúmenes de Amazon EFS

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Implementar funciones de Lambda con imágenes de contenedor

Ram Kandaswamy, Amazon Web Services

Resumen

AWS Lambda admite imágenes de contenedores como modelo de implementación. Este patrón muestra cómo implementar funciones de Lambda a través de imágenes de contenedor.

Lambda es un servicio de computación controlado por eventos sin servidor que permite ejecutar código para prácticamente cualquier tipo de aplicación o servicio de backend, sin aprovisionar ni administrar servidores. La compatibilidad con imágenes de contenedores para las funciones de Lambda le otorga hasta 10 GB de almacenamiento para el artefacto de la aplicación y la posibilidad de utilizar herramientas de desarrollo de imágenes de contenedores conocidas.

El ejemplo de este patrón usa Python como lenguaje de programación subyacente, pero puede usar otros lenguajes, como Java, Node.js o Go. Para la fuente, considere un sistema basado en Git como GitHub GitLab, o Bitbucket, o utilice Amazon Simple Storage Service (Amazon S3).

Requisitos previos y limitaciones

Requisitos previos

- Amazon Elastic Container Registry (Amazon ECR) activado
- Código de la aplicación
- Imágenes de Docker con el cliente de interfaz de tiempo de ejecución y la última versión de Python
- Conocimientos prácticos de Git

Limitaciones

- El máximo tamaño de imagen soportado es de 10 GB.
- El tiempo de ejecución máximo para una implementación de contenedores basada en Lambda es de 15 minutos.

Arquitectura

Arquitectura de destino

1. Cree un repositorio de Git y confirme el código de la aplicación en el repositorio.
2. El AWS CodeBuild proyecto se desencadena mediante la confirmación de cambios.
3. El CodeBuild proyecto crea la imagen de Docker y publica la imagen creada en Amazon ECR.
4. Cree una función de Lambda con la imagen de Amazon ECR.

Automatización y escala

Este patrón se puede automatizar mediante operaciones de API o mediante AWS CloudFormation el AWS Cloud Development Kit (AWS CDK) uso de operaciones de API desde un SDK. Lambda puede escalar automáticamente en función del número de solicitudes y se puede ajustar mediante los parámetros de simultaneidad. Para obtener más información, consulte la documentación de Lambda.

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormationAWS, CloudFormationhelps usted configura AWS los recursos, los aprovisiona de forma rápida y coherente y los administra a lo largo de su ciclo de vida en todo el Cuentas de AWS mundo Regiones de AWS. Este patrón utiliza AWS CloudFormation Application Composer, que le ayuda a ver y editar CloudFormation plantillas de forma visual.
- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

Otras herramientas

- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización a nivel del sistema operativo para entregar software en contenedores.
- GitHubGitLab, y Bitbucket son algunos de los sistemas de control de código fuente basados en Git más utilizados para realizar un seguimiento de los cambios en el código fuente.

Prácticas recomendadas

- Cree funciones lo más eficientes y pequeñas que sea posible para evitar la carga de archivos innecesarios.
- Trate de colocar las capas estáticas en la parte superior de la lista de archivos de Docker y coloque las capas que cambien con más frecuencia en la parte inferior. Esto mejora el almacenamiento en caché, lo que mejora el rendimiento.
- El propietario de la imagen es responsable de actualizar y parchear la imagen. Añada esa cadencia de actualización a sus procesos operativos. Para obtener más información, consulte la Documentación de AWS Lambda.

Epics

Crea un proyecto en CodeBuild

Tarea	Descripción	Habilidades requeridas
Cree un repositorio de Git.	Cree un repositorio de Git que contendrá el código fuente de la aplicación, el Dockerfile y el archivo `buildspec.yaml` .	Desarrollador
Crea un CodeBuild proyecto.	Para usar un CodeBuild proyecto para crear la imagen Lambda personalizada, haga lo siguiente: 1. Inicie sesión en y abra Consola de administración de AWS la CodeBuild consola en https://c onsole.aws.amazon.com/ codesuite/ codebuild/. 2. Cree un nuevo proyecto de . Como origen, elija el repositorio de Git que creó. Para obtener información	Desarrollador

Tarea	Descripción	Habilidades requeridas
	sobre los diferentes tipos de integración de repositorios de Git, consulte la documentación sobre cómo trabajar con conexiones. 3. Confirme que el modo con privilegios esté habilitado. Esto es necesario para compilar imágenes de Docker. De lo contrario, la imagen no se compilará correctamente. 4. Proporcione valores para el nombre y la descripción del proyecto.	
Edite el Dockerfile.	El Dockerfile debe estar ubicado en el directorio de nivel superior en el que se está desarrollando la aplicación. El código de Python debe estar en la carpeta `src`. Al crear la imagen, utilice las imágenes oficiales compatibles con Lambda. De lo contrario, se producirá un error de arranque que dificultará el proceso de empaquetado. Para obtener más información, consulte la sección Información adicional.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Cree un repositorio en Amazon ECR.	Cree un repositorio de contenedores en Amazon ECR. En el siguiente comando de ejemplo, el nombre del repositorio creado es `cf-demo`: `aws ecr create-repository --cf-demo` Se hará referencia al repositorio en el archivo `buildspec.yaml` .	Administrador de AWS, desarrollador
Enviar la imagen a Amazon ECR.	Puede utilizarla CodeBuild para realizar el proceso de creación de imágenes. CodeBuild necesita permiso para interactuar con Amazon ECR y trabajar con S3. Como parte del proceso, la imagen de Docker se compila y envía al registro de Amazon ECR. Para obtener información sobre la plantilla y el código, consulte la sección Información adicional.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Verificar que la imagen está en el repositorio.	Para verificar que la imagen se encuentra en el repositorio, seleccione Repositorios en la consola de Amazon ECR. Si esa característica estaba activada en la configuración de Amazon ECR, la imagen debería aparecer en la lista, junto con etiquetas y los resultados de un informe de análisis de vulnerabilidades. Para obtener más información, consulte la documentación de AWS.	Desarrollador

Crear la función de Lambda para ejecutar la imagen

Tarea	Descripción	Habilidades requeridas
Crear la función de Lambda.	En la consola de Lambda, seleccione Crear función y, a continuación, seleccione Imagen de contenedor. Introduzca el nombre de la función y el URI de la imagen que se encuentra en el repositorio de Amazon ECR y, a continuación, seleccione Crear función. Para obtener más información, consulte la documentación de AWS Lambda.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Probar la función de Lambda.	Seleccione Probar para invocar y probar la función. Para obtener más información, consulte la documentación de AWS Lambda.	Desarrollador de aplicaciones

Resolución de problemas

Problema	Solución
La compilación no se está realizando correctamente.	1. Compruebe si el modo privilegiado está activado para el CodeBuild proyecto. 2. Asegúrese de que los comandos relacionados con Docker tengan los permisos necesarios. Se intenta añadir `sudo` a los comandos. 3. Compruebe que la función de IAM asociada CodeBuild tenga una política con las acciones adecuadas para interactuar con Amazon ECR, Amazon S3 y CloudWatch los registros.

Recursos relacionados

- Imágenes base para Lambda
- Ejemplo de Docker para CodeBuild
- Credenciales de paso temporales

Información adicional

Editar el Dockerfile

El siguiente código muestra los comandos que edita en el Dockerfile.

```
FROM public.ecr.aws/lambda/python:3.xx

# Copy function code
COPY app.py ${LAMBDA_TASK_ROOT}
COPY requirements.txt  ${LAMBDA_TASK_ROOT}

# install dependencies
RUN pip3 install --user -r requirements.txt

# Set the CMD to your handler (could also be done as a parameter override outside of
 the Dockerfile)
CMD [ "app.lambda_handler" ]
```

En el comando `FROM`, utilice el valor adecuado para la versión de Python compatible con Lambda (por ejemplo, `3.12`). Será la imagen base que estará disponible en el repositorio público de imágenes de Amazon ECR.

El comando `COPY app.py ${LAMBDA_TASK_ROOT}` copia el código en el directorio raíz de la tarea, que la función de Lambda utilizará. Este comando usa la variable de entorno, por lo que no hay que preocuparse por la ruta real. La función que se va a ejecutar se pasa como argumento al comando `CMD [ "app.lambda_handler" ]`.

El comando `COPY requirements.txt` captura las dependencias necesarias para el código.

El comando `RUN pip install --user -r requirements.txt` instala las dependencias en el directorio de usuarios local.

Para compilar su imagen, ejecute el siguiente comando.

```
docker build -t <image name> .
```

Cómo añadir la imagen en Amazon ECR

En el siguiente código, sustituya `aws_account_id` por el número de cuenta, y sustituya `us-east-1` si utiliza una región diferente. El `buildspec` archivo usa el número de CodeBuild compilación para identificar de forma exclusiva las versiones de las imágenes como un valor de etiqueta. Puede cambiarlo para adaptarlo a sus necesidades.

El código personalizado de buildspec

```
phases:
```

```
  install:
    runtime-versions:
       python: 3.xx
  pre_build:
    commands:
      - python3 --version
      - pip3 install --upgrade pip
      - pip3 install --upgrade awscli
      - sudo docker info
  build:
    commands:
      - echo Build started on `date`
      - echo Building the Docker image...
      - ls
      - cd app
      - docker build -t cf-demo:$CODEBUILD_BUILD_NUMBER .
      - docker container ls
  post_build:
    commands:
      - echo Build completed on `date`
      - echo Pushing the Docker image...
      - aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin aws_account_id.dkr.ecr.us-east-1.amazonaws.com
      - docker tag cf-demo:$CODEBUILD_BUILD_NUMBER aws_account_id.dkr.ecr.us-
east-1.amazonaws.com/cf-demo:$CODEBUILD_BUILD_NUMBER
      - docker push aws_account_id.dkr.ecr.us-east-1.amazonaws.com/cf-demo:
$CODEBUILD_BUILD_NUMBER
```

Implementar microservicios de Java en Amazon ECS con AWS Fargate

Vijay Thompson y Sandeep Bondugula, Amazon Web Services

Resumen

Este patrón proporciona orientación para implementar microservicios de Java en contenedores en Amazon Elastic Container Service (Amazon ECS) mediante AWS Fargate. El patrón no utiliza Amazon Elastic Container Registry (Amazon ECR) para la administración de contenedores; en su lugar, las imágenes de Docker se extraen de un hub de Docker.

Requisitos previos y limitaciones

Requisitos previos

- Una aplicación de microservicios de Java existente en un hub de Docker
- Un repositorio público de Docker
- Una cuenta de AWS activa
- Conocimientos de los servicios de AWS, incluyendo Amazon ECS y Fargate
- Marco Docker, Java y Spring Boot
- Amazon Relational Database Service (Amazon RDS) en funcionamiento (opcional)
- Una nube privada virtual (VPC) si la aplicación requiere Amazon RDS (opcional)

Arquitectura

Pila de tecnología de origen

- Microservicios de Java (por ejemplo, implementados en Spring Boot) e implementados en Docker

Arquitectura de origen

Pila de tecnología de destino

- Un clúster de Amazon ECS que aloja cada microservicio mediante Fargate
- Una red de VPC para alojar el clúster de Amazon ECS y los grupos de seguridad asociados
- Una cluster/task definición para cada microservicio que hace girar contenedores mediante Fargate

Arquitectura de destino

Tools (Herramientas)

Herramientas

- Amazon ECS elimina la necesidad de instalar y operar su propio software de orquestación de contenedores, administrar y escalar un clúster de máquinas virtuales o programar contenedores en esas máquinas virtuales.
- AWS Fargate le ayuda a ejecutar contenedores sin necesidad de administrar servidores o instancias de Amazon Elastic Compute Cloud EC2 (Amazon). Se utiliza en conjunto con Amazon Elastic Container Service (Amazon ECS).
- Docker es una plataforma de software que le permite compilar, probar e implementar aplicaciones de forma rápida. Docker agrupa el software en unidades estandarizadas denominadas contenedores que contienen todo lo que el software necesita para ejecutarse, incluyendo las bibliotecas, las herramientas del sistema, el código y el tiempo de ejecución.

Código de Docker

El siguiente Dockerfile especifica la versión del kit de desarrollo de Java (JDK) que se utiliza, dónde se encuentra el archivo de almacenamiento Java (JAR), el número de puerto que está expuesto y el punto de entrada a la aplicación.

```
FROM openjdk:11
ADD target/Spring-docker.jar Spring-docker.jar
EXPOSE 8080
ENTRYPOINT ["java","-jar","Spring-docker.jar"]
```

Epics

Crear nuevas definiciones de tareas

Tarea	Descripción	Habilidades requeridas
Cree una definición de tarea.	Para ejecutar contenedores de Docker en Amazon ECS, se requiere una definición	Administrador de sistemas de AWS, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	de tareas. Abra la consola de Amazon ECS en https://console.aws.amazon.com/ecs/, elija Definiciones de tareas y, a continuación, cree una nueva definición de tarea. Para obtener más información, consulte la documentación de Amazon ECS.	
Seleccione el tipo de lanzamiento.	Seleccione Fargate como tipo de lanzamiento.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Configure la tarea.	Defina un nombre de tarea y configure la aplicación con la cantidad adecuada de memoria de tareas y CPU.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Defina el contenedor.	Especifique el nombre del contenedor. Para la imagen, introduzca el nombre del sitio de Docker, el nombre del repositorio y el nombre de la etiqueta de la imagen de Docker (`docker.io/sample-repo/sample-application:sample-tag-name`). Establezca los límites de memoria para la aplicación y establezca las asignaciones de puertos (`8080, 80`) para los puertos permitidos.	Administrador de sistemas de AWS, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Cree la tarea.	Cuando las configuraciones de la tarea y el contenedor se hayan establecido, cree la tarea. Para obtener instrucciones detalladas, consulte los enlaces de la sección Recursos relacionados.	Administrador de sistemas de AWS, desarrollador de aplicaciones

Configure el clúster

Tarea	Descripción	Habilidades requeridas
Crear y configurar un clúster.	Seleccione Solo redes como tipo de clúster, configure el nombre y, a continuación, cree el clúster o utilice un clúster existente si está disponible. Para obtener más información, consulte la documentación de Amazon ECS.	Administrador de sistemas de AWS, desarrollador de aplicaciones

Configurar la tarea

Tarea	Descripción	Habilidades requeridas
Cree una tarea de .	Dentro del clúster, seleccione Ejecutar nueva tarea.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Seleccione el tipo de lanzamiento.	Seleccione Fargate como tipo de lanzamiento.	Administrador de sistemas de AWS, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Seleccione la definición de la tarea, la revisión y la versión de la plataforma.	Seleccione la tarea que desee ejecutar, la revisión de la definición de la tarea y la versión de la plataforma.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Seleccione el clúster.	Seleccione el clúster desde el que desea ejecutar la tarea.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Especifique el número de tareas.	Configure el número de tareas que deben ejecutarse. Si lo inicia con dos o más tareas, necesitará un equilibrador de carga para distribuir el tráfico entre las tareas.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Especifique el grupo de tareas.	(Opcional) Especifique un nombre de grupo de tareas para identificar un conjunto de tareas relacionadas como grupo de tareas.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Configure la VPC del clúster, las subredes y los grupos de seguridad.	Configure la VPC del clúster y las subredes en las que desea implementar la aplicación. Cree o actualice grupos de seguridad (HTTP, HTTPS y puerto 8080) para proporcio nar acceso a las conexiones entrantes y salientes.	Administrador de sistemas de AWS, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Configure los ajustes de la IP pública.	Active o desactive la IP pública, en función de si desea utilizar una dirección IP pública para las tareas de Fargate. La opción predeterminada recomendada es Habilitada.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Revisar la configuración y crear la tarea	Revise la configuración y, a continuación seleccione Ejecutar tarea.	Administrador de sistemas de AWS, desarrollador de aplicaciones

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Copie la URL de la aplicación.	Cuando el estado de la tarea se haya actualizado a En ejecución, seleccione la tarea. En la sección Redes, copie la IP pública.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Pruebe su aplicación.	En su navegador, introduzc a la IP pública para probar la aplicación.	Administrador de sistemas de AWS, desarrollador de aplicaciones

Recursos relacionados

- Conceptos básicos de Docker para Amazon ECS (documentación de Amazon ECS)
- Amazon ECS en AWS Fargate (documentación de Amazon ECS)
- Creación de una definición de tarea (documentación de Amazon ECS)
- Creación de un clúster (documentación de Amazon ECS)
- Configuración de los parámetros básicos del servicio (documentación de Amazon ECS)

- Configuración de una red (documentación de Amazon ECS)
- Implementación de microservicios de Java en Amazon ECS (entrada del blog)

Implementar recursos y paquetes de Kubernetes con Amazon EKS y un repositorio de gráficos de Helm en Amazon S3

Sagar Panigrahi, Amazon Web Services

Resumen

Este patrón le ayuda a administrar las aplicaciones de Kubernetes de forma eficiente, independientemente de su complejidad. El patrón integra Helm en sus canalizaciones de integración y entrega continuas (CI/CD) existentes para implementar aplicaciones en un clúster de Kubernetes. Helm es un administrador de paquetes de Kubernetes que le ayuda a gestionar las aplicaciones de Kubernetes. Los gráficos de Helm le ayudan a definir, instalar y actualizar aplicaciones complejas de Kubernetes. Los gráficos se pueden versionar y almacenar en repositorios de Helm, lo que mejora el tiempo medio de restauración (MTTR) durante las interrupciones.

Este patrón utiliza Amazon Elastic Kubernetes Service (Amazon EKS) para el clúster de Kubernetes. Utiliza Amazon Simple Storage Service (Amazon S3) como repositorio de gráficos de Helm, de modo que todos los desarrolladores de la organización puedan gestionar y acceder a los gráficos de forma centralizada.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa con una nube privada virtual (VPC)
- Un clúster de Amazon EKS
- Nodos de trabajo configurados dentro del clúster de Amazon EKS y preparados para soportar cargas de trabajo
- Kubectl para configurar el archivo kubeconfig de Amazon EKS para el clúster de destino en la máquina cliente
- Acceso de AWS Identity and Access Management (IAM) para crear el bucket de S3
- Acceso de IAM (mediante programación o de rol) a Amazon S3 desde la máquina cliente
- Gestión del código fuente y CI/CD canalización

Limitaciones

- En este momento, no se admite la actualización, la eliminación o la administración de definiciones de recursos personalizadas (CRDs).
- Si utiliza un recurso que hace referencia a una CRD, la CRD debe instalarse por separado (fuera del gráfico).

Versiones de producto

- Helm v3.6.3

Arquitectura

Pila de tecnología de destino

- Amazon EKS
- Amazon VPC
- Amazon S3
- Gestión de código fuente
- Helm
- Kubectl

Arquitectura de destino

Automatización y escala

- AWS se CloudFormation puede utilizar para automatizar la creación de la infraestructura. Para obtener más información, consulte Creación de recursos de Amazon EKS con AWS CloudFormation en la documentación de Amazon EKS.
- Helm se incorporará a su herramienta de CI/CD automatización existente para automatizar el empaquetado y el control de versiones de los gráficos de Helm (algo fuera del alcance de este patrón).
- GitVersion o bien, se pueden utilizar los números de compilación de Jenkins para automatizar el control de versiones de los gráficos.

Tools (Herramientas)

Herramientas

- Amazon EKS: Amazon Elastic Kubernetes Service (Amazon EKS) es un servicio administrado para ejecutar Kubernetes en AWS sin necesidad de crear ni mantener su propio plano de control de Kubernetes. Kubernetes es un sistema de código abierto para automatizar la implementación, el escalado y la administración de las aplicaciones en contenedores.
- Helm: Helm es un administrador de paquetes para Kubernetes que le ayuda a instalar y administrar aplicaciones en su clúster de Kubernetes.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web.
- Kubectl: Kubectl es una utilidad de la línea de comandos para la ejecución de comandos en clústeres de Kubernetes.

Código

Se adjunta el código de ejemplo.

Epics

Configurar e inicializar Helm

Tarea	Descripción	Habilidades requeridas
Instalar el cliente Helm.	Para descargar e instalar el cliente Helm en su sistema local, utilice el siguiente comando. `sudo curl https://raw.githubusercontent.com/helm/helm/master/scripts/get-helm-3 | bash`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Validar la instalación de Helm.	Para validar que Helm puede comunicarse con el servidor API de Kubernetes del clúster de Amazon EKS, ejecute `helm version`.	DevOps ingeniero

Crear e instalar un gráfico de Helm en el clúster de Amazon EKS

Tarea	Descripción	Habilidades requeridas
Crear un gráfico de Helm para NGINX.	Para crear un gráfico de Helm llamado `my-nginx` en la máquina cliente, ejecute `helm create my-nginx`.	DevOps ingeniero
Revisar la estructura del gráfico.	Para revisar la estructura del gráfico, ejecute el comando tree `tree my-nginx/` .	DevOps ingeniero
Desactive la creación de cuentas de servicio en el gráfico.	En `values.yaml` , en la sección `serviceAccount` , establezca la clave `create` en `false`. Esta opción está desactivada porque no es necesario crear una cuenta de servicio para este patrón.	DevOps ingeniero
Validar (lint) el gráfico modificado para detectar errores sintácticos.	Para validar el gráfico para detectar cualquier error sintáctico antes de instalarl o en el clúster de destino, ejecute `helm lint my-nginx/` .	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Instale el gráfico para implementar los recursos de Kubernetes.	Para ejecutar la instalación del gráfico de Helm, utilice el siguiente comando. `helm install --name my-nginx-release --debug my-nginx/ --namespace helm-space` La marca opcional `debug` muestra todos los mensajes de depuración durante la instalación. La marca `namespace` especifica el espacio de nombres en el que se creará la parte de recursos de este gráfico.	DevOps ingeniero
Revisar los recursos del clúster de Amazon EKS.	Para revisar los recursos que se crearon como parte del gráfico de Helm en el espacio de nombres `helm-space` , utilice el siguiente comando. `kubectl get all -n helm-space`	DevOps ingeniero

Restaurar una versión anterior de una aplicación de Kubernetes

Tarea	Descripción	Habilidades requeridas
Modifique y actualice la versión.	Para modificar el gráfico, en `values.yaml` , cambie el valor `replicaCount` a 2. A continuación, ejecute	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	el siguiente comando para actualizar la versión ya instalada. `helm upgrade my-nginx-release my-nginx/ --namespace helm-space`	
Revisar el historial de la versión de Helm.	Para ver todas las revisiones de una versión específica instalada con Helm, ejecute el siguiente comando. `helm history my-nginx-release`	DevOps ingeniero
Comprobar los detalles de una revisión específica.	Antes de cambiar a o restaurar una versión operativa, y para obtener una capa adicional de validación antes de instalar una revisión, compruebe qué valores se han pasado a cada una de las revisiones mediante el siguiente comando. `helm get --revision=2 my-nginx-release`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Restaurar una versión anterior.	Para restaurar una revisión anterior, utilice el siguiente comando. `helm rollback my-nginx-release 1` Este ejemplo restaura la revisión número 1.	DevOps ingeniero

Inicializar un bucket de S3 como repositorio de Helm

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3 para gráficos de Helm.	Cree un bucket de S3 único. En el bucket, cree una carpeta llamada `charts`. El ejemplo de este patrón usa `s3://my-helm-charts/charts` como repositorio de gráficos de destino.	Administrador de la nube
Instalar el complemento de Helm para Amazon S3.	Para instalar el complemento helm-s3 en su máquina cliente, utilice el siguiente comando. `helm plugin install https://github.com/hypnoglow/helm-s3.git --version 0.10.0` Nota: El soporte de Helm V3 está disponible con la	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	versión 0.9.0 y superior del complemento.	
Inicializar el repositorio de Helm de Amazon S3.	Para inicializar la carpeta de destino como repositorio de Helm, utilice el siguiente comando. `helm S3 init s3://my-helm-charts/charts` El comando crea un archivo `index.yaml` en el destino para rastrear toda la información del gráfico almacenada en esa ubicación.	DevOps ingeniero
Añada el repositorio de Amazon S3 a Helm.	Para añadir el repositorio a la máquina cliente, utilice el siguiente comando. `helm repo add my-helm-charts s3://my-helm-charts/charts` Este comando añade un alias al repositorio de destino de la máquina cliente de Helm.	DevOps ingeniero
Revisar la lista de repositorios.	Para ver la lista de repositorios de la máquina cliente de Helm, ejecute `helm repo list`.	DevOps ingeniero

Empaquetar y almacenar gráficos en el repositorio de Helm de Amazon S3

Tarea	Descripción	Habilidades requeridas
Empaquetar el gráfico.	Para empaquetar el gráfico `my-nginx` que creó, ejecute `helm package ./my-nginx/` . El comando empaqueta todo el contenido de la carpeta de gráficos `my-nginx` en un archivo de almacenamiento que se nombra según el número de versión mencionado en el archivo `Chart.yaml` .	DevOps ingeniero
Almacenar el paquete en el repositorio de Helm de Amazon S3.	Para cargar el paquete en el repositorio de Helm de Amazon S3, ejecute el siguiente comando usando el nombre correcto del archivo `.tgz`. `helm s3 push ./my-nginx-0.1.0.tgz my-helm-charts`	DevOps ingeniero
Buscar el gráfico de Helm.	Para confirmar que el gráfico aparece tanto localmente como en el repositorio de Helm de Amazon S3, ejecute el siguiente comando. `helm search repo my-nginx`	DevOps ingeniero

Modificar, versionar y empaquetar un gráfico

Tarea	Descripción	Habilidades requeridas
Modifique y empaquete el gráfico.	En `values.yaml` , defina el valor de `replicaCount` en 1. A continuación, ejecute `helm package ./my-nginx/` para empaquetar el gráfico, esta vez cambiando la versión en `Chart.yaml` a `0.1.1`. Lo ideal es actualizar el control de versiones mediante la automatización mediante herramientas como GitVersion los números de compilación de Jenkins en un CI/CD proceso. La automatización del número de versión está fuera del alcance de este patrón.	DevOps ingeniero
Enviar la nueva versión al repositorio de Helm de Amazon S3.	Para enviar el nuevo paquete, versión 0.1.1, al repositorio de Helm `my-helm-charts` de Amazon S3, ejecute el siguiente comando. `helm s3 push ./my-nginx-0.1.1.tgz my-helm-charts`	DevOps ingeniero

Buscar e instalar un gráfico en el repositorio de Helm de Amazon S3

Tarea	Descripción	Habilidades requeridas
Buscar todas las versiones del gráfico my-nginx.	Para ver todas las versiones disponibles de un gráfico, ejecute el siguiente comando con la marca `--versions` . `helm search repo my-nginx --versions` Sin la marca, Helm mostrará de forma predeterminada la última versión cargada de un gráfico.	DevOps ingeniero
Instalar un gráfico desde el repositorio de Helm de Amazon S3.	Los resultados de búsqueda de la tarea anterior mostrarán las múltiples versiones del gráfico `my-nginx`. Para instalar la nueva versión (0.1.1) desde el repositorio de Helm de Amazon S3, utilice el siguiente comando. `helm upgrade my-nginx-release my-helm-charts/my-nginx --version 0.1.1 --namespace helm-space`	DevOps ingeniero

Recursos relacionados

- Documentación de HELM
- Complemento helm-s3 (licencia MIT)
- Binario del cliente HELM

- Documentación de Amazon EKS

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Implemente un clúster de CockroachDB en Amazon EKS mediante Terraform

Sandip Gangapadhyay y Kalyan Senthilnathan, Amazon Web Services

Resumen

Este patrón proporciona un módulo HashiCorp Terraform para implementar un clúster CockroachDB de varios nodos en Amazon Elastic Kubernetes Service (Amazon EKS) mediante el operador CockroachDB. CockroachDB es una base de datos SQL distribuida que proporciona fragmentación horizontal automática, alta disponibilidad y un rendimiento uniforme en clústeres distribuidos geográficamente. Este patrón usa Amazon EKS como plataforma de Kubernetes administrada e implementa cert-manager para la comunicación de nodos segura por TLS. También utiliza un Network Load Balancer para la distribución del tráfico y crea CockroachDB StatefulSetscon módulos que replican automáticamente los datos para garantizar la tolerancia a los errores y el rendimiento.

Destinatarios previstos

Para implementar este patrón, le recomendamos que se familiarice con lo siguiente:

- HashiCorp Conceptos y prácticas de infraestructura como código (IaC) de Terraform
- Servicios de AWS, en particular Amazon EKS
- Los aspectos básicos de Kubernetes StatefulSets, incluidos los operadores y las configuraciones de los servicios
- Bases de datos SQL distribuidas
- Conceptos de seguridad, como la gestión de certificados TLS.
- DevOps prácticas, CI/CD flujos de trabajo y automatización de infraestructuras

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Permisos para implementar recursos en un clúster de Amazon EKS
- Un clúster de Amazon EKS versión 1.23 o posterior, con los nodos etiquetados `node=cockroachdb`

- Controlador de la interfaz de almacenamiento de contenedores (CSI) de Amazon Elastic Block Store, versión 1.19.0 o posterior, instalado en el clúster Amazon EKS
- Terraform CLI versión 1.0.0 o posterior, instalada
- kubectl, instalado
- Git, instalado
- AWS Command Line Interface (AWS CLI) versión 2.9.18 o posterior, instalada y configurada

Limitaciones

- El operador Kubernetes de CockroachDB no admite varios clústeres de Kubernetes para despliegues en varias regiones. Para más limitaciones, consulte Cómo organizar CockroachDB en varios clústeres de Kubernetes (documentación de CockroachDB) y CockroachDB Kubernetes Operator (). GitHub
- Actualmente, la eliminación automática PVCs de las notificaciones por volumen persistentes () está deshabilitada de forma predeterminada. Esto significa que, tras desmantelar y retirar un nodo, el operador no eliminará el volumen persistente que estaba montado en su módulo. Para obtener más información, consulte Eliminación automática de PVC en la documentación de CockroachDB.

Versiones de producto

- CockroachDB versión 22.2.2

Arquitectura

Arquitectura de destino

El siguiente diagrama muestra una implementación de CockroachDB de alta disponibilidad en tres zonas de AWS disponibilidad dentro de una nube privada virtual (VPC). Los pods CockroachDB se administran a través de Amazon EKS. La arquitectura ilustra cómo los usuarios acceden a la base de datos a través de un Network Load Balancer, que distribuye el tráfico a los pods de CockroachDB. Los pods se ejecutan en instancias de Amazon Elastic Compute Cloud (Amazon EC2) en cada zona de disponibilidad, lo que proporciona resiliencia y tolerancia a errores.

Recursos creados

Al implementar el módulo Terraform utilizado en este patrón, se crean los siguientes recursos:

1. Network Load Balancer: este recurso sirve como punto de entrada para las solicitudes de los clientes y distribuye el tráfico de manera uniforme entre las instancias de CockroachDB.
2. CockroachDB StatefulSet: StatefulSet define el estado deseado de la implementación de CockroachDB dentro del clúster de Amazon EKS. Administra el despliegue ordenado, el escalado y las actualizaciones de los pods de CockroachDB.
3. Módulos CockroachDB: estos pods son instancias de CockroachDB que se ejecutan como contenedores dentro de los pods de Kubernetes. Estos pods almacenan y administran los datos en el clúster distribuido.
4. Base de datos CockroachDB: se trata de la base de datos distribuida que administra CockroachDB y que abarca varios módulos. Replica los datos para garantizar una alta disponibilidad, tolerancia a errores y rendimiento.

Tools (Herramientas)

Servicios de AWS

- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar Servicios de AWS mediante comandos en su shell de línea de comandos.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar AWS Kubernetes sin necesidad de instalar o mantener su propio plano de control o nodos de Kubernetes.

Otras herramientas

- HashiCorp Terraform es una herramienta de infraestructura como código (IaC) que facilita usar el código para aprovisionar y administrar los recursos y la infraestructura en la nube.
- kubectl: una interfaz de la línea de comandos que le ayuda en la ejecución de comandos en clústeres de Kubernetes.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub Deploy a CockroachDB en Amazon EKS mediante Terraform. El repositorio de código contiene los siguientes archivos y carpetas para Terraform:

- `modules`carpeta: esta carpeta contiene el módulo Terraform para CockroachDB

- `main`carpeta: esta carpeta contiene el módulo raíz que llama al módulo secundario de CockroachDB para crear el clúster de base de datos de CockroachDB.

Prácticas recomendadas

- No reduzca la escala a menos de tres nodos. Esto se considera un antipatrón en CockroachDB y puede provocar errores. Para obtener más información, consulte el escalado de clústeres en la documentación de CockroachDB.
- Implemente el escalado automático de Amazon EKS mediante Karpernter o Cluster Autoscaler. Esto permite que el clúster de CockroachDB se escale horizontalmente y que los nuevos nodos se creen automáticamente. Para más información, consulte Escalado de computación en clústeres ´con Karpenter y Cluster Autoscaler en la documentación de Amazon EKS.

> **Note**
>
> Debido a la regla de programación de `podAntiAffinity` Kubernetes, solo se puede programar un pod de CockroachDB en un nodo de Amazon EKS.

- Para conocer las prácticas recomendadas de seguridad de Amazon EKS, consulte Prácticas recomendadas de seguridad en la documentación de Amazon EKS.
- Para conocer las prácticas recomendadas de rendimiento de SQL para CockroachDB, consulte las prácticas recomendadas de rendimiento de SQL en la documentación de CockroachDB.
- Para obtener más información sobre cómo configurar un backend remoto de Amazon Simple Storage Service (Amazon S3) para el archivo de estado de Terraform, consulte Amazon S3 en la documentación de Terraform.

Epics

Configure su entorno

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código.	Introduzca el siguiente comando para clonar el repositorio:	DevOps ingeniero, Git

Tarea	Descripción	Habilidades requeridas
	`git clone https://github.com/aws-samples/crdb-cluster-eks-terraform.git`	
Actualice las variables de Terraform.	1. Ingresa el siguiente comando para navegar a la carpeta principal del repositorio clonado: `cd crdb-cluster-eks-terraform/main` 2. Abre el archivo variable.tf. 3. Configure el valor predeterminado para las siguientes variables: • `region`— Introduzca el objetivo Región de AWS • `eks_cluster_name` — Introduzca el nombre del clúster Amazon EKS de destino • `number_of_nodes` — Introduzca el número de nodos que se van a implementar 4. Guarde y cierre el archivo variable.tf.	DevOps ingeniero, Terraform

Implementación de recursos

Tarea	Descripción	Habilidades requeridas

Implemente la infraestructura.	1. Ingresa el siguiente comando para inicializar el despliegue de Terraform:
	`terraform init`
	2. Introduzca el comando siguiente para generar un plan de ejecución:
	`terraform plan`
	3. Revise el plan y valide los recursos y los component es de infraestructura que se van a crear.
	4. Introduzca el siguiente comando para implementar la infraestructura:
	`terraform apply`
	5. Cuando se le solicite, introduzca sí para confirmar la implementación.
	6. Espere hasta que se complete la implement ación.
		DevOps ingeniero, Terraform

Verifique la implementación

Tarea	Descripción	Habilidades requeridas

Verificar la creación de recursos.	1. Introduzca el siguiente comando para configurar el contexto de Amazon EKS mediante AWS CLI:
	`aws eks update-kubeconfig –name <eks_cluster_name>`
	2. Introduzca el siguiente comando para verificar el número de pods que utilizan CockroachDB:
	`kubectl get pods -n <namespace>`
	A continuación, se muestra un ejemplo de la salida.
	`NAME READY STATUS RESTARTS AGE cockroach-operator-655fbf7847-zn9v8 1/1 Running 0 30m cockroachdb-0 1/1 Running 0 24m cockroachdb-1 1/1 Running 0 24m`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`cockroachdb-2 1/1 Running 0 24m` 3. Compruebe que la cantidad de pods coincida con el valor que definió en el archivo variable.tf.	
(Opcional) Amplíe o reduzca la escala.	1. En el archivo variable.tf, aumente o disminuya el número de nodos y, a continuación, guarde el archivo. 2. Repita los pasos para implementar la infraestructura a través de Terraform. Terraform agrega o elimina cápsulas. 3. Repita los pasos para verificar la cantidad de cápsulas que utilizan Cockroach DB. Por ejemplo, si aumentaste el número de nodos de tres a cuatro, ahora deberías ver cuatro pods en ejecución.	DevOps ingeniero, Terraform

Limpieza

Tarea	Descripción	Habilidades requeridas
Configurar la infraestructura.	Escalar los nodos para `0` reducir los costos de	Terraform

Tarea	Descripción	Habilidades requeridas
	cómputo. Sin embargo, seguirá incurriendo en cargos por los volúmenes persisten tes de Amazon EBS que creó este módulo. Para eliminar los costes de almacenamiento, siga estos pasos para eliminar todos los volúmenes: 1. Introduzca el siguiente comando para eliminar la infraestructura: `terraform destroy` 2. Cuando se le solicite, introduzca sí para confirmar .	

Resolución de problemas

Problema	Solución
Error al validar las credenciales del proveedor	Al ejecutar Terraform `apply` o el `destroy` comando, es posible que aparezca el siguiente error: `Error: configuring Terraform AWS Provider: error validatin g provider credentials: error calling sts:GetCallerIdentity: operation error STS: GetCaller Identity, https response error StatusCode: 403, RequestID: 123456a9-fbc1-40ed-b8d8-513`

Problema	Solución
	`d0133ba7f, api error InvalidClientTokenId: The security token included in the request is invalid.` Este error se debe a la caducidad del token de seguridad de las credenciales usadas en la configuración de la máquina local. Para obtener instrucciones sobre cómo resolver el error, consulte Establecer y ver los ajustes de configuración en la AWS CLI documentación.

Problema	Solución
Los pods de CockroachDB están en estado pendiente	1. Debido a la regla de programación de `podAntiAffinity` Kubernetes, solo se puede programar un pod de CockroachDB en un nodo de Amazon EKS. Si el número de pods de CockroachDB supera el número de nodos de Amazon EKS disponibles, es posible que los pods de CockroachDB estén en estado pendiente. En ese caso, debe implementar Cluster Autoscaler o Karpenter para que el nodo de Amazon EKS se escale automáticamente. Para obtener más información, consulte Escalar la computación en clústeres con Karpenter y Cluster Autoscaler. 2. Para comprobar si los nodos de trabajo de Kubernetes tienen `node=cockroachdb` etiquetas, introduce el siguiente comando: `kubectl get nodes --show-labels` Si no lo están, asegúrate de que todos los nodos de trabajo estén correctamente etiquetados. Para obtener más información, consulte Editar la configuración de un grupo de nodos en la documentación de Amazon EKS.

Recursos relacionados

- Implemente CockroachDB en un único clúster de Kubernetes (documentación de CockroachDB)
- Organice CockroachDB en varios clústeres de Kubernetes (documentación de CockroachDB)
- AWS Proveedor (documentación de Terraform)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Implemente un microservicio Java de muestra en Amazon EKS y exponga el microservicio mediante un Equilibrador de carga de aplicación

Vijay Thompson y Akkamahadevi Hiremath, Amazon Web Services

Resumen

Este patrón describe cómo implementar un microservicio Java de muestra como una aplicación en contenedores en Amazon Elastic Kubernetes Service (Amazon EKS) mediante la utilidad de línea de comandos `eksctl` y Amazon Elastic Container Registry (Amazon ECR). Puede usar un equilibrador de carga de aplicación para equilibrar la carga del tráfico de la aplicación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- La interfaz de la línea de comandos de AWS (AWS CLI) versión 1.7, instalada y configurada en Linux, macOS o Windows
- Un daemon de Docker en ejecución
- La utilidad de línea de comandos `eksctl`, instalada y configurada en macOS, Linux o Windows (para obtener más información, consulte Introducción a Amazon EKS — eksctl en la documentación de Amazon EKS).
- La utilidad de línea de comandos `kubectl`, instalada y configurada en macOS, Linux o Windows (para obtener más información, consulte Instalar o actualizar eksctl en la documentación de Amazon EKS).

Limitaciones

- Este patrón no cubre la instalación de un certificado SSL para el Equilibrador de carga de aplicación.

Arquitectura

Pila de tecnología de destino

- Amazon ECR

- Amazon EKS
- Elastic Load Balancing

Arquitectura de destino

El siguiente diagrama muestra una arquitectura para organizar en contenedores un microservicio Java en Amazon EKS.

Tools (Herramientas)

- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon Elastic Kubernetes Service (Amazon EKS) lo ayuda a ejecutar Kubernetes en AWS sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- Elastic Load Balancing distribuye automáticamente el tráfico entrante entre varios destinos, como instancias, contenedores y direcciones IP de Amazon Elastic Compute Cloud (Amazon EC2), en una o más zonas de disponibilidad.
- eksctl le ayuda a crear clústeres en Amazon EKS.
- kubectl permite ejecutar comandos en clústeres de Kubernetes.
- Docker le ayuda a crear, probar y entregar aplicaciones en paquetes llamados contenedores.

Epics

Crear un clúster de Amazon EKS mediante eksctl

Tarea	Descripción	Habilidades requeridas
Cree un clúster de Amazon EKS.	Para crear un clúster de Amazon EKS que utilice dos EC2 instancias de Amazon t2.small como nodos, ejecute el siguiente comando:	Desarrollador, administrador del sistema

Tarea	Descripción	Habilidades requeridas
	`eksctl create cluster --name <your-cluster-name> --version <version-number> --nodes=1 --node-type=t2.small` **Note** El proceso puede tardar entre 15 y 20 minutos. Una vez creado el clúster, se añade la configuración de Kubernetes adecuada al archivo kubeconfig. Puede usar el archivo `kubeconfig` con `kubectl` para implementar la aplicación en pasos posteriores.	
Verifique el clúster de Amazon EKS.	Para comprobar que se ha creado el clúster y que puede conectarse a él, ejecute el comando `kubectl get nodes`.	Desarrollador, administrador del sistema

Cree un repositorio de Amazon ECR y envíe la imagen de Docker.

Tarea	Descripción	Habilidades requeridas
Cree un repositorio de Amazon ECR.	Siga las instrucciones de Creación de un repositorio privado en la documentación de Amazon ECR.	Desarrollador, administrador del sistema
Cree un archivo XML POM.	Cree un archivo `pom.xml` basado en el ejemplo de código de archivo POM de la sección de información adicional de este patrón.	Desarrollador, administrador del sistema

Cree un archivo de origen.	Cree un archivo de origen llamado `HelloWorld.java` en la ruta `src/main/java/eksExample` según el siguiente ejemplo:
	`package eksExample;`
	`import static spark.Spark.get;`
	`public class HelloWorld {`
	`  public static void main(String[] args) {`
	`  get("/", (req, res) -> {`
	`  return "Hello World!";`
	`  });`
	`  }`
	`}`
	Asegúree de usar la siguiente estructura de directorios:	

Tarea	Descripción	Habilidades requeridas

	``
	### Dockerfile
	### deployment.yaml
	### ingress.yaml
	### pom.xml
	### service.yaml
	### src
	    ### main
	        ### java
	            ###
	 eksExample
	                ###
	 HelloWorld.java
	``	

Cree un Dockerfile.	Cree un archivo `Dockerfile` basado en el ejemplo de código de Dockerfile de la sección de información adicional de este patrón.	Desarrollador, administrador del sistema

Tarea	Descripción	Habilidades requeridas

Cree y envíe la imagen de Docker.	En el directorio en el que desee que su `Dockerfile` compile, etiquete y envie la imagen a Amazon ECR, ejecute los siguientes comandos:
	`aws ecr get-login -password --region <region>| docker login --username <username> --password-stdin <account_number>.dkr.ecr.<region>.amazonaws.com`
	`docker buildx build --platform linux/amd64 -t hello-world-java:v1 .`
	`docker tag hello-world-java:v1 <account_number>.dkr.ecr.<region>.amazonaws.com/<repository_name>:v1`
	`docker push <account_number>.dkr.ecr.<region>.amazonaws.com/<repository_name>:v1`
	Note
	Modifique la región de AWS, el número de cuenta y los detalles del repositorio en los comandos anteriores. Asegúrese de anotar la URL de la	

Tarea	Descripción	Habilidades requeridas
	imagen para usarla más adelante. **Important** Un sistema macOS con un chip M1 tiene problemas para crear una imagen que sea compatible con Amazon EKS que se ejecuta en una AMD64 plataforma. Para resolver este problema, utilice docker buildx para crear una imagen de Docker que funcione en Amazon EKS.	

Implemente los microservicios de Java

Tarea	Descripción	Habilidades requeridas
Cree un archivo implement ación.	Cree un archivo YAML llamado `deployment.yaml` basado en el ejemplo de código de archivo de implementación de la sección de información adicional de este patrón.	Desarrollador, administrador del sistema

Tarea	Descripción	Habilidades requeridas
	Note Utilice la URL de la imagen que copió anteriormente como ruta del archivo de imagen para el repositorio de Amazon ECR.	
Implemente los microservicios de Java en el clúster de Amazon EKS.	Para crear una implementación en su clúster de Amazon EKS, ejecute el comando `kubectl apply -f deployment.yaml` .	Desarrollador, administrador del sistema
Verifique el estado de los pods.	1. Para verificar el estado de los pods, ejecute el comando `kubectl get pods`. 2. Espere a que el estado cambie a Listo.	Desarrollador, administrador del sistema
Cree un servicio.	1. Cree un archivo llamado `service.yaml` basado en el ejemplo de código de archivo de servicio de la sección de información adicional de este patrón. 2. Ejecute el comando `kubectl apply -f service.yaml` .	Desarrollador, administrador del sistema

Tarea	Descripción	Habilidades requeridas
Instalación del complemento controlador del equilibrador de carga de AWS.	Siga las instrucciones de Instalación del complemento controlador del equilibrador de carga de AWS en la documentación de Amazon EKS. **Note** Debe tener el complemento instalado para crear un Equilibrador de carga de aplicación o un Equilibrador de carga de red para un servicio de Kubernetes.	Desarrollador, administrador del sistema
Cree un recurso de ingreso.	Cree un archivo YAML llamado `ingress.yaml` basado en el ejemplo de código de archivo de recurso de la sección de información adicional de este patrón.	Desarrollador, administrador del sistema
Cree un Equilibrador de carga de aplicación.	Para implementar el recurso de ingreso y crear un Equilibrador de carga de aplicación, ejecute el comando `kubectl apply -f ingress.yaml .`	Desarrollador, administrador del sistema

Pruebe la aplicación

Tarea	Descripción	Habilidades requeridas
Pruebe y verifique la aplicación.	1. Para obtener el nombre DNS del equilibrador de carga en el campo ADDRESS, ejecute el comando `kubectl get ingress.networking.k8s.io/java-microservice-ingress` . 2. En una EC2 instancia de la misma VPC que los nodos de Amazon EKS, ejecute el `curl -v <DNS address from previous command>` comando.	Desarrollador, administrador del sistema

Recursos relacionados

- Creación de un repositorio privado (documentación de Amazon ECR)
- Enviar una imagen de Docker (documentación de Amazon ECR)
- Controladores de ingreso (taller de Amazon EKS)
- Docker buildx (documentación de Docker)

Información adicional

Ejemplo de archivo POM

```
<?xml version="1.0" encoding="UTF-8"?>
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/
maven-4.0.0.xsd">
```

```
  <modelVersion>4.0.0</modelVersion>


  <groupId>helloWorld</groupId>
  <artifactId>helloWorld</artifactId>
  <version>1.0-SNAPSHOT</version>


  <dependencies>
    <dependency>
      <groupId>com.sparkjava</groupId><artifactId>spark-core</
artifactId><version>2.0.0</version>
    </dependency>
  </dependencies>
  <build>
    <plugins>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId><artifactId>maven-jar-plugin</
artifactId><version>2.4</version>
        <configuration><finalName>eksExample</finalName><archive><manifest>
              <addClasspath>true</addClasspath><mainClass>eksExample.HelloWorld</
mainClass><classpathPrefix>dependency-jars/</classpathPrefix>
            </manifest></archive>
        </configuration>
      </plugin>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId><artifactId>maven-compiler-plugin</
artifactId><version>3.1</version>
        <configuration><source>1.8</source><target>1.8</target></configuration>
      </plugin>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId><artifactId>maven-assembly-plugin</
artifactId>
        <executions>
          <execution>
            <goals><goal>attached</goal></goals><phase>package</phase>
            <configuration>
              <finalName>eksExample</finalName>
              <descriptorRefs><descriptorRef>jar-with-dependencies</descriptorRef></
descriptorRefs>
              <archive><manifest><mainClass>eksExample.HelloWorld</mainClass></
manifest></archive>
            </configuration>
          </execution>
```

```
        </executions>
      </plugin>
    </plugins>
  </build>
</project>
```

Ejemplo de Dockerfile

```
FROM bellsoft/liberica-openjdk-alpine-musl:17

RUN apk add maven
WORKDIR /code

# Prepare by downloading dependencies
ADD pom.xml /code/pom.xml
RUN ["mvn", "dependency:resolve"]
RUN ["mvn", "verify"]

# Adding source, compile and package into a fat jar
ADD src /code/src
RUN ["mvn", "package"]

EXPOSE 4567
CMD ["java", "-jar", "target/eksExample-jar-with-dependencies.jar"]
```

Ejemplo de archivo de implementación

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: microservice-deployment
spec:
  replicas: 2
  selector:
    matchLabels:
      app.kubernetes.io/name: java-microservice
  template:
    metadata:
      labels:
        app.kubernetes.io/name: java-microservice
    spec:
      containers:
      - name: java-microservice-container
```

```
        image: .dkr.ecr.amazonaws.com/:
        ports:
        - containerPort: 4567
```

Ejemplo de archivo de servicio

```
apiVersion: v1
kind: Service
metadata:
  name: "service-java-microservice"
spec:
  ports:
    - port: 80
      targetPort: 4567
      protocol: TCP
  type: NodePort
  selector:
    app.kubernetes.io/name: java-microservice
```

Ejemplo de archivo de recursos de ingreso

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: "java-microservice-ingress"
  annotations:
    kubernetes.io/ingress.class: alb
    alb.ingress.kubernetes.io/load-balancer-name: apg2
    alb.ingress.kubernetes.io/target-type: ip
  labels:
    app: java-microservice
spec:
  rules:
    - http:
        paths:
          - path: /
            pathType: Prefix
            backend:
              service:
                name: "service-java-microservice"
                port:
                  number: 80
```

Implemente una aplicación basada en gRPC en un clúster de Amazon EKS y acceda a ella con un Equilibrador de carga de aplicación

Kirankumar Chandrashekar y Huy Nguyen, Amazon Web Services

Resumen

Este patrón describe cómo alojar una aplicación basada en gRPC en un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) y cómo acceder a ella de forma segura a través de un Equilibrador de carga de aplicación.

gRPC es un marco de llamada a procedimientos remotos (RPC) de código abierto que se puede ejecutar en cualquier entorno. Puede usarlo para integraciones de microservicios y comunicaciones cliente-servidor. Para obtener más información sobre el gRPC, consulte la entrada del blog de AWS sobre el soporte del Application Load Balancer para end-to-end HTTP/2 y gRPC.

Este patrón le muestra cómo alojar una aplicación basada en gRPC que se ejecuta como pods de Kubernetes en Amazon EKS. El cliente gRPC se conecta a un Application Load Balancer a través del protocolo HTTP/2 con una conexión cifrada. SSL/TLS El Equilibrador de carga de aplicación reenvía el tráfico a la aplicación gRPC que se ejecuta en los pods de Amazon EKS. La cantidad de pods de gRPC se puede escalar automáticamente en función del tráfico mediante el escalador automático de pods horizontales de Kubernetes. El grupo de destino del equilibrador de carga de aplicación realiza comprobaciones de estado en los nodos de Amazon EKS, evalúa si el destino está en buen estado y solo reenvía el tráfico a los nodos en buen estado.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Docker, instalado y configurado en Linux, macOS o Windows.
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2, instalada y configurada en Linux, macOS o Windows.
- eksctl instalado y configurado en Linux, macOS o Windows.
- `kubectl`, instalado y configurado para acceder a los recursos de su clúster de Amazon EKS. Para más información, consulte Instalar o actualizar kubectl en la documentación de Amazon EKS.
- g RPCurl, instalado y configurado.

- Un clúster existente o nuevo de Amazon EKS. Para obtener más información, consulte Getting started with Amazon EKS.
- Su terminal de equipo está configurado para acceder al clúster de Amazon EKS. Para obtener más información, consulte Configuración del equipo para que se comunique con el clúster en la documentación de Amazon EKS.
- Controlador del equilibrador de carga de AWS, aprovisionado en el clúster de Amazon EKS.
- Un nombre de host DNS existente con un SSL/TLS certificado o SSL válido. Puede obtener un certificado para su dominio mediante AWS Certificate Manager (ACM) o cargando un certificado existente en ACM. Para obtener más información sobre estas dos opciones, consulte Solicitud de un certificado público e Importación de certificados a AWS Certificate Manager en la documentación de ACM.

Arquitectura

En el siguiente diagrama, se muestra la arquitectura implementada por este patrón.

El siguiente diagrama muestra un flujo de trabajo en el que SSL/TLS el tráfico se recibe de un cliente gRPC que se descarga a un Application Load Balancer. El tráfico se reenvía en texto sin formato al servidor gPC porque proviene de una nube privada virtual (VPC).

Tools (Herramientas)

Servicios de AWS

- La Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de la línea de comandos.
- Elastic Load Balancing permite distribuir el tráfico entrante de las aplicaciones o de la red entre varios destinos. Así, por ejemplo, puede distribuir el tráfico a través de instancias de Amazon Elastic Compute Cloud (Amazon EC2), contenedores y direcciones IP de una o varias zonas de disponibilidad.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.

- Amazon Elastic Kubernetes Service (Amazon EKS) lo ayuda a ejecutar Kubernetes en AWS sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.

Herramientas

- eksctl es una herramienta de CLI sencilla para crear clústeres de Amazon EKS.
- kubectl: es una utilidad de línea de comandos para la ejecución de comandos en clústeres de Kubernetes.
- El controlador del equilibrador de carga de AWS le ayuda a administrar los Elastic Load Balancer de AWS para un clúster de Kubernetes.
- g RPCurl es una herramienta de línea de comandos que te ayuda a interactuar con los servicios de gRPC.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub grpc-traffic-on-alb-to-eks.

Epics

Cree y envíe la imagen de Docker del servidor gRPC a Amazon ECR

Tarea	Descripción	Habilidades requeridas
Cree un repositorio de Amazon ECR.	Inicie sesión en la Consola de administración de AWS, abra la consola de Amazon ECR y, luego, cree un repositorio de Amazon ECR. Para obtener más información, consulte Creación de un repositorio en la documentación de Amazon ECR. Asegúrese de registrar la URL del repositorio de Amazon ECR. También puede crear un repositorio de Amazon ECR	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	con la CLI de AWS ejecutando el siguiente comando: `aws ecr create-repository --repository-name helloworld-grpc`	

Tarea	Descripción	Habilidades requeridas

Cree la imagen de Docker.	1. Clona el repositorio GitHub grpc-traffic-on-alb-to-eks.
	`git clone https://github.com/aws-samples/grpc-traffic-on-alb-to-eks.git`
	2. Desde el directorio raíz del repositorio, asegúrese de que el Dockerfile existe y, a continuación, ejecute el siguiente comando para crear la imagen de Docker:
	`docker build -t <amazon_ecr_repository_url>:<Tag> .`
	⚠ Important
	Asegúrese de sustituir `<amazon_ecr_repository_url>` por la URL del repositorio de Amazon ECR que creó anteriormente.
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Envíe la imagen de Docker a Amazon ECR.	1. Ejecute el siguiente comando para iniciar sesión en el repositorio de Amazon ECR:
	`aws ecr get-login -password --region us-east-1 --no-cli-auto-prompt | docker login --username AWS --password-stdin <your_aws_account_id>.dkr.ecr.us-east-1.amazonaws.com`
	2. Envíe la imagen de Docker en el repositorio de Amazon ECR ejecutando el siguiente comando:
	`docker push <your_aws_account_id>.dkr.ecr.us-east-1.amazonaws.com/helloworld-grpc:1.0`
	⚠ Important
	Asegúrese de sustituir `<your_aws_account_id>` por el ID de su cuenta de AWS.
		DevOps ingeniero

Implemente los manifiestos de Kubernetes en el clúster de Amazon EKS

Tarea	Descripción	Habilidades requeridas
Modifique los valores del archivo de manifiesto de Kubernetes.	1. Modifique el archivo de manifiesto `grpc-sample.yaml` de Kubernetes en la carpeta de Kubernetes del repositorio según sus necesidades. Debe modificar las anotaciones y el nombre de host en el recurso de entrada. Para ver un ejemplo de recurso de entrada, consulte la sección Información adicional. Para obtener más información sobre anotaciones de entrada, consulte Anotaciones de ingreso en la documentación de Kubernetes. 2. En el recurso de implementación de Kubernetes, cambie el `image` de los recursos de despliegue por el identificador uniforme de recursos (URI) del repositorio de Amazon ECR al que insertó la imagen de Docker. Para ver un ejemplo de recurso de implementación, consulte la sección Información adicional.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Implemente el archivo de manifiesto de Kubernetes.	Para implementar el archivo `grpc-sample.yaml` en el clúster de Amazon EKS, ejecute el siguiente comando `kubectl`: `kubectl apply -f ./kubernetes/grpc-sample.yaml`	DevOps ingeniero

Cree el registro de DNS para el FQDN del Equilibrador de carga de aplicación

Tarea	Descripción	Habilidades requeridas
Registre el FQDN para el Equilibrador de carga de aplicación.	1. Ejecute el siguiente comando `kubectl` para describir el recurso de entrada de Kubernetes que administra el Equilibrador de carga de aplicación: `kubectl get ingress -n grpcserver` En la sección Información adicional se proporciona un ejemplo de resultado. En el resultado, el campo `HOSTS` muestra el nombre de host DNS para el que se crearon los certificados SSL. 2. Registre el nombre de dominio (FQDN) del Equilibrador de carga de	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	aplicación en el campo `Address` del resultado. 3. Cree un registro DNS que apunte al FQDN del Equilibrador de carga de aplicación. Si su proveedor de DNS es Amazon Route 53, puede crear un registro de alias que apunte al FQDN del Equilibrador de carga de aplicación. Para obtener más informaci ón sobre esta opción, consulte Elección entre registros de alias y sin alias en la documentación de Route 53.	

Pruebe la solución

Tarea	Descripción	Habilidades requeridas
Pruebe el servidor gRPC.	Use g RPCurl para probar el punto final ejecutando el siguiente comando: `grpcurl grpc.exam ple.com:443 list grpc.reflection.v 1alpha.ServerRefle ction helloworld.helloworld`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Note Sustituya `grpc.example.com` por su nombre de DNS.	

Tarea	Descripción	Habilidades requeridas

Pruebe el servidor gRPC con un cliente gRPC.	En el ejemplo de cliente gRPC de `helloworld_client_ssl.py` , sustituya el nombre de host de `grpc.example.com` por el nombre de host utilizado para el servidor gRPC.
	
	El siguiente ejemplo de código muestra la respuesta del servidor gRPC a la solicitud del cliente:
	
	`python ./app/helloworld_client_ssl.py`
	`message: "Hello to gRPC server from Client"`
	
	`message: "Thanks for talking to gRPC server!! Welcome to hello world. Received message is \"Hello to gRPC server from Client\""`
	`received: true`
	
	Esto demuestra que el cliente puede hablar con el servidor y que la conexión se ha realizado correctamente.
		DevOps ingeniero

Limpieza

Tarea	Descripción	Habilidades requeridas
Elimine el registro de DNS.	Elimine el registro DNS que apunta al FQDN del Equilibrador de carga de aplicación que creó anteriormente.	Administrador de la nube
Elimine el equilibrador de carga.	En la consola Amazon EC2, elija Equilibradores de carga y, a continuación, elimine el equilibrador de carga que el controlador de Kubernetes creó para su recurso de entrada.	Administrador de la nube
Elimine el clúster de Amazon EKS.	Elimine el clúster de Amazon EKS mediante `eksctl`: `eksctl delete cluster -f ./eks.yaml`	AWS DevOps

Recursos relacionados

- Equilibrio de carga de red en Amazon EKS
- Grupos de destino para los Equilibradores de carga de aplicación

Información adicional

Ejemplo de recurso de ingreso:

```
---
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  annotations:
```

```
    alb.ingress.kubernetes.io/healthcheck-protocol: HTTP
    alb.ingress.kubernetes.io/ssl-redirect: "443"
    alb.ingress.kubernetes.io/backend-protocol-version: "GRPC"
    alb.ingress.kubernetes.io/listen-ports: '[{"HTTP": 80}, {"HTTPS":443}]'
    alb.ingress.kubernetes.io/scheme: internet-facing
    alb.ingress.kubernetes.io/target-type: ip
    alb.ingress.kubernetes.io/certificate-arn: arn:aws:acm:<AWS-
Region>:<AccountId>:certificate/<certificate_ID>
  labels:
    app: grpcserver
    environment: dev
  name: grpcserver
  namespace: grpcserver
spec:
  ingressClassName: alb
  rules:
  - host: grpc.example.com # <----- replace this as per your host name for which the
 SSL certtficate is available in ACM
    http:
      paths:
      - backend:
          service:
            name: grpcserver
            port:
              number: 9000
        path: /
        pathType: Prefix
```

Ejemplo de recurso de implementación:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: grpcserver
  namespace: grpcserver
spec:
  selector:
    matchLabels:
      app: grpcserver
  replicas: 1
  template:
    metadata:
      labels:
```

```
        app: grpcserver
    spec:
      containers:
      - name: grpc-demo
        image: <your_aws_account_id>.dkr.ecr.us-east-1.amazonaws.com/helloworld-
grpc:1.0   #<------- Change to the URI that the Docker image is pushed to
        imagePullPolicy: Always
        ports:
        - name: grpc-api
          containerPort: 9000
        env:
        - name: POD_IP
          valueFrom:
            fieldRef:
              fieldPath: status.podIP
      restartPolicy: Always
```

Resultado de ejemplo:

```
NAME             CLASS           HOSTS                          Address
 PORTS          AGE
 grpcserver      <none>      <DNS-HostName>                 <ELB-address>
 80            27d
```

Implemente aplicaciones en contenedores si se AWS IoT Greengrass V2 ejecutan como un contenedor Docker

Salih Bakir, Giuseppe Di Bella y Gustav Svalander, Amazon Web Services

Resumen

AWS IoT Greengrass Version 2, cuando se implementa como un contenedor de Docker, no admite la ejecución de contenedores de aplicaciones de Docker de forma nativa. Este patrón le muestra cómo crear una imagen de contenedor personalizada basada en la última versión AWS IoT Greengrass V2 que habilite la funcionalidad Docker-in-Docker (DiND). Con DiND, puede ejecutar aplicaciones en contenedores dentro del entorno. AWS IoT Greengrass V2

Puede implementar este patrón como una solución independiente o integrarlo con plataformas de organización de contenedores como Amazon ECS Anywhere. En cualquiera de los dos modelos de implementación, mantiene todas las AWS IoT Greengrass V2 funciones, incluidas las capacidades de procesamiento AWS IoT SiteWise perimetral, al tiempo que permite implementaciones escalables basadas en contenedores.

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- Para conocer AWS IoT Greengrass Version 2 los requisitos previos generales, consulte los requisitos previos en la AWS IoT Greengrass Version 2 documentación.
- Docker Engine, instalado y configurado en Linux, macOS o Windows.
- Docker Compose (si utiliza la interfaz de línea de comandos (CLI) de Docker Compose para ejecutar imágenes de Docker).
- Un sistema operativo Linux.
- Un hipervisor con un servidor host que admite la virtualización.
- Requisitos del sistema:
  - 2 GB de RAM (mínimo)
  - 5 GB de espacio disponible en disco (mínimo)
  - Para AWS IoT SiteWise Edge, una CPU x86_64 de cuatro núcleos con 16 GB de RAM y 50 GB de espacio disponible en disco. Para obtener más información sobre el procesamiento de

AWS IoT SiteWise datos, consulte los requisitos del paquete de procesamiento de datos en la documentación. AWS IoT SiteWise

Versiones de producto

- AWS IoT Greengrass Version 2 versión 2.5.3 o posterior
- Docker-in-Docker versión 1.0.0 o posterior
- Docker Compose versión 1.22 o posterior
- Docker Engine, versión 20.10.12 o posterior

Limitaciones

- Algunas Servicios de AWS no están disponibles en todos. Regiones de AWS Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

Pila de tecnología de destino

- Fuentes de datos: dispositivos de IoT, sensores o equipos industriales que generan datos para su procesamiento
- AWS IoT Greengrass V2— Funciona como un contenedor Docker con D-in-D capacidades, implementado en infraestructuras perimetrales
- Aplicaciones en contenedores: aplicaciones personalizadas que se ejecutan en el AWS IoT Greengrass V2 entorno como contenedores Docker anidados
- (Opcional) Amazon ECS Anywhere: organización de contenedores que gestiona la implementación de AWS IoT Greengrass V2 contenedores
- Otros Servicios de AWS: AWS IoT Core AWS IoT SiteWise, y otros Servicios de AWS para el procesamiento y la administración de datos

Arquitectura de destino

El siguiente diagrama muestra un ejemplo de arquitectura de implementación de destino que utiliza Amazon ECS Anywhere, que es una herramienta de administración de contenedores.

En el diagrama, se muestra el siguiente flujo de trabajo:

1: Almacenamiento de imágenes de contenedores: Amazon ECR almacena las imágenes del AWS IoT Greengrass contenedor y cualquier contenedor de aplicaciones personalizadas necesario para el procesamiento perimetral.

2 y 3: Despliegue de contenedores: Amazon ECS Anywhere despliega la imagen del AWS IoT Greengrass contenedor desde Amazon ECR en la ubicación perimetral, gestionando el ciclo de vida del contenedor y el proceso de despliegue.

4: Despliegue de componentes: el AWS IoT Greengrass núcleo implementado despliega automáticamente sus componentes relevantes en función de su configuración. Los componentes incluyen AWS IoT SiteWise Edge y otros componentes de procesamiento perimetral necesarios dentro del entorno contenerizado.

5: Ingesta de datos: una vez que esté completamente configurado, AWS IoT Greengrass comienza a ingerir datos de telemetría y sensores de varias fuentes de datos de IoT en la ubicación perimetral.

6: Procesamiento de datos e integración en la nube: el AWS IoT Greengrass núcleo contenerizado procesa los datos de forma local mediante sus componentes desplegados (incluido AWS IoT SiteWise Edge para datos industriales). Luego, envía los datos procesados a los Nube de AWS servicios para su posterior análisis y almacenamiento.

Tools (Herramientas)

Servicios de AWS

- Amazon ECS Anywhere le ayuda a implementar, usar y gestionar las tareas y los servicios de Amazon ECS en su propia infraestructura.
- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- AWS IoT Greengrass es un servicio en la nube y de tiempo de ejecución en la periferia de Internet de las cosas (IoT) de código abierto que ayuda a crear, implementar y administrar aplicaciones de IoT en los dispositivos.

- AWS IoT SiteWise lo ayuda a recopilar, modelar, analizar y visualizar datos de equipos industriales a escala.

Otras herramientas

- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización del sistema operativo para entregar software en contenedores.
- Docker Compose es una herramienta para definir y ejecutar aplicaciones de varios contenedores.
- Docker Engine es una tecnología de contenerización de código abierto para crear y contenedorizar aplicaciones.

Repositorio de código

El código de este patrón está disponible en el repositorio de la versión 2. GitHub AWS IoT Greengrass Docker-in-Docker

Epics

Construye la AWS IoT Greengrass V2 Docker-in-Docker imagen

Tarea	Descripción	Habilidades requeridas

Clona y navega hasta el repositorio.	Para clonar el repositorio, utilice el siguiente comando:
	`git clone https://github.com/aws-samples/aws-iot-greengrass-docker-in-docker.git`
	Para navegar hasta el `docker` directorio, utilice el siguiente comando:
	`cd aws-iot-greengrass-docker-in-docker/docker`
		DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas

Cree la imagen de Docker.	Para crear la imagen de Docker con la versión predeterminada (la más reciente), ejecute el siguiente comando:
	`docker build -t x86_64/aws-iot-greengrass:latest .`
	O bien, para crear la imagen de Docker con una versión específica, ejecute el siguiente comando:
	`docker build --build-arg GREENGRASS_RELEASE_VERSION=2.12.0 -t x86_64/aws-iot-greengrass:2.12.0 .`
	Para verificar la compilación, ejecuta el siguiente comando:
	`docker images | grep aws-iot-greengrass`
		AWS DevOps, DevOps ingeniero, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

(Opcional) Empuje a Amazon ECR.	1. Para crear el repositorio, ejecute el siguiente comando:
	`aws ecr create-repository --repository-name aws-iot-greengrass-dind --region us-east-1`
	2. Para autenticarse, ejecute el siguiente comando:
	`aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-stdin <ACCOUNT-ID>.dkr.ecr.us-east-1.amazonaws.com`
	3. Para etiquetar y enviar, ejecuta los siguientes comandos:
	`docker tag x86_64/aws-iot-greengrass:latest <ACCOUNT-ID>.dkr.ecr.us-east-1.amazonaws.com/aws-iot-greengrass-dind:latest`
	`docker push <ACCOUNT_ID>.dkr.ecr.us-east-1.amazo`
		Desarrollador de aplicaciones, AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`naws.com/aws-iot-greengrass-dind:latest`	

Configure AWS las credenciales

Tarea	Descripción	Habilidades requeridas
Seleccione el método de autenticación.	Elija una de las siguientes opciones: • Opción 1 (recomendada): funciones de IAM: utilícela si se ejecuta en Amazon EC2, Amazon ECS o Amazon EKS con las funciones de IAM adecuadas. No se necesita ninguna configuración adicional. • Opción 2: Variables de entorno: para pruebas y desarrollo. • Opción 3: Archivo de credenciales: no se recomienda para producción. • Opción 4: `env.cfg` archivo heredado.	Administrador de AWS
Configure el método de autenticación.	Para el método de autenticación que ha seleccionado, utilice las siguientes instrucciones de configuración:	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	• Opción 2 (variables de entorno): Preparar y `AWS_ACCES S_KEY_ID AWS_SECRE T_ACCESS_KEY` , de forma opcional`AWS_SESSI ON_TOKEN` .
	• Opción 3 (archivo de credenciales): crear un directorio y un archivo de credenciales:
	  • (a) Ejecute el siguiente comando:
	  `mkdir -p ~/ greengrass-v2-cr edentials`
	  • (b) Cree el siguiente archivo en`~/greengr ass-v2-cr edentials/ credentials` :
	  `[default]`
	  `aws_access_key_id= YourAccessKey`
	  `aws_secret_access_ key=YourSecretKey`
	  • (c) Proteja el archivo de la siguiente manera:
	  `chmod 600 ~/ greengrass-v2-`	

Tarea	Descripción	Habilidades requeridas

	`credentials/credentials`
	• Opción 4 (**`env.cfg`**): cree el `env.cfg` archivo en el `docker` directorio de la siguiente manera:
	`GGC_ROOT_PATH=/greengrass/v2`
	`AWS_REGION=us-east-1`
	`PROVISION=true`
	`THING_NAME=MyGreengrassCore`
	`THING_GROUP_NAME=MyGreengrassCoreGroup`
	`TES_ROLE_NAME=GreengrassV2TokenExchangeRole`
	`TES_ROLE_ALIAS_NAME=GreengrassCoreTokenExchangeRoleAlias`
	`COMPONENT_DEFAULT_USER=ggc_user:ggc_group`	

Ejecute con Docker Compose

Tarea	Descripción	Habilidades requeridas

Configuración `docker-compose.yml` .	Actualice el `docker-compose.yml` archivo con las variables de entorno de la siguiente manera:
	• Variables clave: `PROVISION, AWS_REGION THING_NAME ,THING_GROUP_NAME ,TES_ROLE_NAME , TES_ROLE_ALIAS_NAME`
	• En el caso de las credenciales a través de variables de entorno, elimine los comentarios siguientes:
	`environment:`
	`- AWS_ACCESS_KEY_ID=YourKey`
	`- AWS_SECRET_ACCESS_KEY=YourSecret`
	• En el caso del archivo de credenciales, elimine los comentarios siguientes:
	`volumes:`
	`- ~/greengrass-v2-credentials:/root/.aws/:ro`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	• Para la persistencia del registro, añada lo siguiente:
	`volumes:`
	`- ./logs:/greengrass/v2/logs`	

Inicie y verifique el contenedor.	Para empezar en primer plano, ejecute el siguiente comando:
	`docker-compose up --build`
	O bien, para empezar en segundo plano, ejecute el siguiente comando:
	`docker-compose up --build -d`
	Para comprobar el estado, ejecute el siguiente comando:
	`docker-compose ps`
	Para supervisar los registros, ejecute el siguiente comando:
	`docker-compose logs -f`
		DevOps ingeniero

Ejecute con Docker CLI

Tarea	Descripción	Habilidades requeridas

Ejecute el contenedor con la CLI de Docker.	• Para iniciar una ejecución básica sin aprovisio namiento, ejecute el siguiente comando:
	`docker run --init --privileged -it --name aws-iot-g reengrass x86_64/aw s-iot-greengrass:l atest`
	• Para iniciar una ejecución con variables de entorno, ejecute el siguiente comando:
	`docker run --init --privileged - it --name aws- iot-greengrass - e PROVISION=true - e AWS_REGION=us- east-1 -e AWS_ACCES S_KEY_ID=YourKey - e AWS_SECRET_ACCESS_ KEY=YourSecret -e THING_NAME=MyGreen grassCore -e THING_GROUP_NAME=M yGreengrassCoreGro up -p 8883:8883`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	`x86_64/aws-iot-gre engrass:latest`
	
	• Para iniciar una ejecución con un archivo de credencia les, ejecute el siguiente comando:
	
	`docker run --init --privileged -it --name aws-iot-g reengrass -v ~/ greengrass-v2-cr edentials:/root/.a ws:ro -e PROVISION =true -e AWS_REGIO N=us-east-1 -e THING_NAME=MyGreen grassCore -p 8883:8883 x86_64/aw s-iot-greengrass:l atest`
	
	• Para iniciar una ejecución con un `env.cfg` archivo, ejecute el siguiente comando:
	
	`docker run --init --privileged -it --name aws-iot-g reengrass -v ~/ greengrass-v2-cr edentials:/root/.a ws:ro --env-file`	

Tarea	Descripción	Habilidades requeridas

	`env.cfg -p 8883:8883 x86_64/aws-iot-greengrass:latest`
	• Para iniciar una ejecución con registros persistentes, ejecuta el siguiente comando:
	`docker run --init --privileged -it --name aws-iot-greengrass -v \ $(pwd)/logs:/greengrass/v2/logs x86_64/aws-iot-greengrass:latest`	

Verifica el contenedor.	• Para comprobar el estado del contenedor, ejecuta el siguiente comando:
	`docker ps | grep aws-iot-greengrass`
	• Para supervisar los registros, ejecute el siguiente comando:
	`docker logs -f aws-iot-greengrass`
		DevOps ingeniero

Gestione aplicaciones contenerizadas

Tarea	Descripción	Habilidades requeridas

Implemente aplicaciones.	• Para implementar el contenedor de aplicaciones, ejecute el siguiente comando:
	`docker run -d --name my-app nginx:alpine`
	• Para verificar la implementación, ejecute el siguiente comando:
	`docker ps`
	• Para acceder a los registros, ejecute el siguiente comando:
	`cd /greengrass/v2/logs && cat greengrass.log`
		Desarrollador de aplicaciones

Acceda y pruébelo Docker-in-Docker.	1. Para abrir un shell en el contenedor, ejecute el siguiente comando:
	`docker exec -it aws-iot-greengrass sh`
	2. Para verificar Docker, ejecuta los siguientes comandos:
	`docker --version`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	`docker ps`
	3. Para realizar una prueba Docker-in-Docker, ejecute el siguiente comando:
	`docker run --rm hello-world`	

(Opcional) Intégrelo con Amazon ECS Anywhere

Tarea	Descripción	Habilidades requeridas

Configure el clúster de Amazon ECS.	• Para crear un clúster de Amazon ECS, ejecute el siguiente comando:
	`aws ecs create-cluster --cluster-name greengrass-cluster --region us-east-1`
	• Para crear la activación de SSM, ejecute el siguiente comando:
	`aws ssm create-activation --default-instance-name greengrass-edge --iam-role GreengrassECSAnywhereRole --registration-limit`
		Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	`10 --region us-east-1`
	
	• Para instalar el agente SSM en un dispositivo perimetral, ejecute el siguiente comando:
	
	`curl -o install.sh https://s3.amazonaws.com/aws-ssm-downloads/latest/linux_amd64/install.sh`
	
	`chmod +x install.sh`
	
	`./install.sh activation-code activation-id us-east-1`	

Tarea	Descripción	Habilidades requeridas

Implemente la tarea Amazon ECS.	• Cree `greengrass-task-definition.json` con la configuración de tareas `privileged:true` , incluidas `containerDefinitions` las variables de entorno y los montajes de volumen para cada `/var/lib/docker` `/greengrass/v2.Register` tarea. Use el siguiente comando:
	
	`aws ecs register-task-definition --cli-input-json file://greengrass-task-definition.json`
	
	• Para crear el servicio, ejecute el siguiente comando:
	
	`aws ecs create-service --cluster greengrass-cluster --service-name greengrass-service --task-definition greengrass-dind --desired-count 1 --launch-type EXTERNAL --region us-east-1`
		Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	• Para verificar la implement ación, ejecute el siguiente comando: `aws ecs describe-services --cluster greengrass-cluster --services greengrass-service --region us-east-1`	

Detenga y limpie

Tarea	Descripción	Habilidades requeridas

Detenga el contenedor.	• Para detener el contenedor mediante Docker Compose, ejecute los siguientes comandos:
	
	`docker-compose stop`
	
	`docker-compose down`
	
	`docker-compose down -v`
	
	• Para detener el contenedor (elimina los volúmenes) mediante la CLI de Docker, ejecute los siguientes comandos:
	
	`docker stop aws-iot-greengrass`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	`docker rm aws-iot-greengrass`
	• Para detener el contenedor mediante force remove, ejecute el siguiente comando:
	`docker rm -f aws-iot-greengrass`	

Resolución de problemas

Problema	Solución

El contenedor no se inicia debido a errores de permiso.	1. Para asegurarte de que el contenedor se ejecuta con la `--privileged` marca requerida Docker-in-Docker, ejecuta el siguiente comando:
	`docker run --init --privileged -it --name aws-iot-greengrass x86_64/aws-iot-greengrass:latest`
	2. En el `docker-compose.yml` archivo, defina lo siguiente:
	`privileged: true`

Problema	Solución
	Warning `--privileged` concede privilegios ampliados al contenedor.

El aprovisionamiento falla debido a errores de credenciales.	Para comprobar que las credenciales están configuradas correctamente, siga estos pasos:
	1. Compruebe la función de IAM:
	`aws sts get-caller-identity`
	2. Verifique las variables de entorno:
	`docker exec -it aws-iot-greengrass sh -c 'echo \$AWS_ACCESS_KEY_ID'`
	3. Compruebe el archivo de credenciales:
	`docker exec -it aws-iot-greengrass sh -c 'cat /root/.aws/credentials'`
	Asegúrese de que los permisos de IAM incluyan `iot:CreateThing` `iot:CreatePolicy` , `iot:AttachPolicy` `iam:CreateRole` , `yiam:AttachRolePolicy` .

Problema	Solución

No se puede conectar al daemon de Docker dentro del contenedor.	1. Compruebe el estado del daemon de Docker:
	`docker exec -it aws-iot-greengrass sh -c 'ps aux | grep dockerd'`
	2. Compruebe que existe el socket Docker:
	`docker exec -it aws-iot-greengrass sh -c 'ls -la /var/run/docker.sock'`
	3. Inicie manualmente si es necesario:
	`docker exec -it aws-iot-greengrass sh -c 'dockerd > /var/log/docker.log 2>&1 &'`

El contenedor se queda sin espacio en disco.	1. Compruebe el espacio en disco:
	`df -h`
	2. Limpie los recursos de Docker:
	`docker system prune -a --volumes`
	3. Elimine los artefactos antiguos de Greengrass:
	`docker exec -it aws-iot-greengrass sh -c 'rm -rf /greengrass/v2/work/*  '`
	Garantice un espacio mínimo en disco: 5 GB para las operaciones básicas y 50 GB para Edge AWS IoT SiteWise

Problema	Solución

Problemas de compilación.	1. Asegúrese de estar en el `docker` directorio:
	`cd docker && pwd`
	2. Comprueba que `Dockerfile` existe:
	`ls -la Dockerfile`
	3. Compruebe que Docker esté instalado y en ejecución:
	`docker --version && docker ps`

Problemas de conectividad de red.	1. Pruebe de la resolución de DNS:
	`docker exec -it aws-iot-greengrass sh -c 'nslookup google.com'`
	2. Pruebe AWS la conectividad:
	`docker exec -it aws-iot-greengrass sh -c 'curl https://iot.us-east-1.amazonaws.com'`
	Compruebe que el firewall permita el tráfico saliente de HTTPS (443) y MQTT (8883).

Problema	Solución

Los componentes de Greengrass no se despliegan.	1. Compruebe los registros de Greengrass:
	`docker exec -it aws-iot-greengrass sh -c 'cat /greengrass/v2/logs/greengrass.log'`
	2. Verifique la configuración del rol de TES:
	`aws iot describe-role-alias --role-alias TES_ROLE_ALIAS_NAME`
	Compruebe los registros específicos de los componentes en el `/greengrass/v2/logs/` directorio.

El contenedor sale inmediatamente después del inicio.	1. Compruebe si hay errores en los registros del contenedor:
	`docker logs aws-iot-greengrass`
	2. Ejecute con un shell interactivo para la depuración:
	`docker run --init --privileged -it --entrypoint sh x86_64/aws-iot-greengrass:latest`
	Compruebe que todas las variables de entorno requeridas estén configuradas correctamente si`PROVISION=true` . Asegúrese de utilizar la `--init` marca al iniciar el contenedor.

Recursos relacionados

AWS resources

- Amazon Elastic Container Service

- Configure el procesamiento de datos AWS IoT SiteWise perimetrales para modelos y activos
- ¿Qué es AWS IoT Greengrass

Otros recursos

- Documentación de Docker

Información adicional

- Para el procesamiento de datos de AWS IoT SiteWise Edge, Docker debe estar disponible en el AWS IoT Greengrass entorno.
- Para ejecutar un contenedor anidado, debe ejecutarlo con credenciales de AWS IoT Greengrass nivel de administrador.

Implementar contenedores mediante Elastic Beanstalk

Thomas Scott y Jean-Baptiste Guillois, Amazon Web Services

Resumen

En la nube de Amazon Web Services (AWS), AWS Elastic Beanstalk admite Docker como plataforma disponible, de forma que los contenedores pueden ejecutarse en el entorno creado. Este patrón muestra cómo implementar contenedores mediante el servicio Elastic Beanstalk. La implementación de este patrón utilizará el entorno de servidor web basado en la plataforma Docker.

Para usar Elastic Beanstalk para implementar y escalar aplicaciones y servicios web, debe cargar el código y la implementación se gestiona automáticamente. También se incluyen el aprovisionamiento de capacidad, el equilibrio de carga, el escalado automático y la supervisión del estado de las aplicaciones. Cuando usa Elastic Beanstalk, puede tomar el control total de los recursos de AWS que crea en su nombre. No se aplican cargos adicionales por utilizar Elastic Beanstalk. Solo tiene que pagar por los recursos de AWS que se utilizan para almacenar y ejecutar sus aplicaciones.

Este patrón incluye instrucciones de implementación utilizando la interfaz de la línea de comandos de AWS Elastic Beanstalk (CLI de EB) y la consola de administración de AWS.

Casos de uso

Los casos de uso de Elastic Beanstalk incluyen los siguientes:

- Implementar un entorno prototipo para hacer una demostración de una aplicación frontend. (Este patrón usa un Dockerfile como ejemplo).
- Implemente una API para gestionar las solicitudes de API de un dominio determinado.
- Implemente una solución de orquestación mediante Docker-Compose (`docker-compose.yml` no se utiliza como ejemplo práctico en este patrón).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS
- AWS EB CLI instalada localmente
- Instalación de Docker en un equipo local

Limitaciones

- En el plan gratuito, hay un límite de 100 extracciones de Docker cada 6 horas por dirección IP.

Arquitectura

Pila de tecnología de destino

- Instancias de Amazon Elastic Compute Cloud (Amazon EC2)
- Security group (Grupo de seguridad)
- Equilibrador de carga de aplicación
- Grupo de escalado automático

Arquitectura de destino

Automatización y escala

AWS Elastic Beanstalk puede escalarse automáticamente en función del número de solicitudes realizadas. Los recursos de AWS creados para un entorno incluyen un Application Load Balancer, un grupo de Auto Scaling y una o más instancias de Amazon EC2 .

El balanceador de carga se encuentra frente a las EC2 instancias de Amazon, que forman parte del grupo Auto Scaling. Amazon EC2 Auto Scaling inicia automáticamente EC2 instancias de Amazon adicionales para adaptarse al aumento de la carga de la aplicación. Si la carga de la aplicación disminuye, Amazon EC2 Auto Scaling detiene las instancias, pero mantiene al menos una instancia en ejecución.

Activadores de escalado automáticos

El grupo Auto Scaling del entorno de Elastic Beanstalk utiliza CloudWatch dos alarmas de Amazon para iniciar las operaciones de escalado. Los desencadenadores predeterminados adaptan su capacidad cuando el tráfico de la red saliente promedio de cada instancia es superior a 6 MB o inferior a 2 MB durante un periodo de cinco minutos. Para utilizar Amazon EC2 Auto Scaling de forma eficaz, configure los activadores adecuados para su aplicación, tipo de instancia y requisitos de servicio. Puede optar por la escala en función de varias estadísticas, como la latencia, E/S de disco, la utilización de la CPU y el recuento de solicitudes. Para obtener más información, consulte Límites de escalado automático.

Tools (Herramientas)

Servicios de AWS

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- La interfaz de la línea de comandos de AWS EB (CLI de EB) es un cliente de línea de comandos que puede utilizar para crear, configurar y administrar entornos de Elastic Beanstalk.
- Elastic Load Balancing permite distribuir el tráfico entrante de las aplicaciones o de la red entre varios destinos. Por ejemplo, puede distribuir el tráfico entre instancias, contenedores y direcciones IP de Amazon Elastic Compute Cloud (Amazon EC2) en una o más zonas de disponibilidad.

Otros servicios

- Docker agrupa el software en unidades estandarizadas denominadas contenedores que incluyen bibliotecas, herramientas del sistema, código y tiempo de ejecución.

Código

El código de este patrón está disponible en el repositorio de aplicaciones de muestra de GitHub clúster.

Epics

Creación con un Dockerfile

Tarea	Descripción	Habilidades requeridas
Clone el repositorio remoto.	• Para clonar el repositorio, ejecute el comando `git clone https://github.com/aws-samples/cluster-sample-app.git . </p>`	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Inicialice el proyecto Docker de Elastic Beanstalk.	1. Cree un archivo llamado `aws.json` en la raíz. 2. Añada el siguiente código al archivo `aws.json`: `{ "AWSEBDockerrunVersion":"1", "Image":{ "Name":"cluster-sample-app" }, "Ports":[ { "ContainerPort":80 , "HostPort":8080 } ] }` 3. Ejecute el comando `eb init -p docker` en la raíz del proyecto.	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps
Ejecute el proyecto localmente.	1. Ejecute el comando `eb local run` en la raíz del proyecto. 2. Pruebe la aplicación navegando hasta `http://localhost` .	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Implemente utilizando la CLI de EB

Tarea	Descripción	Habilidades requeridas
Ejecute el comando de implementación	1. Ejecute el comando `eb create docker-sample-cluster-app` en la raíz del proyecto.	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps
Acceda a la versión implementada.	Una vez finalizado el comando de implementación, acceda al proyecto mediante el comando `eb open`.	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Implementación con la consola

Tarea	Descripción	Habilidades requeridas
Implemente la aplicación mediante el navegador.	1. Abra la consola de . 2. Vuelva a la consola de Elastic Beanstalk. 3. Elija Create application (Crear aplicación). 4. Para el Application Name (Nombre de la aplicación), introduzca Cluster-Sample-App. 5. Elija Docker como plataforma. 6. Seleccione Upload your code (Sube código). 7. Elija su archivo .zip local (en la raíz del proyecto clonado) o una URL pública	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	de Amazon Simple Storage Service (Amazon S3).	
Acceda a la versión implement ada.	Tras la implementación, acceda a la aplicación implementada y elija la URL proporcionada.	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Recursos relacionados

- Entornos del servidor web
- Instalación de la CLI de EB en macOS
- Instalación manual de la CLI de EB

Información adicional

Ventajas de utilizar Elastic Beanstalk

- Aprovisionamiento automático de infraestructura
- Administración automática de la plataforma subyacente
- Parches y actualizaciones automáticos para dar soporte a la aplicación
- Escalado automático de la aplicación
- Posibilidad de personalizar el número de nodos
- Posibilidad de acceder a los componentes de la infraestructura si es necesario
- Facilidad de implementación en comparación con otras soluciones de implementación de contenedores

Habilite el modo automático de Amazon EKS en todos los clústeres de EKS mediante GitHub acciones

Urbija Goswami y Anugrah Lakra, Amazon Web Services

Resumen

Los clústeres de Amazon Elastic Kubernetes Service (EKS) suelen requerir la administración manual de los recursos informáticos a través de grupos de nodos. Esto genera una sobrecarga operativa para:

- Decisiones de planificación y escalamiento de la capacidad
- Aprovisionamiento de nodos y administración del ciclo de vida
- Optimización de costos en diferentes tipos de carga de trabajo
- Mantenimiento y actualizaciones de la infraestructura

Amazon EKS Auto Mode automatiza la administración de los recursos informáticos al aprovisionar y escalar los nodos de forma dinámica en función de las demandas de carga de trabajo, lo que elimina la necesidad de administrar manualmente los grupos de nodos.

Sin embargo, muchas organizaciones tienen dificultades para habilitar y administrar Amazon EKS Auto Mode de manera uniforme en sus clústeres nuevos y existentes. Los desafíos más comunes incluyen:

- Procesos de migración complejos desde grupos de nodos existentes
- Riesgo de interrupción del servicio durante la transición
- Necesidad de planificar y probar cuidadosamente la capacidad
- Requisito de permisos y configuraciones específicos de Amazon IAM
- Coordinación entre varios equipos y entornos

Este patrón implementa un flujo de trabajo de GitHub acciones que habilita el modo automático de EKS en los clústeres de EKS de una región de AWS específica. Antes de activar el modo automático, el flujo de trabajo crea copias de seguridad con fecha y hora del estado del clúster (configuración del clúster, grupos de nodos, versiones de Helm y recursos personalizados) y las carga en un bucket de Amazon S3.

Tras activar el modo automático, el flujo de trabajo vacía y elimina los grupos de nodos antiguos, actualiza los permisos de los roles del clúster y limpia los componentes de escalado anteriores, como Karpenter y Cluster Autoscaler. El flujo de trabajo se puede integrar con las canalizaciones de integración continua y continua () existentes. delivery/deployment CI/CD

Requisitos previos y limitaciones

Requisitos previos

1. Necesario

- Una GitHub cuenta y tu propio GitHub repositorio para ejecutar el flujo de trabajo
- Una cuenta de AWS activa con permisos administrativos

2. Instalación de herramientas locales

- Terraform versión 1.13.0 o posterior
- GitHub CLI (gh), configurada con las credenciales adecuadas
- kubectl y eksctl, configurados para la administración de clústeres

3. Requisitos del clúster EKS

- Kubernetes versión 1.29 o posterior
- Configuración de acceso al punto final:
  - O bien está configurada para puntos finales públicos y privados
  - O punto final privado con puerta de enlace NAT en subredes privadas
- La API de EKS y el acceso a los ConfigMapclústeres están habilitados (se requiere para que EKS pueda gestionar dinámicamente los nodos del modo automático y actualizar el aws-auth ConfigMap para una correcta autenticación del clúster durante la migración)
- Grupos de nodos activos o grupos de nodos gestionados

4. Requisitos de configuración de IAM OIDC

- El rol de IAM y el proveedor de identidades para ello incluyen: GitHub
  - Política de confianza para OIDC GitHub
  - Permisos para:

    - Administración de clústeres de EKS
    - acceso a buckets de S3
    - Administración de roles de IAM
    - Administración de redes EC2
- Consulte el código iam.tf para una configuración sencilla con Terraform. El rol de IAM (GitHubActionsEKSRole) se creará cuando se aplique el código de Terraform.

Limitaciones

- Solo es compatible con clústeres de EKS con la versión 1.29 y superior de Kubernetes
- Solo es compatible con la versión 1.1.0 y superior de Karpenter
- Region-specific implementación. Algunos servicios de AWS no están disponibles en todas las regiones de AWS. Para conocer la disponibilidad regional, consulte los servicios de AWS por región
- Requiere accesibilidad a los puntos de conexión del clúster
- Limitado a grupos AWS-managed de nodos

Arquitectura

Pila de tecnología de destino

1. GitHub Acciones
2. AWS IAM
3. AWS EKS
4. Amazon S3

Arquitectura de destino

1. El usuario activa el flujo de trabajo de GitHub acciones desde el GitHub repositorio.
2. El flujo de trabajo de GitHub acciones asume una función de IAM y utiliza OIDC para realizar los cambios necesarios en la cuenta de AWS. También comprueba la presencia del rol EKS Auto Node en la cuenta y, si no está presente, se crea el rol y se adjuntan las políticas necesarias.

3. Se carga en un bucket de S3 una copia de seguridad del estado actual del clúster de EKS que necesita el modo automático activado.
4. Se recupera la función de clúster del clúster que necesita el modo automático activado y se le añaden permisos adicionales (AmazonEKSComputePolicy AmazonEKSBlockStoragePolicy AmazonEKSLoadBalancingPolicy, AmazonEKSNetworkingPolicy,,, AmazonEKSClusterPolicy) si no están presentes en el modo automático de EKS. Además, como paso previo a la migración, las subredes de los clústeres se actualizan con etiquetas para habilitar el modo automático de EKS.
5. El flujo de trabajo habilita el modo automático de EKS en el clúster de EKS.
6. Los grupos de nodos antiguos se identifican y eliminan. Esto se omite si el usuario no ha concedido los permisos para la función de IAM que se describen en los pasos de configuración opcionales que se indican a continuación.
7. Los componentes de escalado (Karpenter y Cluster Autoscaler) también se eliminan si estaban presentes anteriormente.

El flujo de trabajo de GitHub Actions consta de tres tareas principales:

1. `check-clusters`: identifica los clústeres que no tienen el modo automático activado y actualiza las políticas de IAM y las etiquetas de subred.
2. `backup-and-check`: Realiza una copia de seguridad del estado del clúster antes de la migración.
3. `gradual-migration`: Activa el modo automático y, al mismo tiempo, agota gradualmente los grupos de nodos existentes y limpia los componentes de escalado antiguos. También realiza una verificación final del estado de los clústeres tras la migración.

> **Note**
>
> Si necesita copias de seguridad de la configuración de los nodos o planea eliminar nodes/node grupos durante la migración al modo automático de EKS, puede añadir a aws-auth el rol de IAM creado con el código terraform. ConfigMap Sin él, aún puede ver las configuraciones de los grupos de nodos.

Tools (Herramientas)

AWS CLI:

La Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de la línea de comandos. En nuestra solución, utilizamos la interfaz de línea de comandos para que los servicios de AWS ejecuten las actualizaciones de la configuración del clúster de EKS, las actualizaciones de los roles de IAM y consulten el estado del clúster durante todo el proceso de automatización.

Amazon EKS:

Amazon Elastic Kubernetes Service (Amazon EKS) lo ayuda a ejecutar Kubernetes en AWS sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes. En este patrón, Amazon EKS es el servicio de destino en el que el modo automático está habilitado para automatizar el aprovisionamiento informático y el escalado de nodos en los clústeres de una región específica.

IAM:

AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos. En nuestra solución, lo utilizamos para administrar los permisos de GitHub Actions para modificar las configuraciones de los clústeres de EKS mediante la federación OIDC. La solución también modifica los permisos de los roles del clúster y añade una tarea para crear el rol de nodo de EKS, de modo que el modo automático de EKS pueda programar los módulos pendientes en los nuevos nodos que activa como parte de los grupos de nodos.

Amazon S3:

Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos. En nuestra solución, utilizamos un depósito S3 para almacenar las copias de seguridad con fecha y hora de los clústeres antes de que se habilite el modo automático de EKS en ellos, lo que ayudaría a la recuperación ante desastres.

Otras herramientas:

GitHub Acciones:

GitHub Actions es una CI/CD plataforma que se utiliza en nuestra solución para automatizar el flujo de trabajo de activación del modo automático de EKS. También proporciona una autenticación segura a través del OIDC y gestiona la ejecución de los procesos en varios clústeres.

HashiCorp Terraform:

Terraform es una herramienta de infraestructura como código (IaC) que facilita usar el código para aprovisionar y administrar los recursos y la infraestructura en la nube. Nuestra solución utiliza terraform para aprovisionar las funciones y políticas de IAM y para añadir la configuración de proveedores de OIDC para una integración segura de Actions. GitHub

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub EKS Auto Mode Enablement via Actions. GitHub

Prácticas recomendadas

- Seguridad:
  - Siga el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte las mejores prácticas de seguridad y concesión de privilegios mínimos en la documentación de IAM. Consulte el archivo iam.tf del repositorio para ver la configuración mínima requerida.
  - Aplica la política de confianza de roles de IAM a tu GitHub repositorio y sucursal específicos para evitar que grupos de trabajo no autorizados asuman ese rol.
  - Habilite el registro del plano de control de EKS (servidor API, auditoría, autenticador) antes de iniciar la migración para poder diagnosticar los problemas de programación o autenticación una vez activado el modo automático.
  - Añada --sse AES256 a todos los comandos aws s3 cp del script de respaldo para aplicar el cifrado del lado del servidor en las copias de seguridad del estado del clúster.
- Fiabilidad:
  - Pruebe primero el flujo de trabajo con un clúster que no sea de producción. Compruebe que las cargas de trabajo se reprograman correctamente en los nodos de modo automático antes de migrar los clústeres de producción.
  - Compruebe que las copias de seguridad de S3 se hayan completado correctamente y que contengan datos válidos sobre la configuración del clúster, el grupo de nodos, la versión de Helm y los recursos personalizados antes de continuar con la activación del modo automático.
  - Tras activar el modo automático, supervise los eventos de programación de los pods y la latencia de aprovisionamiento de nodos mediante Amazon CloudWatch Container Insights para detectar problemas de forma temprana.
- Rendimiento:

  - Revise periódicamente los patrones de escalado del grupo de nodos en modo automático y ajuste las solicitudes y los límites de los recursos de la carga de trabajo para evitar el sobreaprovisionamiento o los retrasos en la programación.
- Costo:
  - Etiquete los clústeres de EKS y los recursos asociados (funciones de IAM, depósitos de backup de S3, subredes) con metadatos de entorno y propiedad para facilitar el seguimiento de los costes y la visibilidad operativa. Para obtener más información, consulte la documentación sobre el etiquetado de los recursos de AWS. Puede editar el archivo de flujo de trabajo para añadir etiquetas personalizadas durante el proceso de migración.
  - Configure alertas de AWS Cost Explorer para monitorear los cambios en los costos de procesamiento después de habilitar el modo automático, ya que el modo automático puede cambiar los tipos de instancias y el comportamiento de escalado. Para obtener más información, consulte la documentación sobre cómo analizar los costos con AWS Cost Explorer.
- Operaciones:
  - Mantenga el archivo de flujo de trabajo y las configuraciones de Terraform en el control de versiones y documente cualquier anulación específica del entorno, como la región, el ARN del rol o el nombre del bucket de S3.

Epics

Herramienta SetUp

Tarea	Descripción	Habilidades requeridas
Configure el GitHub repositorio.	1. Clona y bifurca el GitHub repositorio. Una vez clonado, copia el archivo de flujo de trabajo a tu repositorio GitHub `git clone https://github.com/aws-samples/sample-enable-eks-auto-mode-using-github-actions.git`	AWS DevOps, arquitecto de nube

Tarea	Descripción	Habilidades requeridas

	`cd sample-enable-eks-auto-mode-using-github-actions`
	
	`cp .github/workflows/enable-eks-auto-mode.yml /path/to/your/repository/.github/workflows`
	
	2. Confirma y envía los cambios a tu repositorio GitHub
	
	`cd <path/to/your/repository>`
	`git add .`
	`git commit -m "Added EKS Auto Mode configurations"`
	`git push origin main`
	
	3. Configura los secretos de git para el repositorio:
	
	`gh auth login --web #authenticate to your github account using web`
	
	`#create secrets`
	`gh secret set AWS_REGION --body "us-east-1"`
	
	`gh secret set AWS_ROLE_ARN --body`	

Tarea	Descripción	Habilidades requeridas
	`"arn:aws:iam:ACCOUNT_ID:role/GitHubActionsEKSRole" #replace the account id with your account ID`	

(Opcional) Configure un rol de IAM

Tarea	Descripción	Habilidades requeridas
Configure IAM para realizar copias de seguridad y eliminar grupos de nodos	1. Añada el rol a aws-auth ConfigMap desde su terminal: `eksctl create iamidentitymapping \ --cluster $CLUSTER_NAME\ --region us-east-1 \ --arn arn:aws:iam::$ACCOUNT_ID:role/GitHubActionsEKSRole \ --group system:masters \ --username github-actions` Sustituya $CLUSTER_NAME y $ACCOUNT_ID por los valores adecuados. 1. Para más de un clúster, puede ejecutar los siguientes comandos en el terminal asumiendo un rol que tenga acceso de administrador o	AWS DevOps, arquitecto de nube

Tarea	Descripción	Habilidades requeridas

	de nivel equivalente a su cuenta:
	
	`CLUSTERS=$(aws eks list-clusters --region $AWS_REGION --query 'clusters[]' --output text)`
	
	`CLUSTERS_NEEDING_AUTO_MODE=""`
	
	`for cluster in $CLUSTERS; do`
	
	`AUTO_MODE=$(aws eks describe-cluster --name $cluster --region $AWS_REGION --query 'cluster.computeConfig.enabled' --output text 2>/dev/null || echo "false")`
	
	`if [ "$AUTO_MODE" != "True" ]; then`
	
	`CLUSTERS_NEEDING_AUTO_MODE="$CLUSTERS_NEEDING_AUTO_MODE $cluster"`
	
	`echo " Adding role access to cluster..."`
	`eksctl create iamidentitymapping \`
	`--cluster $cluster \`	

Tarea	Descripción	Habilidades requeridas

	<pre>--region $AWS_REGION \
	--arn $ROLE_ARN \
	--group system:masters\
	--username github-actions || echo " ## Role mapping may already exist"
	
	echo " # Role access configured for $cluster"
	done</pre> Sustituya $AWS_REGION y $ROLE_ARN por la región específica y el ARN del rol de IAM creado anteriormente, respectivamente.	

Ejecute y valide

Tarea	Descripción	Habilidades requeridas
Activa el flujo de trabajo de GitHub acciones.	El flujo de trabajo se activa automáticamente cuando se introduce algún cambio en las ramas de funciones, principales o de desarrollo. Para activarlo manualmente mediante la GitHub interfaz de usuario: 1. Ve al repositor io el GitHub 2. Haga clic en la pestaña «Acciones » 3. Seleccione el flujo de	AWS DevOps, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	trabajo (canalización de modo automático) 4. Haga clic en el botón «Ejecutar flujo de trabajo» 5. Elija la rama y haga clic en «Ejecutar flujo de trabajo» El flujo de trabajo gestiona la verificación tras la migración consultando la configuración informática de cada clúster migrado mediante la AWS CLI para confirmar que el modo automático de EKS se ha activado correctamente y muestra la configuración informática actual en formato de tabla.	

Configure la implementación en varios entornos

Tarea	Descripción	Habilidades requeridas
Implementación de un despliegue en varios entornos.	• La solución se puede personalizar para cada entorno al aprovechar las implementaciones basadas en sucursales. • Las diferentes ramas (main, dev, feat/*) activan flujos de trabajo con configuraciones específic as del entorno a través de secretos (AWS_REGION,	

Tarea	Descripción	Habilidades requeridas
	S3_BACKUP_BUCKET). GitHub AWS_ROLE_ARN • Esto permite separar las regiones de AWS, las funciones de IAM y los conjuntos de clústeres por entorno, a la vez que se mantiene una lógica de automatización coherente en todos los entornos.	

Limpieza

Tarea	Descripción	Habilidades requeridas
Eliminación de recursos.	1. Para separar la función de IAM de la de aws-auth ConfigMap, utilice el siguiente comando de terminal: `eksctl delete iamidentitymapping \ --cluster $cluster \ --region $AWS_REGION \ --arn $ROLE_ARN`	AWS general, arquitecto de nube

Resolución de problemas

Problema	Solución
Problemas de autenticación	• Compruebe que el proveedor de GitHub OIDC esté configurado correctamente en AWS IAM

Problema	Solución
	• Comprueba que el ARN del rol de IAM en git secrets coincide con el rol real creado con terraform () GitHubActionsEKSRole • Asegúrese de que el GitHub repositorio tenga configurados los secretos necesarios: AWS_REGION y. AWS_ROLE_ARN • Valide que la configuración de la región de AWS coincida con las ubicaciones de sus clústeres
¿Problemas con los permisos	<role-arn>• Pruebe los permisos de los roles de IAM localmente: bash aws sts assume-role --role-arn --role-session-name test-session aws eks list-clusters • Asegúrese de UpdateClusterConfig que el DescribeCluster rol tenga los permisos eks: y eks:
Compatibilidad de clústeres	<cluster-name>• Confirme que los clústeres de EKS ejecutan Kubernetes 1.29 o superior: bash aws eks describe-cluster --name --query 'cluster.version' • Compruebe que los clústeres estén en estado ACTIVO antes de activar el modo automático

Problema	Solución
Fallos en el flujo	• Compruebe los registros de GitHub acciones para ver si hay mensajes de error específicos • Compruebe la sintaxis del archivo de flujo de trabajo en. github/workflows/auto-mode-pipeline.yml • Asegúrese de que las variables de entorno estén configuradas correctamente en el flujo de trabajo

Recursos relacionados

1. Documentación oficial del modo automático EKS para empezar
2. Actualización de la documentación de CLI de configuración de clústeres
3. GitHub secretos de las GitHub acciones
4. GitHub Documentación de acciones
5. Documentación de la federación de la OIDC

Genere una dirección IP saliente estática mediante una función de Lambda, Amazon VPC y una arquitectura sin servidor

Thomas Scott, Amazon Web Services

Resumen

En este patrón se describe la forma de generar una dirección IP saliente estática en la nube de Amazon Web Services (AWS) mediante una arquitectura sin servidor. Su organización puede beneficiarse de este enfoque si quiere enviar archivos a una entidad empresarial independiente mediante el protocolo seguro File Transfer (SFTP). Esto significa que la entidad empresarial debe tener acceso a una dirección IP que permita que los archivos pasen por su firewall.

El enfoque del patrón lo ayuda a crear una función de AWS Lambda que utilice una dirección IP elástica como dirección IP de salida. Si sigue los pasos de este patrón, puede crear una función de Lambda y una nube privada virtual (VPC) que enrute el tráfico saliente a través de una puerta de enlace de Internet con una dirección IP estática. Para usar la dirección IP estática, debe adjuntar la función de Lambda a la VPC y sus subredes.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Permisos de AWS Identity and Access Management (IAM) para crear e implementar una función de Lambda y para crear una VPC y sus subredes. Para obtener más información, consulte Rol de ejecución y permisos de usuario en la documentación de AWS Lambda.
- Si planea usar la infraestructura como código (IaC) para implementar el enfoque de este patrón, necesitará un entorno de desarrollo integrado (IDE) como AWS Cloud9. Para obtener más información, consulte ¿Qué es AWS Cloud9? en la documentación de AWS Cloud9.

Arquitectura

El siguiente diagrama muestra la arquitectura sin servidor para este patrón.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El tráfico saliente deja `NAT gateway 1` en `Public subnet 1`.
2. El tráfico saliente deja `NAT gateway 2` en `Public subnet 2`.
3. La función de Lambda se puede ejecutar en `Private subnet 1` o `Private subnet 2`.
4. `Private subnet 1` y `Private subnet 2` enrutan el tráfico a las puertas de enlace NAT de las subredes públicas.
5. Las puertas de enlace NAT envían tráfico saliente a la puerta de enlace de Internet desde las subredes públicas.
6. Los datos salientes se transfieren desde la puerta de enlace de Internet al servidor externo.

Pila de tecnología

- Lambda
- Amazon Virtual Private Cloud (Amazon VPC)

Automatizar y escalar

Puede garantizar la alta disponibilidad (HA) mediante el uso de dos subredes públicas y dos privadas en distintas zonas de disponibilidad. Incluso si una zona de disponibilidad deja de estar disponible, la solución del patrón sigue funcionando.

Tools (Herramientas)

- AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.
- Amazon VPC: Amazon Virtual Private Cloud (Amazon VPC) le permite aprovisionar una sección aislada de forma lógica de la nube de AWS donde puede lanzar recursos de AWS en una red virtual que haya definido. Dicha red virtual es prácticamente idéntica a las redes tradicionales que se utilizan en sus propios centros de datos, con los beneficios que supone utilizar la infraestructura escalable de AWS.

Epics

Cree una nueva VPC

Tarea	Descripción	Habilidades requeridas
Cree una nueva VPC.	Inicie sesión en la consola de administración de AWS, abra la consola de Amazon VPC y, a continuación, cree una VPC con el nombre `Lambda VPC` que tenga `10.0.0.0/25` como rango CIDR. IPv4 Para obtener más información, consulte Introducción a Amazon VPC en la documentación de Amazon VPC.	Administrador de AWS

Crear dos subredes públicas

Tarea	Descripción	Habilidades requeridas
Cree la primera subred pública.	1. En la consola de Amazon VPC, elija Subredes y, a continuación, elija Crear subred. 2. En Etiqueta de nombre, ingrese `public-one` . 3. En VPC, elija `Lambda VPC`. 4. Elija una zona de disponibilidad y regístrela. 5. Para el bloque IPv4 CIDR, introduzca **`10.0.0.0/28`** y, a continuación, seleccione Crear subred.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Cree la segunda subred pública.	1. En la consola de Amazon VPC, elija Subredes y, a continuación, elija Crear subred. 2. En Etiqueta de nombre, ingrese `public-two` . 3. En VPC, elija `Lambda VPC`. 4. **Important** Elija una zona de disponibilidad y regístrela. : no puede utilizar la zona de disponibilidad que contenga la subred `public-one` . 5. Para el bloque IPv4 CIDR, introduzca **`10.0.0.16/28`** y, a continuación, seleccione Crear subred.	Administrador de AWS

Crear dos subredes privadas

Tarea	Descripción	Habilidades requeridas
Cree la primera subred privada.	1. En la consola de Amazon VPC, elija Subredes y, a continuación, elija Crear subred. 2. En Etiqueta de nombre, ingrese `private-one` .	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	3. En VPC, elija `Lambda VPC`. 4. Elija la zona de disponibilidad que contiene la subred `public-one` que creó anteriormente. 5. Para el bloque IPv4 CIDR, introduzca **`10.0.0.32/28`** y, a continuación, seleccione Crear subred.	
Cree la segunda subred privada.	1. En la consola de Amazon VPC, elija Subredes y, a continuación, elija Crear subred. 2. En Etiqueta de nombre, ingrese `private-two` . 3. En VPC, elija `Lambda VPC`. 4. Elija la misma zona de disponibilidad que contiene la subred `public-two` que creó anteriormente. 5. Para el bloque IPv4 CIDR, introduzca **`10.0.0.64/28`** y, a continuación, seleccione Crear subred.	Administrador de AWS

Crear dos direcciones IP elásticas para su gateway NAT

Tarea	Descripción	Habilidades requeridas
Cree la primera dirección IP elástica.	1. En la consola de Amazon VPC, elige Elastic IPs y, a	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	continuación, selecciona Asignar nueva dirección. 2. Elija Asignar y registre el ID de asignación de la dirección IP elástica recién creada. **Note** Esta dirección IP elástica se utiliza para su primera puerta de enlace de NAT.	
Cree la segunda dirección IP elástica.	1. En la consola de Amazon VPC, elige Elastic IPs y, a continuación, selecciona Asignar nueva dirección. 2. Elija Allocate (Asignar) y registre el Allocation ID (ID de asignación) de la dirección IP elástica recién creada. **Note** Esta dirección IP elástica se utiliza para su segunda puerta de enlace de NAT.	Administrador de AWS

Cree un puerta de enlace de Internet

Tarea	Descripción	Habilidades requeridas
Cree una puerta de enlace de Internet.	1. En la consola de Amazon VPC, elija Internet Gateways (Puertas de enlace de Internet) y, luego, elija Create internet gateway (Crear puerta de enlace de Internet). 2. Introduzca `Lambda internet gateway` como nombre y, a continuación, seleccione Crear puerta de enlace de Internet. Asegúrese de registrar el ID de la puerta de enlace de Internet.	Administrador de AWS
Adjunte la puerta de enlace de Internet a la VPC.	Seleccione el puerta de enlace de Internet que acaba de crear y, a continuación, elija Actions, Attach to VPC (Acciones, Adjuntar a la VPC).	Administrador de AWS

Cree dos puertas de enlace NAT

Tarea	Descripción	Habilidades requeridas
Cree la primera puerta de enlace NAT.	1. En la consola de Amazon VPC, elija NAT Gateways (Puertas de enlace NAT) y, luego, elija Create NAT Gateway (Crear puerta de enlace NAT).	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	2. Introduzca `nat-one` como nombre de la puerta de enlace NAT. 3. Seleccione `public-one` como la subred en la que crear la puerta de enlace NAT. 4. En el tipo de conectividad, elija Pública. 5. En Elastic IP Allocation ID (ID de asignación de IP elástica), elija el primer ID de la dirección IP elástica que creó anteriormente y asoció con la puerta de enlace NAT. 6. Elija Crear una puerta de enlace de NAT.	

Tarea	Descripción	Habilidades requeridas
Cree la segunda puerta de enlace NAT.	1. En la consola de Amazon VPC, elija NAT Gateways (Puertas de enlace NAT) y, luego, elija Create NAT Gateway (Crear puerta de enlace NAT). 2. Introduzca `nat-two` como nombre de la puerta de enlace NAT. 3. Seleccione `public-two` como la subred en la que crear la puerta de enlace NAT. 4. En el tipo de conectividad, elija Pública. 5. En Elastic IP Allocation ID (ID de asignación de IP elástica), elija el segundo ID de la dirección IP elástica que creó anteriormente y asoció con la puerta de enlace NAT. 6. Elija Crear una puerta de enlace de NAT.	Administrador de AWS

Cree tablas de enrutamiento para sus subredes públicas y privadas

Tarea	Descripción	Habilidades requeridas
Crear la tabla de enrutamiento de la subred pública.	1. En la consola de Amazon VPC, elija Route Tables (Tablas de enrutamiento) y, a continuación, elija Create	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	route table (Crear tabla de enrutamiento). 2. Introduzca `public-one-subnet` el nombre de tabla de enrutamiento y, a continuación, elija Crear tabla de enrutamiento. 3. Seleccione la tabla de enrutamiento `public-one-subnet` , elija Edit routes (Editar rutas), y luego elija Add route (Agregar ruta). 4. Especifique `0.0.0.0` en el cuadro Destino y seleccione el ID del puerta de enlace de Internet en la lista Objetivo. 5. En la pestaña Subnet associations (Asociaciones de subred), elija Edit subnet associations (Editar asociaciones de subred), seleccione la subred `public-one` con el rango CIDR `10.0.0.0/28` y, a continuación, elija Save associations (Guardar asociaciones). 6. Elija Save changes (Guardar cambios).	

Tarea	Descripción	Habilidades requeridas
Crear la tabla de enrutamiento de la segunda subred pública.	1. En la consola de Amazon VPC, elija Route Tables (Tablas de enrutamiento) y, a continuación, elija Create route table (Crear tabla de enrutamiento). 2. Introduzca `public-two-subnet` el nombre de tabla de enrutamiento y, a continuación, elija Crear tabla de enrutamiento. 3. Elija la `public-two-subnet`route table (tabla de enrutamiento), elija Edit routes (Editar rutas) y luego elija Add route (Agregar ruta). 4. Especifique `0.0.0.0` en el cuadro Destino y seleccione el ID del puerta de enlace de Internet en la lista Objetivo. 5. En la pestaña Subnet associations (Asociaciones de subred), elija Edit subnet associations (Editar asociaciones de subred), seleccione la subred `public-two` con el rango CIDR `10.0.0.16/28` y, a continuación, elija Save associations (Guardar asociaciones).	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	6. Elija Save changes (Guardar cambios).	

Tarea	Descripción	Habilidades requeridas
Crear la tabla de enrutamiento de la subred privada.	1. En la consola de Amazon VPC, elija Route Tables (Tablas de enrutamiento) y, a continuación, elija Create route table (Crear tabla de enrutamiento). 2. Introduzca `private-one-subnet` el nombre de tabla de enrutamiento y, a continuación, elija Crear tabla de enrutamiento. 3. Elija la `private-one-subnet` route table (tabla de enrutamiento), elija Edit routes (Editar rutas) y luego elija Add route (Agregar ruta). 4. Especifique `0.0.0.0` en el cuadro Destino y seleccione la puerta de enlace de NAT en la subred `public-one` de la lista Objetivo. 5. En la pestaña Subnet associations (Asociaciones de subred), elija Edit subnet associations (Editar asociaciones de subred), seleccione la subred `private-one` `10.0.0.32/28` con el rango CIDR y, a continuación, elija Save associations (Guardar asociaciones).	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	6. Elija Save changes (Guardar cambios).	

Tarea	Descripción	Habilidades requeridas
Crear la tabla de enrutamiento de la segunda subred privada.	1. En la consola de Amazon VPC, elija Route Tables (Tablas de enrutamiento) y, a continuación, elija Create route table (Crear tabla de enrutamiento). 2. Introduzca `private-two-subnet` el nombre de tabla de enrutamiento y, a continuación, elija Crear tabla de enrutamiento. 3. Elija la `private-two-subnet` route table (tabla de enrutamiento), elija Edit routes (Editar rutas) y luego elija Add route (Agregar ruta). 4. Especifique `0.0.0.0` en el cuadro Destino y seleccione la puerta de enlace de NAT en la subred `public-two` de la lista Objetivo. 5. En la pestaña Subnet associations (Asociaciones de subred), elija Edit subnet associations (Editar asociaciones de subred), seleccione la subred `private-two` con el rango CIDR `10.0.0.64/28` y, a continuación, elija Save associations (Guardar asociaciones).	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	6. Elija Save changes (Guardar cambios).	

Cree la función de Lambda, agréguela a la VPC y pruebe la solución

Tarea	Descripción	Habilidades requeridas
Crear una nueva función de Lambda.	1. Abra la consola AWS Lambda y, a continuación, elija Create a function (Crear una función) 2. En Información básica, inserte `Lambda test` en Nombre de la función y, a continuación, elija el idioma que prefiera en Tiempo de ejecución. 3. Seleccione Creación de función.	Administrador de AWS
Agregue la función de Lambda a su VPC.	1. En la consola de AWS Lambda, seleccione Funciones y, a continuación, elija la función que creó anteriormente. 2. Elija Configuración y, a continuación, elija VPC. 3. Elija Editar y, a continuación, elija `Lambda VPC` y ambas subredes privadas. 4. Elija el Grupo de seguridad predeterminado para realizar las pruebas y, a	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	continuación, seleccione Guardar.	
Escriba el código para llamar a un servicio externo.	1. En el lenguaje de programación que prefiera, escriba el código para llamar a un servicio externo que devuelva su dirección IP. 2. Compruebe que la dirección IP devuelta coincide con una de sus direcciones IP elásticas.	Administrador de AWS

Recursos relacionados

- Configuración de una función Lambda para obtener acceso a los recursos en una PC

Identificación automática de las imágenes de contenedor duplicadas al migrar a un repositorio de Amazon ECR

Rishabh Yadav y Rishi Singla, Amazon Web Services

Resumen

El patrón proporciona una solución automatizada para identificar si las imágenes almacenadas en diferentes repositorios de contenedores son duplicadas. Esta comprobación resulta útil si planea migrar imágenes de otros repositorios de contenedor a Amazon Elastic Container Registry (Amazon ECR).

Para obtener información básica, el patrón también describe los componentes de una imagen de contenedor, como el resumen de la imagen, el manifiesto y las etiquetas. Cuando planifique una migración a Amazon ECR, puede decidir sincronizar las imágenes de los contenedores entre los registros de contenedores comparando los resúmenes de las imágenes. Antes de migrar las imágenes de contenedor, debe comprobar si estas imágenes ya existen en el repositorio de Amazon ECR para evitar la duplicación. Sin embargo, puede resultar difícil detectar la duplicación comparando los resúmenes de imágenes, y esto podría provocar problemas en la fase inicial de migración. Este patrón compara los resúmenes de dos imágenes similares que están almacenadas en diferentes registros de contenedores y explica por qué varían los resúmenes con el fin de ayudarle a comparar las imágenes con precisión.

Requisitos previos y limitaciones

- Un activo Cuenta de AWS
- Acceso al registro público de Amazon ECR
- Familiaridad con lo siguiente: Servicios de AWS
  - AWS CodeCommit
  - AWS CodePipeline
  - AWS CodeBuild
  - AWS Identity and Access Management (IAM)
  - Amazon Simple Storage Service (Amazon S3)
- CodeCommit Credenciales configuradas (consulte las instrucciones)

Arquitectura

Componentes de la imagen de contenedor

En el siguiente diagrama se ilustran algunos de los componentes de una imagen de contenedor. Estos componentes se describen después del diagrama.

Términos y definiciones

Los siguientes términos se definen en la especificación de imagen de la Open Container Initiative (OCI).

- Registro: servicio de almacenamiento y administración de imágenes.
- Cliente: herramienta que se comunica con los registros y funciona con imágenes locales.
- Inserción: proceso para cargar imágenes a un registro.
- Extracción: proceso de descarga de imágenes de un registro.
- Blob: formato binario de contenido que almacena un registro y al que se puede acceder mediante un resumen.
- Índice: constructo que identifica varios manifiestos de imágenes para distintos tipos de plataformas informáticas (como x86-64 o ARM de 64 bits) o contenido multimedia. Para obtener más información, consulte la especificación del índice de imágenes de OCI.
- Manifiesto: documento JSON que define una imagen o un artefacto que se carga a través del punto de conexión del manifiesto. Un manifiesto puede hacer referencia a otros blobs de un repositorio mediante descriptores. Para obtener más información, consulte la especificación del manifiesto de imágenes de OCI.
- Capa del sistema de archivos: bibliotecas del sistema y otras dependencias de una imagen.
- Configuración: un blob que contiene metadatos de artefactos y al que se hace referencia en el manifiesto. Para obtener más información, consulte la especificación de la configuración de imágenes de OCI.
- Objeto o artefacto: elemento de contenido conceptual que se almacena como un blob y se asocia a un manifiesto adjunto con una configuración.
- Resumen: identificador único que se crea a partir de un hash criptográfico del contenido de un manifiesto. El resumen de imágenes ayuda a identificar de forma única una imagen de contenedor inmutable. Al extraer una imagen mediante su resumen, descargará siempre la misma

imagen en cualquier sistema operativo o arquitectura. Para obtener más información, consulte la especificación de imágenes de OCI.

- Etiqueta: un identificador de manifiesto legible para los humanos. En comparación con los resúmenes de imágenes, que son inmutables, las etiquetas son dinámicas. Una etiqueta que apunta a una imagen puede cambiar y pasar de una imagen a otra, aunque el resumen de la imagen subyacente sigue siendo el mismo.

Arquitectura de destino

El siguiente diagrama muestra la arquitectura de alto nivel de la solución proporcionada por este patrón para identificar imágenes de contenedor duplicadas mediante la comparación de las imágenes almacenadas en Amazon ECR y en repositorios privados.

Tools (Herramientas)

Servicios de AWS

- CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y administrarlos a lo largo de su ciclo de vida en todas Cuentas de AWS las regiones.
- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- AWS CodeCommit es un servicio de control de versiones que permite almacenar y administrar repositorios de Git de forma privada, sin necesidad de administrar su propio sistema de control de origen.
- AWS CodePipeline permite diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software y automatizar los pasos necesarios para lanzar los cambios en el software de manera continua.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.

Código

El código de este patrón está disponible en la solución automatizada de GitHub repositorios para identificar imágenes de contenedores duplicadas entre repositorios.

Prácticas recomendadas

- prácticas recomendadas de CloudFormation
- prácticas recomendadas de AWS CodePipeline

Epics

Extracción de imágenes de contenedor de repositorios públicos y privados de Amazon ECR

Tarea	Descripción	Habilidades requeridas

Extraiga una imagen de un repositorio público de Amazon ECR.	Desde el terminal, ejecute el siguiente comando para extraer la imagen `amazonlinux` del repositorio público de Amazon ECR.
	`$~ % docker pull public.ecr.aws/amazonlinux/amazonlinux:2018.03`
	Cuando la imagen se haya trasladado a su máquina local, verá el siguiente resumen de extracción, que representa el índice de la imagen.
	`2018.03: Pulling from amazonlinux/amazonlinux`
	`4ddc0f8d367f: Pull complete`
	`Digest: sha256:f972d24199508c52de7ad37a298bda35d8a1bd7df158149b381c03f6c6e363b5`
		Desarrollador de aplicaciones, AWS DevOps, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	``` Status: Downloade d newer image for public.ecr.aws/ama zonlinux/amazonlin ux:2018.03 public.ecr.aws/a mazonlinux/amazonl inux:2018.03 ```	

Tarea	Descripción	Habilidades requeridas

Inserte la imagen en un repositorio privado de Amazon ECR	1. Cree un repositorio privado de Amazon ECR denominado `test_ecr_repository` en la región Este de EE. UU. (Norte de Virginia) (`us-east-1`).
	`$~ % aws ecr get-login -password --region us-east-1 | docker login --username AWS --password-stdin <account-id>.dkr.ecr.us-east-1.amazonaws.com`
	`Login Succeeded`
	donde `<account-id>` se refiere a su Cuenta de AWS.
	2. Etiquete la imagen local que extrajo anteriormente. Use el valor `public.ecr.aws/amazonlinux/amazonlinux:2018.03` e insértelo en un repositorio privado de Amazon ECR.
	`$~ % docker tag public.ecr.aws/amazonlinux/amazonlinux:2018.03 <account-id>.dkr.ecr.us-east-1.amazonaws.com/`
		Administrador de AWS, AWS DevOps, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	`test_ecr_repositor y:latest`
	
	`$~ % docker push <account-id>.dkr.e cr.us-east-1.amazo naws.com/test_ecr_ repository:latest`
	
	Cuando inserte la imagen en el repositorio de Amazon ECR, Docker insertará la imagen subyacente y no el índice de la imagen.
	
	`The push refers to repository [<account -id>.dkr.ecr.us-ea st-1.amazonaws.com/ test_ecr_repository] d5655967c2c4: Pushed latest: digest: sha256:52db9000073 d93b9bdee6a7246a68 c35a741aaade05a8f4 febba0bf795cdac02 size: 529`	

Tarea	Descripción	Habilidades requeridas

Extraiga la misma imagen del repositorio privado de Amazon ECR.	1. Desde el terminal, ejecute el siguiente comando para extraer la imagen que ha insertado anteriormente en el repositorio privado de Amazon ECR.
	
	`$~ % docker pull <account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	`latest: Pulling from test_ecr_repository`
	`Digest: sha256:52db9000073d93b9bdee6a7246a68c35a741aaade05a8f4febba0bf795cdac02`
	`Status: Image is up to date for <account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	`<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	
	El resumen de esta imagen coincide con el resumen de la imagen que ha enviado al repositorio privado de Amazon ECR y represent a la imagen subyacente. Este valor no coincide con el índice de imágenes que
		Desarrollador de aplicaciones, AWS DevOps, administrador de AWS

Tarea	Descripción	Habilidades requeridas

	ha extraído del repositorio público.
	2. Para verificarlo, recupere el índice de imágenes por resumen.
	
	`curl -k -H "Authorization: Bearer $TOKEN" https://public.ecr.aws/v2/amazonlinux/amazonlinux/manifests/sha256:f972d24199508c52de7ad37a298bda35d8a1bd7df158149b381c03f6c6e363b55`
	`{`
	`"schemaVersion": 2,`
	`"mediaType": "application/vnd.docker.distribution.manifest.list.v2+json",`
	`"manifests": [`
	`{`
	`"mediaType": "application/vnd.docker.distribution.manifest.v2+json",`
	`"size": 529,`
	`"digest": "sha256:52db9000073d93b9bdee6a7246a68c35a741aaade05a8f4febba0bf795cdac02",`
	`"platform": {`	

Tarea	Descripción	Habilidades requeridas

	<pre>"architec
	ture": "amd64",
	"os":
	"linux"
	}
	}
	]
	}</pre>	

Comparación de los manifiestos de imágenes

Tarea	Descripción	Habilidades requeridas

Busque el manifiesto de la imagen almacenada en el repositorio público de Amazon ECR.	Desde el terminal, ejecute el siguiente comando para extraer el manifiesto de la imagen `public.ec r.aws/amazonlinux/ amazonlinux:2018.0 3` del repositorio público de Amazon ECR.
	<pre>$~ % docker manifest
	inspect public.ec
	r.aws/amazonlinux/
	amazonlinux:2018.03
	{
	"schemaVersion": 2,
	"mediaType":
	"application/vnd.d
	ocker.distribution
	.manifest.list.v2+
	json",
	"manifests": [
	{
	"mediaType":
	"application/vnd.d</pre>
		Administrador de AWS, AWS DevOps, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	ocker.distribution
	.manifest.v2+json",
	"size": 529,
	"digest":
	"sha256:52db900007
	3d93b9bdee6a7246a6
	8c35a741aaade05a8f
	4febba0bf795cdac02",
	"platform": {
	"architec
	ture": "amd64",
	"os":
	"linux"
	}
	}
	]
	}	

Tarea	Descripción	Habilidades requeridas

Busque el manifiesto de la imagen almacenada en el repositorio privado de Amazon ECR.	Desde el terminal, ejecute el siguiente comando para extraer el manifiesto de la imagen `<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest` del repositorio privado de Amazon ECR.
	
	`$~ % docker manifest inspect <account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	
	`{ "schemaVersion": 2, "mediaType": "application/vnd.docker.distribution.manifest.v2+json", "config": { "mediaType": "application/vnd.docker.container.image.v1+json", "size": 1477, "digest": "sha256:f7cee5e1af28ad4e147589c474d399b12d9b551ef4c3e11e02d982fce5eebc68" }, "layers": [ {`
		AWS DevOps, administrador de sistemas de AWS, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	"mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip", "size": 62267075, "digest": "sha256:4ddc0f8d367f424871a060e2067749f32bd36a91085e7140dcb159952f2d71453" }] }	

Tarea	Descripción	Habilidades requeridas
Compare el resumen extraído por Docker con el resumen del manifiesto de la imagen en el repositorio privado de Amazon ECR.	Otra pregunta es por qué el resumen proporcionado por el comando docker pull difiere del resumen del manifiesto de la imagen `<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest` . El resumen utilizado para docker pull representa el resumen del manifiesto de la imagen, que se almacena en un registro. Este resumen se considera la raíz de una cadena de hash, porque el manifiesto contiene el hash del contenido que se descargará e importará a Docker. El ID de imagen utilizado en Docker se encuentra en este manifiesto como `config.digest` . Representa la configuración de imagen que usa Docker. Por lo tanto, se podría decir que el manifiesto es el sobre y la imagen es el contenido del sobre. El resumen del manifiesto siempre es diferente del ID de la imagen. Sin embargo, un manifiesto específico	AWS DevOps, administrador de sistemas de AWS, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	siempre debe producir el mismo ID de imagen. Como el resumen del manifiesto es una cadena de hash, no podemos garantizar que siempre sea igual para un ID de imagen determinado. En la mayoría de los casos, produce el mismo resumen, aunque Docker no puede garantizarlo. La posible diferencia en el resumen del manifiesto se debe a que Docker no almacena localmente los blobs comprimidos con gzip. Por lo tanto, la exportación de capas puede producir un resumen diferente, aunque el contenido sin comprimir siga siendo el mismo. El ID de imagen comprueba que el contenido sin comprimir es el mismo; es decir, el ID de imagen es ahora un identificador de contenido direccionable (`chainID`). Para confirmar esta información, puede comparar el resultado del comando docker inspect en los repositorios públicos y privados de Amazon ECR:	

Tarea	Descripción	Habilidades requeridas

	1. Ejecute el siguiente comando desde el terminal para la imagen almacenada en el repositorio público de Amazon ECR.
	
	`$~ % docker inspect public.ecr.aws/amazonlinux/amazonlinux:2018.03`
	
	Para ver un ejemplo de comando, consulte la sección Información adicional.
	2. Ejecute el siguiente comando desde el terminal para la imagen almacenada en el repositorio privado de Amazon ECR.
	
	`$~ % docker inspect <account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	
	Para ver un ejemplo de comando, consulte la sección Información adicional.
	
	Los resultados verifican que ambas imágenes tienen el	

Tarea	Descripción	Habilidades requeridas
	mismo resumen de ID de imagen y resumen de capa. ID: `f7cee5e1af28ad4e147589c474d399b12d9b551ef4c3e11e02d982fce5eebc68` Capas: `d5655967c2c4e8d68f8ec7cf753218938669e6c16ac1324303c073c736a2e2a2` Además, los resúmenes se basan en los bytes del objeto que se administra localmente (el archivo local es un tar de la capa de imágenes de contenedor) o en el blob que se inserta en el servidor de registro. Sin embargo, al insertar el blob en un registro, el tar se comprime y el resumen se calcula en el archivo tar comprimido. Por lo tanto, la diferencia en el valor del resumen de extracción de docker se debe a la compresión que se aplica a nivel de registro (Amazon ECR privado o público). **Note** Esta explicación es específica del uso de	

Tarea	Descripción	Habilidades requeridas
	un cliente Docker. No verá este comportamiento en otros clientes, como nerdctl o Finch, porque no comprimen automáticamente la imagen durante las operaciones de inserción y extracción.	

Identificación automática de las imágenes duplicadas entre los repositorios públicos y privados de Amazon ECR

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Clone el repositorio de GitHub para este patrón en una carpeta local: `$git clone https://github.com/aws-samples/automated-solution-to-identify-duplicate-container-images-between-repositories`	Administrador de AWS, AWS DevOps
Configure una CI/CD canalización.	El GitHub repositorio incluye un `.yaml` archivo que crea una CloudFormation pila para configurar una canalización AWS CodePipeline. 1. Inicie sesión en la CloudFormation consola	Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Consola de administración de AWS y ábrala. 2. Cree una pila con el archivo `pipeline.yaml` de plantilla, que se encuentra en la carpeta `code` del repositorio clonado. 3. Acepte o cambie los valores predeterminados de los parámetros. Especifique los valores para los siguientes campos: • Nombre de pila • `ArtifactStoreBucketName` — Un depósito de S3 existente que se utilizará para almacenar AWS CodePipeline artefactos • `OutputBucket` — Un depósito de S3 existente que se utilizará URIs para almacenar las imágenes duplicadas • `SourceImageFile` — Un archivo de texto existente denominado `input.txt` que contiene la imagen URIs del repositorio público y que se comparará con el repositorio privado de Amazon ECR para detectar la duplicación	

Tarea	Descripción	Habilidades requeridas
	4. Revise y ajuste las opciones de pila y, a continuación, seleccione Enviar para ejecutar la plantilla. El proceso se configurará con dos etapas (CodeCommit y CodeBuild, como se muestra en el diagrama de arquitectura), para identificar las imágenes del repositorio privado que también existen en el repositorio público. La canalización está configurada con los siguientes recursos: • CodePipeline para la organización del proceso de despliegue. • Un CodeCommit repositorio para almacenar el script bash y el archivo de entrada. El script bash se usa para comparar la imagen del contenedor IDs en los repositorios público y privado para encontrar duplicaciones. Esta comprobación se realiza en todos los repositorios especificados Cuenta de AWS en uno solo. Región de AWS	

Tarea	Descripción	Habilidades requeridas
	• Un CodeBuild proyecto para invocar el script bash para identificar las imágenes que ya están presentes en el repositorio de Amazon ECR. • Roles de IAM necesarios para permitir el acceso. • Un bucket de S3 para almacenar el archivo de salida que contiene la imagen. URIs • Otro depósito de S3 para almacenar CodePipeline artefactos.	

Tarea	Descripción	Habilidades requeridas
Rellene el CodeCommit repositorio.	Para rellenar el CodeCommit repositorio, lleve a cabo estos pasos: 1. Abre la CodeCommit consola y navega hasta el Región de AWS lugar donde creaste la CloudFormation pila. 2. Busca el repositorio que aprovisionaste mediante el CloudFormation script de la lista, selecciona Clonar URL y, a continuación, copia el protocolo URL HTTPS para conectarte al repositorio. 3. Abra un símbolo del sistema y ejecute el comando git clone con la URL HTTPS que ha copiado en el paso anterior. 4. Vaya al directorio raíz. Cree un archivo con el nombre `input.txt` y rellénelo con el registro público de imágenes de Amazon ECR URIs que desee buscar en el repositorio privado de Amazon ECR. 5. Copie los archivos y `script.sh buildspec.yml` , `input.txt` desde su copia local,	Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas

	del GitHub repositorio. Solución automatizada para identificar las imágenes de contenedores duplicadas entre los repositorios y colocarlas en el repositorio clonado. CodeCommit
	6. Cargue los archivos en él CodeCommit mediante estos comandos:
	`git add .`
	`git commit -m "added input files"`
	`git push`	

Elimine recursos.	Para evitar incurrir en cargos en el futuro, elimine los recursos siguiendo estos pasos: 1. Navegue hasta el depósito de S3 que almacena los CodePipeline artefactos y vacíe el depósito. 2. Navegue hasta el depósito de S3 que almacena la imagen URIs duplicada y vacíe el depósito. 3. Ve a la CloudFormation consola y elimina la pila que creaste para configurar la canalización.	Administrador de AWS

Resolución de problemas

Problema	Solución
Cuando intentas insertar, extraer o interactuar con un CodeCommit repositorio desde el terminal o la línea de comandos, se te pide que proporciones un nombre de usuario y una contraseña, y debes proporcionar las credenciales de Git de tu usuario de IAM.	Las siguientes son las causas comunes para esto: • Su equipo local ejecuta un sistema operativo que no admite la administración de credenciales o no tiene instalada una utilidad de administración de credenciales. • Las credenciales de Git de su usuario de IAM no se han guardado en uno de estos sistemas de administración de credenciales. Según el sistema operativo y el entorno local, es posible que tenga que instalar un gestor de credenciales, configurar el gestor de credenciales que se incluye en el sistema operativo o personalizar su entorno local para utilizar el almacenamiento de credenciales. Por ejemplo, si su equipo ejecuta macOS, puede usar la utilidad Keychain Access para almacenar sus credenciales. Si su equipo utiliza Windows, puede utilizar el Administrador de credenciales de Git que se instala en Git para Windows. Para obtener más información, consulte Configuración para usuarios de HTTPS que utilizan credenciales de Git en la CodeCommit documentación y Almacenamiento de credenciales en la documentación de Git.
Al insertar una imagen en el repositorio de Amazon ECR, se producen errores HTTP 403 o “no basic auth credentials”.	Es posible que encuentre estos mensajes de error en los comandos docker push o docker pull, incluso si se ha autenticado correctamente

Problema	Solución
	en Docker mediante el comando aws ecr. get-login-password Las causas conocidas son: • Se ha autenticado en una región diferente . Para obtener más información, consulte Autenticación de registro privado en la documentación de Amazon ECR. • Se ha autenticado para insertar contenido en un repositorio para el que no tiene permisos. Para obtener más información, consulte Políticas de repositorios privados en la documentación de Amazon ECR. • Su token ha vencido. El periodo predeterm inado de vencimiento de los tokens obtenidos mediante la operación `GetAuthor izationToken` es de 12 horas.

Recursos relacionados

- Solución automatizada para identificar imágenes de contenedores duplicadas entre repositorios (repositorio) GitHub
- Galería pública de Amazon ECR
- Imágenes privadas en Amazon ECR (documentación de Amazon ECR)
- AWS::CodePipeline::Pipeline recurso (CloudFormation documentación)
- Especificación del formato de imagen OCI

Información adicional

Resultado de la inspección de Docker para una imagen en el repositorio público de Amazon ECR

```
[
    {
        "Id":
 "sha256:f7cee5e1af28ad4e147589c474d399b12d9b551ef4c3e11e02d982fce5eebc68",
```

```
        "RepoTags": [
            "<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest",
            "public.ecr.aws/amazonlinux/amazonlinux:2018.03"
        ],
        "RepoDigests": [
            "<account-id>.dkr.ecr.us-east-1.amazonaws.com/
test_ecr_repository@sha256:52db9000073d93b9bdee6a7246a68c35a741aaade05a8f4febba0bf795cdac02",
            "public.ecr.aws/amazonlinux/
amazonlinux@sha256:f972d24199508c52de7ad37a298bda35d8a1bd7df158149b381c03f6c6e363b5"
        ],
        "Parent": "",
        "Comment": "",
        "Created": "2023-02-23T06:20:11.575053226Z",
        "Container":
 "ec7f2fc7d2b6a382384061247ef603e7d647d65f5cd4fa397a3ccbba9278367c",
        "ContainerConfig": {
            "Hostname": "ec7f2fc7d2b6",
            "Domainname": "",
            "User": "",
            "AttachStdin": false,
            "AttachStdout": false,
            "AttachStderr": false,
            "Tty": false,
            "OpenStdin": false,
            "StdinOnce": false,
            "Env": [
                "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
            ],
            "Cmd": [
                "/bin/sh",
                "-c",
                "#(nop) ",
                "CMD [\"/bin/bash\"]"
            ],
            "Image":
 "sha256:c1bced1b5a65681e1e0e52d0a6ad17aaf76606149492ca0bf519a466ecb21e51",
            "Volumes": null,
            "WorkingDir": "",
            "Entrypoint": null,
            "OnBuild": null,
            "Labels": {}
        },
        "DockerVersion": "20.10.17",
        "Author": "",
```

```
        "Config": {
            "Hostname": "",
            "Domainname": "",
            "User": "",
            "AttachStdin": false,
            "AttachStdout": false,
            "AttachStderr": false,
            "Tty": false,
            "OpenStdin": false,
            "StdinOnce": false,
            "Env": [
                "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
            ],
            "Cmd": [
                "/bin/bash"
            ],
            "Image":
 "sha256:c1bced1b5a65681e1e0e52d0a6ad17aaf76606149492ca0bf519a466ecb21e51",
            "Volumes": null,
            "WorkingDir": "",
            "Entrypoint": null,
            "OnBuild": null,
            "Labels": null
        },
        "Architecture": "amd64",
        "Os": "linux",
        "Size": 167436755,
        "VirtualSize": 167436755,
        "GraphDriver": {
            "Data": {
                "MergedDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/merged",
                "UpperDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/diff",
                "WorkDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/work"
            },
            "Name": "overlay2"
        },
        "RootFS": {
            "Type": "layers",
            "Layers": [

 "sha256:d5655967c2c4e8d68f8ec7cf753218938669e6c16ac1324303c073c736a2e2a2"
```

```
            ]
        },
        "Metadata": {
            "LastTagTime": "2023-03-02T10:28:47.142155987Z"
        }
    }
]
```

Resultado de la inspección de Docker para una imagen en el repositorio privado de Amazon ECR

```
[
    {
        "Id":
 "sha256:f7cee5e1af28ad4e147589c474d399b12d9b551ef4c3e11e02d982fce5eebc68",
        "RepoTags": [
            "<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest",
            "public.ecr.aws/amazonlinux/amazonlinux:2018.03"
        ],
        "RepoDigests": [
            "<account-id>.dkr.ecr.us-east-1.amazonaws.com/
test_ecr_repository@sha256:52db9000073d93b9bdee6a7246a68c35a741aaade05a8f4febba0bf795cdac02",
            "public.ecr.aws/amazonlinux/
amazonlinux@sha256:f972d24199508c52de7ad37a298bda35d8a1bd7df158149b381c03f6c6e363b5"
        ],
        "Parent": "",
        "Comment": "",
        "Created": "2023-02-23T06:20:11.575053226Z",
        "Container":
 "ec7f2fc7d2b6a382384061247ef603e7d647d65f5cd4fa397a3ccbba9278367c",
        "ContainerConfig": {
            "Hostname": "ec7f2fc7d2b6",
            "Domainname": "",
            "User": "",
            "AttachStdin": false,
            "AttachStdout": false,
            "AttachStderr": false,
            "Tty": false,
            "OpenStdin": false,
            "StdinOnce": false,
            "Env": [
                "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
            ],
            "Cmd": [
```

```
                "/bin/sh",
                "-c",
                "#(nop) ",
                "CMD [\"/bin/bash\"]"
            ],
            "Image":
"sha256:c1bced1b5a65681e1e0e52d0a6ad17aaf76606149492ca0bf519a466ecb21e51",
            "Volumes": null,
            "WorkingDir": "",
            "Entrypoint": null,
            "OnBuild": null,
            "Labels": {}
        },
        "DockerVersion": "20.10.17",
        "Author": "",
        "Config": {
            "Hostname": "",
            "Domainname": "",
            "User": "",
            "AttachStdin": false,
            "AttachStdout": false,
            "AttachStderr": false,
            "Tty": false,
            "OpenStdin": false,
            "StdinOnce": false,
            "Env": [
                "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
            ],
            "Cmd": [
                "/bin/bash"
            ],
            "Image":
"sha256:c1bced1b5a65681e1e0e52d0a6ad17aaf76606149492ca0bf519a466ecb21e51",
            "Volumes": null,
            "WorkingDir": "",
            "Entrypoint": null,
            "OnBuild": null,
            "Labels": null
        },
        "Architecture": "amd64",
        "Os": "linux",
        "Size": 167436755,
        "VirtualSize": 167436755,
        "GraphDriver": {
```

```
            "Data": {
                "MergedDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/merged",
                "UpperDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/diff",
                "WorkDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/work"
            },
            "Name": "overlay2"
        },
        "RootFS": {
            "Type": "layers",
            "Layers": [

 "sha256:d5655967c2c4e8d68f8ec7cf753218938669e6c16ac1324303c073c736a2e2a2"
            ]
        },
        "Metadata": {
            "LastTagTime": "2023-03-02T10:28:47.142155987Z"
        }
    }
]
```

Instalación del agente SSM en los nodos de trabajo de Amazon EKS mediante Kubernetes DaemonSet

Mahendra Revanasiddappa, Amazon Web Services

Resumen

Nota, septiembre de 2021: La última versión optimizada para Amazon EKS AMIs instala SSM Agent automáticamente. Para obtener más información, consulte las notas de la versión de junio de 2021 AMIs.

En Amazon Elastic Kubernetes Service (Amazon EKS), debido a las directrices de seguridad, los nodos de trabajo no tienen pares de claves de Secure Shell (SSH) adjuntos. Este patrón muestra cómo puede usar el tipo de DaemonSet recurso Kubernetes para instalar AWS Systems Manager Agent (SSM Agent) en todos los nodos de trabajo, en lugar de instalarlo manualmente o reemplazar la Amazon Machine Image (AMI) de los nodos. DaemonSet utiliza una tarea automática en el nodo de trabajo para programar la instalación del agente SSM. También puede usar este patrón para instalar otros paquetes en los nodos de trabajo.

Al solucionar problemas en el clúster, instalar el agente SSM bajo demanda le permite establecer una sesión de SSH con el nodo de trabajo, recopilar registros o analizar la configuración de la instancia, sin pares de claves SSH.

Requisitos previos y limitaciones

Requisitos previos

- Un clúster de Amazon EKS existente con nodos de trabajo de Amazon Elastic Compute Cloud (Amazon EC2).
- Las instancias contenedoras deben tener los permisos necesarios para comunicarse con el servicio SSM. Amazon, la función gestionada por AWS Identity and Access Management (IAM), SSMManaged InstanceCore proporciona los permisos necesarios para que SSM Agent se ejecute en EC2 las instancias. Para obtener más información, consulte la documentación de AWS Systems Manager.

Limitaciones

- Este patrón no se aplica a AWS Fargate porque DaemonSets no es compatible con la plataforma Fargate.

- Este patrón solo se aplica a los nodos de trabajo basados en Linux.
- Los DaemonSet pods se ejecutan en modo privilegiado. Si el clúster de Amazon EKS tiene un webhook que bloquea los pods en modo privilegiado, el agente SSM no se instalará.

Arquitectura

El siguiente diagrama ilustra la arquitectura de este patrón.

Tools (Herramientas)

Herramientas

- kubectl es una utilidad de línea de comandos que se utiliza para interactuar con un clúster de Amazon EKS. Este patrón se utiliza `kubectl` para implementar un DaemonSet en el clúster de Amazon EKS, que instalará el agente SSM en todos los nodos de trabajo.
- Amazon EKS facilita la ejecución de Kubernetes en AWS sin tener que instalar, operar y mantener su propio plano o nodos de control de Kubernetes. Kubernetes es un sistema de código abierto para automatizar la implementación, el escalado y la administración de las aplicaciones en contenedores.
- El administrador de sesiones de AWS Systems Manager le permite administrar sus EC2 instancias, instancias locales y máquinas virtuales (VMs) mediante un shell interactivo basado en el navegador con un solo clic o mediante la interfaz de línea de comandos de AWS (AWS CLI).

Código

Utilice el siguiente código para crear un archivo de DaemonSet configuración que instalará el agente SSM en el clúster de Amazon EKS. Siga las instrucciones en la sección Epics.

```
cat << EOF > ssm_daemonset.yaml
apiVersion: apps/v1
kind: DaemonSet
metadata:
  labels:
    k8s-app: ssm-installer
  name: ssm-installer
  namespace: kube-system
spec:
  selector:
```

```
    matchLabels:
      k8s-app: ssm-installer
  template:
    metadata:
      labels:
        k8s-app: ssm-installer
    spec:
      containers:
      - name: sleeper
        image: busybox
        command: ['sh', '-c', 'echo I keep things running! && sleep 3600']
      initContainers:
      - image: amazonlinux
        imagePullPolicy: Always
        name: ssm
        command: ["/bin/bash"]
        args: ["-c","echo '* * * * * root yum install -y https://s3.amazonaws.com/
ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm & rm -rf /etc/
cron.d/ssmstart' > /etc/cron.d/ssmstart"]
        securityContext:
          allowPrivilegeEscalation: true
        volumeMounts:
        - mountPath: /etc/cron.d
          name: cronfile
        terminationMessagePath: /dev/termination-log
        terminationMessagePolicy: File
      volumes:
      - name: cronfile
        hostPath:
          path: /etc/cron.d
          type: Directory
      dnsPolicy: ClusterFirst
      restartPolicy: Always
      schedulerName: default-scheduler
      terminationGracePeriodSeconds: 30
EOF
```

Epics

Configurar kubectl

Tarea	Descripción	Habilidades requeridas
Instale y configure kubectl para acceder al clúster de EKS.	Si `kubectl` aún no está instalado y configurado para acceder al clúster de Amazon EKS, consulte Instalación de kubectl en la documentación de Amazon EKS.	DevOps

Implemente el DaemonSet

Tarea	Descripción	Habilidades requeridas
Cree el archivo DaemonSet de configuración.	Utilice el código de la sección Código que aparece anteriormente en este patrón para crear un archivo de DaemonSet configuración denominado `ossm_daemonset.yaml` , que se implementará en el clúster de Amazon EKS. El pod lanzado por DaemonSet tiene un contenedor principal y un `init` contenedor. El contenedor principal tiene un comando `sleep`. El contenedor `init` incluye una sección `command` que crea un archivo cron para instalar el agente SSM en la ruta `/etc/cron.d/` . El trabajo cron	DevOps

Tarea	Descripción	Habilidades requeridas
	se ejecuta solo una vez y el archivo que crea se elimina automáticamente una vez finalizado el trabajo. Cuando el contenedor de inicio ha terminado, el contenedor principal espera 60 minutos antes de salir. Después de 60 minutos, se lanza un nuevo pod. Este pod instala SSM Agent, si falta, o actualiza SSM Agent a la versión más reciente. Si es necesario, puede modificar el comando `sleep` para que se reinicie el pod una vez al día o para que se ejecute con más frecuencia.	
DaemonSet Despliéguelo en el clúster de Amazon EKS.	Para implementar el archivo de DaemonSet configuración que creó en el paso anterior en el clúster de Amazon EKS, utilice el siguiente comando: `kubectl apply -f ssm_daemonset.yaml` Este comando crea un DaemonSet para ejecutar los pods en los nodos de trabajo e instalar el agente SSM.	DevOps

Recursos relacionados

- Instalación de kubectl (documentación de Amazon EKS)
- Configuración del administrador de sesiones (documentación de AWS Systems Manager)

Instale el agente SSM y el CloudWatch agente en los nodos de trabajo de Amazon EKS mediante preBootstrapCommands

Akkamahadevi Hiremath, Amazon Web Services

Resumen

Este patrón proporciona ejemplos de código y pasos para instalar el agente de AWS Systems Manager (SSM Agent) y el agente de Amazon CloudWatch en los nodos de trabajo de Amazon Elastic Kubernetes Service (Amazon EKS) en la nube de Amazon Web Services (AWS) durante la creación del clúster de Amazon EKS. Puede instalar el agente SSM y el CloudWatch agente mediante la `preBootstrapCommands` propiedad del esquema del archivo de `eksctl` configuración (documentación de Weaveworks). Luego, puede usar el agente SSM para conectarse a sus nodos de trabajo sin usar un par de claves de Amazon Elastic Compute Cloud (Amazon EC2). Además, puede usar el CloudWatch agente para monitorear la utilización de memoria y disco en sus nodos de trabajo de Amazon EKS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- La utilidad de línea de comandos eksctl, instalada y configurada en macOS, Linux o Windows
- La utilidad de línea de comandos kubectl, instalada y configurada en macOS, Linux o Windows

Limitaciones

- Le recomendamos que evite añadir scripts de ejecución prolongada a la propiedad `preBootstrapCommands`, ya que esto retrasa la incorporación del nodo al clúster de Amazon EKS durante las actividades de escalado. En su lugar, le recomendamos que cree una imagen de máquina de Amazon Machine (AMI) personalizada.
- Este patrón se aplica únicamente a las instancias de Amazon EC2 Linux.

Arquitectura

Pila de tecnología

- Amazon CloudWatch
- Amazon Elastic Kubernetes Service (Amazon EKS)
- Almacén de parámetros de AWS Systems Manager

Arquitectura de destino

El siguiente diagrama muestra un ejemplo de un usuario que se conecta a los nodos de trabajo de Amazon EKS mediante el agente SSM, que se instaló mediante el`preBootstrapCommands`.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El usuario crea un clúster de Amazon EKS mediante el archivo de `eksctl` configuración con la `preBootstrapCommands` propiedad, que instala el agente y CloudWatch el agente de SSM.
2. Todas las instancias nuevas que se unan al clúster más adelante debido a actividades de escalado se crean con el agente y el agente SSM preinstalados. CloudWatch
3. El usuario se conecta a Amazon EC2 mediante el agente SSM y, a continuación, supervisa el uso de la memoria y el disco mediante el CloudWatch agente.

Tools (Herramientas)

- Amazon le CloudWatch ayuda a supervisar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar Kubernetes en AWS sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.
- El Almacén de parámetros de AWS Systems Manager proporciona un almacenamiento seguro y jerárquico para administrar los datos de configuración y los secretos.
- El administrador de sesiones de AWS Systems Manager lo ayuda a administrar sus EC2 instancias, instancias locales y máquinas virtuales mediante un shell interactivo basado en el navegador con un solo clic o mediante la interfaz de línea de comandos de AWS (AWS CLI).
- eksctl: es una utilidad sencilla de línea de comandos para crear y administrar clústeres de Kubernetes en Amazon EKS.
- kubectl: es una utilidad de línea de comandos para comunicarse con el servidor de la API del clúster.

Epics

Crear un clúster de Amazon EKS

Tarea	Descripción	Habilidades requeridas
Guarde el archivo de configuración del agente CloudWatch .	Guarde el archivo de configuración del CloudWatch agente en el almacén de parámetros de AWS Systems Manager, en la región de AWS en la que desee crear su clúster de Amazon EKS. Para ello, cree un parámetro en el Almacén de parámetros de AWS Systems Manager y anote el nombre del parámetro (por ejemplo, `AmazonCloudwatch-linux`). Para obtener más información, consulte el ejemplo de código del archivo de configuración del CloudWatch agente en la sección de información adicional de este patrón.	DevOps ingeniero
Cree el archivo de configuración y el clúster de eksctl.	1. Cree un archivo `eksctl` de configuración que incluya los pasos de instalación del CloudWatch agente y del agente SSM. Para obtener más información, consulte el ejemplo de código del archivo de configuración eksctl en la sección de información adicional de este patrón.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	2. Crear un clúster ejecutando el comando `eksctl create cluster -f cluster.yaml` .	

Compruebe que el agente y el agente de SSM CloudWatch funcionan

Tarea	Descripción	Habilidades requeridas
Pruebe el agente de SSM.	Utilice SSH para conectarse a los nodos de su clúster de Amazon EKS mediante cualquiera de los métodos descritos en Iniciar una sesión en la documentación de AWS Systems Manager.	AWS DevOps
Pon a prueba el CloudWatch agente.	Utilice la CloudWatch consola para validar el CloudWatch agente: 1. Inicie sesión en la consola de administración de AWS y abra la consola de CloudWatch . 2. En el panel de navegación, expanda Métricas y seleccione Todas las étricas. 3. En el cuadro de búsqueda de la pestaña Examinar, introduzca CWAgent las métricas y, a continuación, selecciónelas para ver	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	las métricas de memoria y disco.	

Recursos relacionados

- Instalación y ejecución del CloudWatch agente en sus servidores (CloudWatch documentación de Amazon)
- Creación de un parámetro de Systems Manager (consola) (documentación de AWS Systems Manager)
- Crear el archivo de configuración del CloudWatch agente (CloudWatch documentación de Amazon)
- Iniciar una sesión (AWS CLI) (documentación de AWS Systems Manager)
- Inicio de una sesión (EC2 consola de Amazon) (documentación de AWS Systems Manager)

Información adicional

Ejemplo de archivo de configuración del CloudWatch agente

En el siguiente ejemplo, el CloudWatch agente está configurado para supervisar el uso del disco y la memoria en las instancias de Amazon Linux:

```
{
    "agent": {
        "metrics_collection_interval": 60,
        "run_as_user": "cwagent"
    },
    "metrics": {
        "append_dimensions": {
            "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
            "ImageId": "${aws:ImageId}",
            "InstanceId": "${aws:InstanceId}",
            "InstanceType": "${aws:InstanceType}"
        },
        "metrics_collected": {
            "disk": {
                "measurement": [
                    "used_percent"
```

```
                ],
                "metrics_collection_interval": 60,
                "resources": [
                    "*"
                ]
            },
            "mem": {
                "measurement": [
                    "mem_used_percent"
                ],
                "metrics_collection_interval": 60
            }
        }
    }
}
```

Ejemplo de archivo de configuración eksctl

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig
metadata:
  name: test
  region: us-east-2
  version: "1.24"
managedNodeGroups:
  - name: test
    minSize: 2
    maxSize: 4
    desiredCapacity: 2
    volumeSize: 20
    instanceType: t3.medium
    preBootstrapCommands:
    - sudo yum install amazon-ssm-agent -y
    - sudo systemctl enable amazon-ssm-agent
    - sudo systemctl start amazon-ssm-agent
    - sudo yum install amazon-cloudwatch-agent -y
    - sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-
config -m ec2 -s -c ssm:AmazonCloudwatch-linux
    iam:
      attachPolicyARNs:
        - arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy
        - arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy
        - arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly
```

```
        - arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
        - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

Detalles de código adicionales

- En la última línea de la propiedad `preBootstrapCommands`, `AmazonCloudwatch-linux` es el nombre del parámetro creado en el almacén de parámetros del Almacén de parámetros de AWS Systems Manager. Debe incluir `AmazonCloudwatch-linux` en el Almacén de parámetros de la misma región de AWS en la que creó el clúster de Amazon EKS. También puede especificar una ruta de archivo, pero le recomendamos que utilice Systems Manager para facilitar la automatización y la reutilización.
- Si las utiliza `preBootstrapCommands` en el archivo `eksctl` de configuración, verá dos plantillas de lanzamiento en la consola de administración de AWS. La primera plantilla de lanzamiento incluye los comandos especificados en `preBootstrapCommands`. La segunda plantilla incluye los comandos especificados `preBootstrapCommands` y los datos de usuario predeterminados de Amazon EKS. Estos datos son necesarios para que los nodos se unan al clúster. El grupo Auto Scaling del grupo de nodos utiliza estos datos de usuario para generar nuevas instancias.
- Si usa el atributo `iam` en el archivo de configuración `eksctl`, debe enumerar las políticas predeterminadas de Amazon EKS junto con cualquier política adicional requerida en las políticas de AWS Identity and Access Management (IAM) adjuntas. En el fragmento de código del paso Crear el clúster y el archivo de configuración eksctl, `AmazonSSMMangedInstanceCore` se añaden políticas adicionales para garantizar que el CloudWatch agente `CloudWatchAgentServerPolicy` y el agente SSM funcionen según lo previsto. Las políticas`AmazonEKSWorkerNodePolicy`, `AmazonEKS_CNI_Policy` y `AmazonEC2ContainerRegistryReadOnly` son políticas obligatorias necesarias para que el clúster de Amazon EKS funcione correctamente.

Migración de los controladores de entrada NGINX al activar el Modo automático de Amazon EKS

Olawale Olaleye y Shamanth Devagari, Amazon Web Services

Resumen

El Modo automático de EKS para Amazon Elastic Kubernetes Service (Amazon EKS) puede recudir la sobrecarga operativa de ejecutar cargas de trabajo en clústeres de Kubernetes. Este modo también le AWS permite configurar y administrar la infraestructura en su nombre. Al habilitar el Modo automático de EKS en un clúster existente, debe planificar cuidadosamente la migración de las configuraciones del controlador de entrada NGINX. Esto se debe a que la transferencia directa de los equilibradores de carga de red no es posible.

Puede utilizar una estrategia de blue/green despliegue para migrar una instancia de NGINX Ingress Controller al habilitar el modo automático de EKS en un clúster de Amazon EKS existente.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Un clúster de Amazon EKS que ejecuta la versión 1.29 de Kubernetes o una posterior
- Complementos de Amazon EKS que ejecutan versiones mínimas
- Versión más recientes de kubectl
- Una instancia del controlador de entrada de NGINX existente
- (Opcional) Una zona alojada en Amazon Route 53 para el desplazamiento de tráfico basado en DNS

Arquitectura

Un despliegue azul/verde es una estrategia de despliegue en la que se crean dos entornos separados pero idénticos. Blue/green las implementaciones ofrecen capacidades de liberación y reversión prácticamente nulas durante el tiempo de inactividad. La idea fundamental es desplazar el tráfico entre dos entornos idénticos que ejecutan versiones diferentes de la aplicación.

En la siguiente imagen se muestra la migración de los equilibradores de carga de red desde dos instancias diferentes del controlador de entrada NGINX al activar el Modo automático de EKS. Se

utiliza una blue/green implementación para transferir el tráfico entre los dos balanceadores de carga de red.

El espacio de nombres original es el espacio de nombres azul. Aquí es donde se ejecutan el servicio y la instancia originales del controlador de entrada NGINX, antes de activar el Modo automático de EKS. El servicio y la instancia originales se conectan a un equilibrador de carga de red que tiene un nombre de DNS configurado en Route 53. El controlador del equilibrador de carga de AWS implementó este equilibrador de carga de red en la nube privada virtual (VPC).

El diagrama muestra el siguiente flujo de trabajo para configurar un entorno para una implementación: blue/green

1. Instale y configure otra instancia del controlador de entrada NGINX en un espacio de nombres diferente, un espacio de nombres verde.
2. En Route 53, configure un nombre de DNS para un nuevo equilibrador de carga de red.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar AWS Kubernetes sin necesidad de instalar o mantener su propio plano de control o nodos de Kubernetes.
- Elastic Load Balancing permite distribuir el tráfico entrante de las aplicaciones o de la red entre varios destinos. Por ejemplo, puede distribuir el tráfico entre instancias, contenedores y direcciones IP de Amazon Elastic Compute Cloud (Amazon EC2) en una o más zonas de disponibilidad.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Otras herramientas

- Helm es un administrador de paquetes de código abierto para Kubernetes que le permite instalar y administrar aplicaciones en el clúster de Kubernetes.

- kubectl: una interfaz de la línea de comandos que le ayuda en la ejecución de comandos en clústeres de Kubernetes.
- El controlador de entrada NGINX conecta las aplicaciones y los servicios de Kubernetes con la gestión de solicitudes, la autenticación, los recursos personalizados de autoservicio y la depuración.

Epics

Revisión del entorno existente

Tarea	Descripción	Habilidades requeridas

Confirme que la instancia original del controlador de entrada NGINX esté operativa.	Ingrese el siguiente comando para verificar que los recursos del espacio de nombres `ingress-nginx` estén operativos. Si ha implement ado el controlador de entrada NGINX en otro espacio de nombres, actualice el nombre del espacio de nombres en este comando.
	`kubectl get all -n ingress-nginx`
	En la salida, confirme que el estado de los pods del controlador de entrada NGINX sea en ejecución. El siguiente es un ejemplo de output:
	`NAME READY STATUS RESTARTS AGE pod/ingress-nginx-admission-create-xqn9d`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	0/1 Completed 0 88m pod/ingress-nginx-admission-patch-lhk4j 0/1 Completed 1 88m pod/ingress-nginx-controller-68f68f859-xrz74 1/1 Running 2 (10m ago) 72m NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE service/ingress-nginx-controller LoadBalancer 10.100.67.255 k8s-ingressn-ingressn-abcdefg-12345.elb.eu-west-1.amazonaws.com 80:30330/TCP,443:31462/TCP 88m service/ingress-nginx-controller-admission ClusterIP 10.100.201.176 <none> 443/TCP 88m NAME	

Tarea	Descripción	Habilidades requeridas
	READY UP-TO-DATE AVAILABLE AGE deployment.apps/ingress-nginx-controller 1/1 1 1 88m NAME DESIRED CURRENT READY AGE replicaset.apps/ingress-nginx-controller-68f68f859 1 1 1 72m replicaset.apps/ingress-nginx-controller-d8c96cf68 0 0 0 88m NAME STATUS COMPLETIONS DURATION AGE job.batch/ingress-nginx-admission-create Complete 1/1 4s 88m job.batch/ingress-nginx-admission-patch Complete 1/1 5s 88m	

Implemente un ejemplo de HTTPd carga de trabajo para usar el controlador de entrada NGINX

Tarea	Descripción	Habilidades requeridas

Cree los recursos de Kubernetes.	Ingrese los siguientes comandos para crear un ejemplo de implement ación, servicio y entrada de Kubernetes:
	`kubectl create deploymen t demo --image=httpd --port=80`
	`kubectl expose deploymen t demo`
	`kubectl create ingress demo --class=nginx \ --rule nginxauto mode.local.dev/=de mo:80`
		DevOps ingeniero

Revise los recursos implement ados.	Ingrese el siguiente comando para ver una lista de los recursos implementados:
	`kubectl get all,ingress`
	En el resultado, confirme que el HTTPd pod de muestra está en ejecución. El siguiente es un ejemplo de output:
	`NAME READY STATUS RESTARTS AGE`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	pod/demo-7d94f8cb4f-q68wc 1/1 Running 0 59m NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE service/demo ClusterIP 10.100.78.155 <none> 80/TCP 59m service/kubernetes ClusterIP 10.100.0.1 <none> 443/TCP 117m NAME READY UP-TO-DATE AVAILABLE AGE deployment.apps/demo 1/1 1 1 59m NAME DESIRED CURRENT READY AGE replicaset.apps/demo-7d94f8cb4f 1 1 1 59m NAME CLASS HOSTS ADDRESS PORTS AGE ingress.networking.k8s.io/demo	

Tarea	Descripción	Habilidades requeridas
	`nginx nginxautomode.local.dev k8s-ingressn-ingressn-abcdefg-12345.elb.eu-west-1.amazonaws.com 80 56m`	

Confirme que se pueda acceder al servicio.	Ingrese el siguiente comando para confirmar que se pueda acceder al servicio a través del nombre de DNS del equilibrador de carga de red:
	`curl -H "Host: nginxautomode.local.dev" http://k8s-ingressn-ingressn-abcdefg-12345.elb.eu-west-1.amazonaws.com`
	La salida esperada es la siguiente:
	`<html><body><h1>It works!</h1></body></html>`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

(Opcional) Cree un registro de DNS.	1. Siga las instrucciones de Creating records by using the Amazon Route 53 console (documentación de Route 53) para crear un registro de DNS para el dominio configurado.
	2. Ingrese el siguiente comando para confirmar que se pueda acceder al servicio a través del nombre de dominio configurado:
	`curl "http://nginxautomode.local.dev/?[1-5]"`
	La salida esperada es la siguiente:
	`<html><body><h1>It works!</h1></body></html>`
	`<html><body><h1>It works!</h1></body></html>`
	`<html><body><h1>It works!</h1></body></html>`
	`<html><body><h1>It works!</h1></body></html>`
	`<html><body><h1>It works!</h1></body></html>`
		DevOps ingeniero, AWS DevOps

Cómo habilitar el modo automático de EKS en el clúster existente

Tarea	Descripción	Habilidades requeridas
Active el Modo automático de EKS.	Siga las instrucciones en Cómo habilitar el modo automático de EKS en un clúster existente (document ación de Amazon EKS).	AWS DevOps

Instalación de un nuevo controlador de entrada NGINX

Tarea	Descripción	Habilidades requeridas

Configure una nueva instancia del controlador de entrada NGINX.	1. Descargue la plantilla deploy.yaml.
	2. Abra la plantilla deploy.yaml en el editor que prefiera.
	3. En la sección `kind: Namespace` , ingrese un nombre único para el espacio de nombres, como `ingress-nginx-v2` :
	`apiVersion: v1`
	`kind: Namespace`
	`metadata:`
	`labels:`
	`app.kuber`
	`netes.io/instance:`
	`ingress-nginx`
	`app.kuber`
	`netes.io/name:`
	`ingress-nginx`
	`name: ingress-n`
	`ginx-v2`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	4. Para cada sección, actualice el valor `namespace` con el nuevo nombre.
	5. En la sección `kind: Deployment`, haga lo siguiente:
	a. Ingrese un valor único para `--controller-class`, como `k8s.io/ingress-nginx-v2`.
	b. Ingrese un valor único para `--ingress-class`, como `nginx-v2`.
	`apiVersion: apps/v1`
	`kind: Deployment`
	`  name: ingress-nginx-controller`
	`  namespace: ingress-nginx-v2`
	`...`
	`    spec:`
	`      containers:`
	`      - args:`
	`        - /nginx-ingress-controller`
	`        - --publish-service=$(POD_NAMESPACE)/ingress-nginx-controller`
	`        - --election-id=ingress-nginx-leader`
	`        - --controller-class=k8s.io/ingress-nginx-v2`	

Tarea	Descripción	Habilidades requeridas

	<pre>- --ingress-class=nginx-v2</pre> 6. En la sección `kind: IngressClass` , ingrese los mismos valores para `--controller-class` y `--ingress-class` que utilizó en la sección anterior: <pre>apiVersion: networking.k8s.io/v1
	kind: IngressClass
	metadata:
	  labels:
	  app.kubernetes.io/component: controller
	  app.kubernetes.io/instance: ingress-nginx
	  app.kubernetes.io/name: ingress-nginx
	  app.kubernetes.io/part-of: ingress-nginx
	  app.kubernetes.io/version: 1.12.0
	  name: nginx-v2
	spec:
	  controller: k8s.io/ingress-nginx-v2</pre> 7. En la siguiente sección, agregue `loadBalancerClass: eks.amazonaws.com/nlb` para	

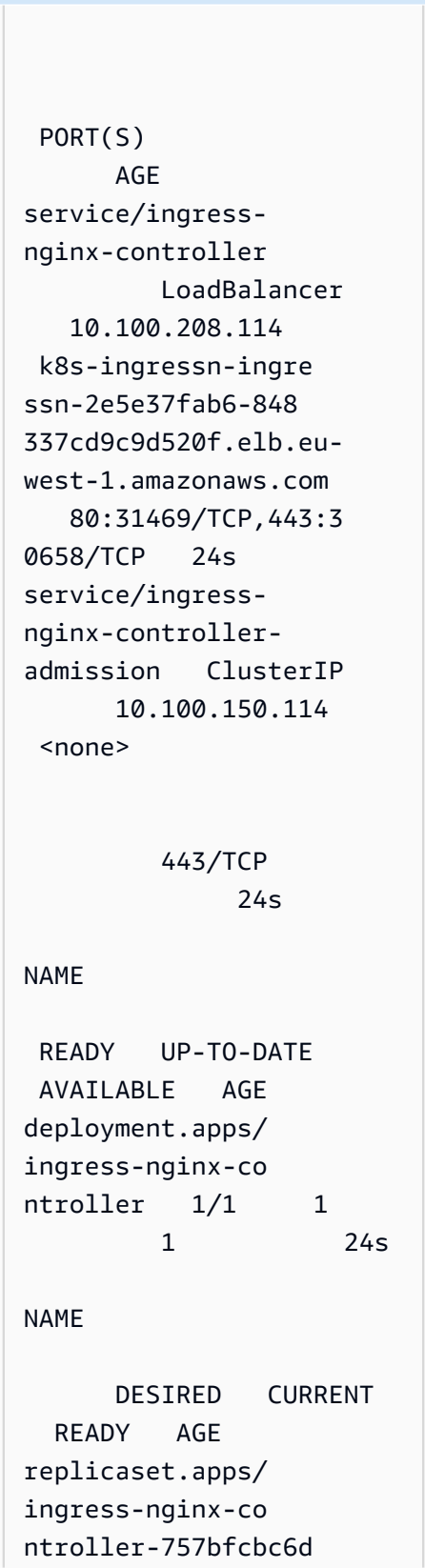
Tarea	Descripción	Habilidades requeridas

	aprovisionar un equilibrador de carga de red para la instancia de controlador de entrada NGINX:
	
	`apiVersion: v1`
	`kind: Service`
	`metadata:`
	`  name: ingress-nginx-controller`
	`  namespace: ingress-nginx-v2`
	`spec:`
	`...`
	`  selector:`
	`  app.kubernetes.io/component: controller`
	`  app.kubernetes.io/instance: ingress-nginx`
	`  app.kubernetes.io/name: ingress-nginx`
	`  type: LoadBalancer`
	`  loadBalancerClass: eks.amazonaws.com/nlb`
	
	8. Guarde y cierre la plantilla deploy.yaml.	

Implemente la nueva instancia del controlador de instancias NGINX.	Ingrese el siguiente comando para aplicar el archivo de manifiesto modificado: `kubectl apply -f deploy.yaml`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Confirme que la implement ación se haya llevado a cabo correctamente.	Ingrese el siguiente comando para verificar que los recursos del espacio de nombres `ingress-nginx-v2` estén operativos:
	`kubectl get all -n ingress-nginx-v2`
	En la salida, confirme que el estado de los pods del controlador de entrada NGINX sea en ejecución. El siguiente es un ejemplo de output:
	`NAME READY STATUS RESTARTS AGE pod/ingress-nginx-admission-create-7shrj 0/1 Completed 0 24s pod/ingress-nginx-admission-patch-vkxr5 0/1 Completed 1 24s pod/ingress-nginx-controller-757bfcbc6d-4fw52 1/1 Running 0 24s NAME TYPE CLUSTER-IP EXTERNAL-IP`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
		

Tarea	Descripción	Habilidades requeridas

	`1 1 1 24s`
	
	`NAME`
	
	`STATUS COMPLETIONS DURATION AGE`
	`job.batch/ingress-nginx-admission-create Complete 1/1 4s 24s`
	`job.batch/ingress-nginx-admission-patch Complete 1/1 5s 24s`	

Cree una nueva entrada para la HTTPd carga de trabajo de muestra.	Introduzca el siguiente comando para crear una nueva entrada para la carga de trabajo de muestra HTTPd existente: `kubectl create ingress demo-new --class=nginx-v2 \ --rule nginxautomode.local.dev/=demo:80`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Confirme que la nueva entrada funcione.	Ingrese el siguiente comando para confirmar que la nueva entrada funcione:
	`curl -H "Host: nginxautomode.local.dev" k8s-ingressn-ingressn-2e5e37fab6-848337cd9c9d520f.elb.eu-west-1.amazonaws.com`
	La salida esperada es la siguiente:
	`<html><body><h1>It works!</h1></body></html>`
		DevOps ingeniero

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Haga la transición al nuevo espacio de nombres.	1. (Opcional) Siga las instrucciones de Editing records (documentación de Route 53) para actualizar el registro de DNS. 2. Cuando haya confirmado que la nueva instancia del controlador de entrada NGINX funcione según lo previsto, elimine la original. 3. Elimine el AWS Load Balancer Controller	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	autogestionado. Para obtener instrucciones, consulte Migración de aplicaciones desde el Controlador de entrada de ALB obsoleto (document ación de Amazon EKS). 4. Vacíe los grupos de nodos administrados. Para obtener instrucci ones, consulte Deleting and draining node groups (documentación de eksctl).	

Tarea	Descripción	Habilidades requeridas

Revise las dos entradas.	Introduzca el siguiente comando para revisar las dos entradas que se crearon para la HTTPd carga de trabajo de muestra:
	`kubectl get ingress`
	El siguiente es un ejemplo de output:
	`NAME  CLASS  HOSTS  ADDRESS  PORTS  AGE`
	`demo  nginx  nginxautomode.local.dev  k8s-ingressn-ingressn-abcdefg-12345.elb.eu-west-1.amazonaws.com  80  95m`
	`demo-new  nginx-v2  nginxautomode.local.dev  k8s-ingressn-ingressn-2e5e37fab6-848337cd9c9d520f.elb.eu-west-1.amazonaws.com  80  33s`
		DevOps ingeniero

Recursos relacionados

- Cómo habilitar el modo automático de EKS en un clúster existente (documentación de Amazon EKS)
- Solucione los problemas de los balanceadores de carga creados por el controlador de servicios de Kubernetes en Amazon EKS (re:POST Knowledge Center)AWS
- NGINX Ingress Controller (documentación de NGINX)

Migre sus cargas de trabajo de contenedores de Azure Red Hat OpenShift (ARO) a Red Hat OpenShift Service en AWS (ROSA)

Naveen Ramasamy, Srikanth Rangavajhala y Gireesh Sreekantan, Amazon Web Services

Resumen

Este patrón proporciona step-by-step instrucciones para migrar cargas de trabajo en contenedores de Azure Red Hat (ARO) a (ROSA). OpenShift Red Hat OpenShift Service en AWS ROSA es un servicio de Kubernetes gestionado que proporciona Red Hat en colaboración con. AWS Le ayuda a implementar, administrar y escalar sus aplicaciones en contenedores mediante el uso de la plataforma Kubernetes, y se beneficia tanto de la experiencia de Red Hat en Kubernetes como en la infraestructura. Nube de AWS

La migración de cargas de trabajo de contenedores desde ARO, otras nubes o entornos en las instalaciones a ROSA implica la transferencia de aplicaciones, configuraciones y datos de una plataforma a otra. Este patrón ayuda a garantizar una transición fluida y, al mismo tiempo, optimiza los servicios, la seguridad y la rentabilidad Nube de AWS . Abarca dos métodos para migrar sus cargas de trabajo a clústeres ROSA: CI/CD y el kit de herramientas de migración para contenedores (MTC).

En este patrón se tratan ambos métodos. El método que elija depende de la complejidad y la certeza del proceso de migración. Si tiene el control total sobre el estado de su aplicación y puede garantizar una configuración uniforme a través de una canalización, le recomendamos que utilice este método. CI/CD Sin embargo, si el estado de la aplicación implica incertidumbres, cambios imprevistos o un ecosistema complejo, le recomendamos que utilice MTC como una ruta fiable y controlada para migrar la aplicación y sus datos a un nuevo clúster. Para obtener una comparación detallada de los dos métodos, consulte la sección Información adicional.

Beneficios de la migración a ROSA:

- ROSA se integra perfectamente AWS como un servicio nativo. Es fácilmente accesible a través de Consola de administración de AWS y se factura a través de una sola Cuenta de AWS. Ofrece total compatibilidad con otros Servicios de AWS y proporciona soporte colaborativo tanto por parte de Red Hat como por parte de ambos AWS .
- ROSA admite implementaciones híbridas y multinube. Permite que las aplicaciones se ejecuten de manera coherente en los centros de datos en las instalaciones y en varios entornos en la nube.

- ROSA se beneficia del enfoque de seguridad de Red Hat y ofrece características como el control de acceso basado en roles (RBAC), el escaneo de imágenes y las evaluaciones de vulnerabilidades para garantizar un entorno de contenedores seguro.
- ROSA se ha diseñado para escalar aplicaciones con facilidad y ofrece opciones de alta disponibilidad. Permite que las aplicaciones crezcan según sea necesario y, al mismo tiempo, mantiene la fiabilidad.
- ROSA automatiza y simplifica la implementación de un clúster de Kubernetes en comparación con los métodos de administración y configuración manuales. Esto acelera el proceso de desarrollo e implementación.
- ROSA se beneficia de los Nube de AWS servicios y proporciona una integración perfecta con AWS ofertas como los servicios de bases de datos, las soluciones de almacenamiento y los servicios de seguridad.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.
- Permisos configurados para los Servicios de AWS que ROSA confía para ofrecer funcionalidad. Para obtener más información, consulte Prerequisites en la documentación de ROSA.
- ROSA activado en la consola de ROSA. Para obtener instrucciones, consulte la documentación de ROSA.
- El clúster de ROSA instalado y configurado. Para obtener más información, consulte Get started with ROSA en la documentación de ROSA. Para comprender los diferentes métodos para configurar un clúster de ROSA, consulte la guía de orientación AWS prescriptiva sobre las estrategias de implementación de ROSA.
- La conectividad de red se establece desde la red local AWS hasta AWS Direct Connect(preferiblemente) o AWS Virtual Private Network (Site-to-Site VPN).
- Una instancia de Amazon Elastic Compute Cloud (Amazon EC2) u otro servidor virtual para instalar herramientas como `aws client` el cliente OpenShift CLI (`oc`), el cliente ROSA y el binario de Git.

Requisitos previos adicionales para el CI/CD método:

- Acceso al servidor Jenkins local con permisos para crear una nueva canalización, añadir etapas, añadir OpenShift clústeres y realizar compilaciones.
- Acceso al repositorio de Git en el que se mantiene el código fuente de la aplicación, con permisos para crear una nueva rama de Git y llevar a cabo confirmaciones en la nueva rama.

Requisitos previos adicionales para el método de MTC:

- Un bucket de Amazon Simple Storage Service (Amazon S3) que se utilizará como repositorio de replicación.
- Acceso administrativo al clúster de ARO de origen. Es necesario para configurar la conexión de MTC.

Limitaciones

- Algunos Servicios de AWS no están disponibles en todos. Regiones de AWS Para conocer la disponibilidad de las regiones, consulte Servicios de AWS by Region. Para los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

ROSA proporciona tres patrones de despliegue de red: pública, privada y AWS PrivateLink. PrivateLinkpermite a los equipos de ingeniería de confiabilidad de sitios (SRE) de Red Hat administrar el clúster mediante una subred privada conectada al PrivateLink punto final del clúster en una VPC existente.

La elección de PrivateLink esta opción proporciona la configuración más segura. Por ese motivo, la recomendamos para cargas de trabajo confidenciales o para requisitos de cumplimiento estrictos. Para obtener información sobre las opciones de implementación de redes públicas y privadas, consulte la OpenShift documentación de Red Hat.

> **Important**
>
> Puede crear un PrivateLink clúster solo en el momento de la instalación. No puede cambiar un clúster para usarlo PrivateLink después de la instalación.

El siguiente diagrama ilustra la PrivateLink arquitectura de un clúster ROSA que se utiliza Direct Connect para conectarse a los entornos locales y ARO.

AWS permisos para ROSA

Para obtener AWS permisos para ROSA, le recomendamos que utilice AWS Security Token Service (AWS STS) con tokens dinámicos de corta duración. Este método utiliza funciones y políticas predefinidas con privilegios mínimos para conceder a ROSA permisos mínimos para operar en la instalación Cuenta de AWS, el plano de control y las funciones informáticas de ROSA.

Reimplementación de la canalización de CI/CD

CI/CD pipeline redeployment is the recommended method for users who have a mature CI/CDcanalización. Si elige esta opción, puede utilizar cualquier estrategia de DevOps despliegue para trasladar gradualmente la carga de aplicaciones a los despliegues en ROSA.

> **Note**
>
> Este patrón supone un caso de uso común en el que tienes una canalización local de Git, JFrog Artifactory y Jenkins. Este enfoque requiere que establezcas la conectividad de red desde la red local AWS hasta Direct Connect ella y que configures el clúster ROSA antes de seguir las instrucciones de la sección Epics. Consulte la sección Requisitos previos para obtener los detalles.

En el siguiente diagrama se muestra el flujo de trabajo para este método.

Método MTC

Puede usar Migration Toolkit for Containers (MTC) para migrar cargas de trabajo en contenedores entre diferentes entornos de Kubernetes; por ejemplo, de ARO a ROSA. MTC simplifica el proceso de migración porque automatiza varias tareas clave y proporciona un marco completo para administrar el ciclo de vida de la migración.

En el siguiente diagrama se muestra el flujo de trabajo para este método.

Tools (Herramientas)

Servicios de AWS

- AWS DataSynces un servicio de transferencia y descubrimiento de datos en línea que le ayuda a mover archivos u datos de objetos hacia, desde y entre los servicios AWS de almacenamiento.
- AWS Direct Connectconecta la red interna a una Direct Connect ubicación a través de un cable Ethernet de fibra óptica estándar. Con esta conexión, puede crear interfaces virtuales directamente con las públicas y, al Servicios de AWS mismo tiempo, omitir a los proveedores de servicios de Internet en su ruta de red.
- AWS PrivateLinkle ayuda a crear conexiones unidireccionales y privadas desde sus nubes privadas virtuales (VPCs) a servicios externos a la VPC.
- Red Hat OpenShift Service en AWS (ROSA) es un servicio gestionado que ayuda a OpenShift los usuarios de Red Hat a crear, escalar y gestionar aplicaciones en contenedores. AWS
- AWS Security Token Service (AWS STS) le ayuda a solicitar credenciales temporales con privilegios limitados para los usuarios.

Otras herramientas

- Migration Toolkit for Containers (MTC) proporciona una consola y una API para migrar aplicaciones en contenedores de ARO a ROSA.

Prácticas recomendadas

- Para mayor resiliencia y si tiene cargas de trabajo que cumplen con las normas de seguridad, configure un clúster ROSA multizona de disponibilidad que utilice. PrivateLink Para obtener más información, consulte la documentación de ROSA.

> **Note**
>
> PrivateLink no se puede configurar después de la instalación.

- El bucket de S3 que utiliza como repositorio de replicación no debe ser público. Utilice las políticas de bucket de S3 adecuadas para restringir el acceso.
- Si elige el método MTC, utilice la opción de migración por etapas para reducir el tiempo de inactividad durante la transición.

- Revise las cuotas de servicio antes y después de aprovisionar el clúster de ROSA. Si es necesario, solicite un aumento de la cuota de acuerdo con sus requisitos. Para obtener más información, consulte la documentación de Service Quotas.
- Consulte ROSA security guidelines e implemente las prácticas recomendadas de seguridad.
- Le recomendamos eliminar el administrador de clústeres predeterminado después de la instalación. Para obtener más información, consulte la OpenShift documentación de Red Hat.
- Utilice el escalado automático del grupo de máquinas para reducir verticalmente los nodos de trabajo no utilizados en el clúster de ROSA a fin de optimizar los costos. Para obtener más información, consulte ROSA Workshop.
- Utilice el servicio de gestión de costes de Red Hat para OpenShift Container Platform para comprender mejor los costes de las nubes y los contenedores y realizar un seguimiento de los mismos. Para obtener más información, consulte ROSA Workshop.
- Supervise y audite los servicios y aplicaciones de infraestructura de clústeres de ROSA mediante el uso de Servicios de AWS. Para obtener más información, consulte ROSA Workshop.

Epics

Opción 1: utilizar una CI/CD canalización

Tarea	Descripción	Habilidades requeridas
Agregue el nuevo clúster de ROSA a Jenkins.	1. En la consola de Jenkins, elija Manage Jenkins, Configure System. 2. En la página Administr ar Jenkins, en la sección OpenShift Plug-in, selecciona Añadir un clúster nuevo. 3. Proporcione la informaci ón obligatoria, como el nombre del clúster, la URL del servidor de la API y la información del token, para autenticarse con ROSA.	Administrador de AWS, administrador de sistemas de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Agregue el cliente `oc` a sus nodos de Jenkins.	1. En la consola de Jenkins, elija Manage Jenkins, Global Tool Configuration. 2. En la sección Herramien tas de OpenShift cliente, instale la versión de cliente OpenShift CLI (`oc`) que es igual a la versión de clúster ROSA.	Administrador de AWS, administrador de sistemas de AWS, AWS DevOps
Cree una nueva rama de Git.	Cree una nueva rama en el repositorio de Git para `rosa-dev`. Esta rama separa los cambios en los parámetros de configuración o el código de ROSA de la canalización existente.	AWS DevOps
Etiquete las imágenes para ROSA.	En la etapa de compilación, utilice una etiqueta diferente para identificar las imágenes que se crearon a partir de la canalización de ROSA.	Administrador de AWS, administrador de sistemas de AWS, AWS DevOps
Crear una canalización.	Cree una nueva canalización de Jenkins que sea similar a la canalización existente . Para esta canalización, utilice la rama de Git `rosa-dev` que creó anteriormente y asegúrese de incluir las etapas de extracción, escaneo de código y compilación de Git que sean idénticas a las de la canalización existente.	Administrador de AWS, administrador de sistemas de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Agregue una etapa de implementación de ROSA.	En la nueva canalización, agregue una etapa de implementación en el clúster de ROSA y haga referencia al clúster de ROSA que agregó a la configuración global de Jenkins.	Administrador de AWS DevOps, administrador de sistemas de AWS
Inicie una nueva compilación.	En Jenkins, seleccione la canalización y elija Build now, o confirme un cambio en la rama `rosa-dev` en Git para iniciar una nueva complicac ión.	Administrador de AWS DevOps, administrador de sistemas de AWS
Comprobar la implementación.	Utilice el comando oc o la consola de ROSA para verificar que la aplicación se haya implementado en el clúster de ROSA de destino.	Administrador de AWS DevOps, administrador de sistemas de AWS
Copie los datos en el clúster de destino.	Para cargas de trabajo con estado, copie los datos del clúster de origen al clúster de destino mediante AWS DataSync utilidades de código abierto como rsync, o puede utilizar el método MTC. Para obtener más información, consulte la Documentación de AWS DataSync.	Administrador de AWS DevOps, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
Pruebe su aplicación.	1. Recupere la URL de la ruta de la aplicación mediante el comando oc route o la consola de ROSA. 2. Pruebe la aplicación mediante la URL de la ruta.	Administrador de AWS DevOps, administrador de sistemas de AWS
Lleve a cabo la transición.	Si las pruebas se llevan a cabo correctamente, utilice la política de Amazon Route 53 adecuada para trasladar el tráfico de la aplicación alojada en ARO a la aplicación alojada en ROSA. Cuando complete este paso, la carga de trabajo de la aplicación pasará por completo al clúster de ROSA.	Administrador AWS, administrador de sistemas AWS

Opción 2: uso de MTC

Tarea	Descripción	Habilidades requeridas
Instale el operador de MTC.	Instale el operador de MTC en los clústeres de ARO y ROSA: 1. En la consola ARO o ROSA, vaya a la OperatorHubpágina Operadores. 2. En el cuadro de palabras clave Filtrar por, busque o escriba MTC. 3. Seleccione el operador de MTC para mostrar información adicional.	Administrador de AWS DevOps, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	4. Tras leer la información sobre el operador, elija Instalar.	
Configure el tráfico de red al repositorio de replicación.	Si utiliza un servidor proxy, configúrelo para permitir el tráfico de red entre el repositorio de replicación y los clústeres. El repositorio de replicación es un objeto de almacenamiento intermedio que MTC utiliza para migrar datos. Los clústeres de origen y destino deben tener acceso de red al repositor io de replicación durante la migración.	Administrador de AWS DevOps, administrador de sistemas de AWS
Agregue el clúster de origen a MTC.	En la consola web de MTC, agregue el clúster de origen de ARO.	Administrador de AWS DevOps, administrador de sistemas de AWS
Agregue Amazon S3 como repositorio de replicación.	En la consola web de MTC, agregue el bucket de Amazon S3 (consulte Requisitos previos) como repositorio de replicación.	Administrador de AWS DevOps, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
Cree un plan de migración.	En la consola web de MTC, cree un plan de migración y especifique el tipo de transferencia de datos como Copy. Esto indicará a MTC que copie los datos del clúster de origen (ARO) al bucket de S3 y del bucket al clúster de destino (ROSA).	Administrador de AWS DevOps, administrador de sistemas de AWS
Ejecute el plan de migración.	Ejecute el plan de migración mediante la opción Stage o Cutover: • Elija Stage para copiar los datos al clúster de destino sin detener la aplicación. Puede ejecutar migraciones en varias etapas para copiar la mayoría de los datos antes de la migración de la transición. De este modo, se acorta la duración de la migración de la transición. • Elija Cutover para detener la aplicación en el clúster de origen y, al mismo tiempo, trasladar los recursos al clúster de destino. Para evitar que la aplicación se detenga, desactive la casilla Halt transactions on the source cluster during migration.	Administrador de AWS DevOps, administrador de sistemas de AWS

Resolución de problemas

Problema	Solución
Problemas de conectividad	Al migrar las cargas de trabajo de contenedo res de ARO a ROSA, es posible que se produzcan problemas de conectividad que deban resolverse para garantizar una migración satisfactoria. Para corregir estos problemas de conectividad (enumerados en esta tabla) durante la migración, es fundament al contar con una planificación meticulosa, coordinarse con los equipos de red y seguridad y llevar a cabo pruebas exhaustivas. La implementación de una estrategia de migración gradual y la verificación de la conectividad en cada paso ayudarán a minimizar las posibles interrupciones y a garantizar una transición fluida de ARO a ROSA.
Diferencias de configuración de la red	ARO y ROSA pueden tener variaciones en sus configuraciones de red, como la configura ción de la red virtual (VNet), las subredes y las políticas de red. Para que la comunicación entre los servicios sea adecuada, asegúrese de que la configuración de red esté alineada entre las dos plataformas.
Reglas de firewall y grupo de seguridad	ROSA y ARO pueden tener una configura ción predeterminada de firewall y grupo de seguridad diferente. Asegúrese de ajustar y actualizar estas reglas para permitir el tráfico necesario a fin de mantener la conectividad entre los contenedores y los servicios durante la migración.

Problema	Solución
Cambios de dirección IP y DNS	Al migrar las cargas de trabajo, los nombres de DNS y las direcciones IP pueden cambiar. Reconfigure las aplicaciones que se basan en nombres DNS estáticos IPs o específicos.
Acceso a servicios externos	Si su aplicación depende de servicios externos, como bases de datos APIs, es posible que tenga que actualizar su configuración de conexión para asegurarse de que pueda comunicarse con los nuevos servicios de ROSA.
Configuración de Azure Private Link	Si utiliza Azure Private Link o servicios de puntos de conexión privados en ARO, necesitar á configurar la funcionalidad equivalente en ROSA para garantizar la conectividad privada entre los recursos.
Site-to-Site VPN o Direct Connect configura ción	Si ya Site-to-Site VPN existen Direct Connect conexiones entre su red local y ARO, necesitar á establecer conexiones similares con ROSA para una comunicación ininterrumpida con sus recursos locales.
Configuración del equilibrador de carga y entrada	Las configuraciones de los controladores de entrada y los equilibradores de carga pueden diferir entre ARO y ROSA. Vuelva a configurar estos ajustes para mantener el acceso externo a los servicios.
Gestión de TLS y certificados	Si las aplicaciones utilizan certificados SSL o TLS, asegúrese de que sean válidos y estén configurados correctamente en ROSA.

Problema	Solución
Acceso al registro de contenedores	Si los contenedores están alojados en un registro de contenedores externo, configure los permisos de acceso y autenticación adecuados para ROSA.
Supervisión y registro	Actualice las configuraciones de supervisión y registro para que reflejen la nueva infraestr uctura de ROSA para que pueda continuar supervisando el estado y el rendimiento de los contenedores de manera eficaz.

Recursos relacionados

AWSreferencias

- ¿Qué es Red Hat OpenShift Service en AWS? (documentación de ROSA)
- Get started with ROSA (documentación de ROSA)
- Red Hat OpenShift Service en AWS estrategias de implementación (orientación AWS prescriptiva)
- Red Hat OpenShift Service en AWS Now GA (AWS entrada de blog)
- ROSA Workshop
- ROSA FAQ
- ROSA Workshop FAQ
- Precios de ROSA

OpenShift Documentación de Red Hat

- Instalación rápida de un clúster en AWS
- Instalar un clúster AWS en una red restringida
- Instalación de un clúster AWS en una VPC existente
- Instalar un clúster en una infraestructura aprovisionada por el usuario mediante plantillas AWS CloudFormation
- Instalar un clúster AWS en una red restringida con una infraestructura aprovisionada por el usuario

- Instalar un clúster con personalizaciones AWS
- Introducción a la OpenShift CLI

Información adicional

Elegir entre las opciones de reimplementación de MTC y de CI/CD canalización

La migración de aplicaciones de un OpenShift clúster a otro requiere una cuidadosa consideración. Lo ideal sería que la transición fuera fluida mediante una CI/CD canalización para volver a implementar la aplicación y gestionar la migración de los volúmenes de datos persistentes. Sin embargo, en la práctica, una aplicación en ejecución en un clúster es susceptible a cambios imprevistos con el tiempo. Estos cambios pueden hacer que la aplicación se desvíe gradualmente de su estado de implementación original. MTC ofrece una solución para casos en los que el contenido exacto de un espacio de nombres es incierto y es importante migrar sin problemas todos los componentes de la aplicación a un nuevo clúster.

Para tomar la decisión correcta, es necesario evaluar el caso específico y sopesar los beneficios de cada enfoque. De este modo, puede garantizar una migración exitosa y fluida que se ajuste a sus necesidades y prioridades. A continuación, se comparan las directrices adicionales para elegir entre las dos opciones.

Reimplementación de la canalización de CI/CD

El método de CI/CD canalización es el enfoque recomendado si la aplicación se puede volver a implementar con confianza mediante una canalización. De este modo, se garantiza que la migración sea controlada, predecible y alineada con sus prácticas de implementación actuales. Si elige este método, puede utilizar estrategias de implementación azul/verde o implementación canario para trasladar la carga a implementaciones en ROSA. En este caso, este patrón supone que Jenkins orquesta las implementaciones de aplicaciones desde el entorno en las instalaciones.

Ventajas:

- No necesita acceso administrativo al clúster de ARO de origen ni implementar ningún operador en el clúster de origen o destino.
- Este enfoque le ayuda a cambiar el tráfico gradualmente mediante una estrategia. DevOps

Desventajas:

- Probar la funcionalidad de la aplicación requiere más esfuerzo.

- Si la aplicación contiene datos persistentes, se requieren pasos adicionales para copiar los datos mediante el uso de AWS DataSync otras herramientas.

Migración de MTC

En un entorno real, las aplicaciones en ejecución pueden sufrir cambios imprevistos que hacen que se alejen de la implementación inicial. Elija la opción de MTC cuando no conozca el estado actual de la aplicación en el clúster de origen. Por ejemplo, si el ecosistema de aplicaciones abarca varios componentes, configuraciones y volúmenes de almacenamiento de datos, le recomendamos que elija MTC para garantizar una migración completa que abarque la aplicación y todo su entorno.

Ventajas:

- MTC proporciona una copia de seguridad y restauración completas de la carga de trabajo.
- Copiará los datos persistentes del origen al destino mientras migra la carga de trabajo.
- No requiere acceso al repositorio de código fuente.

Desventajas:

- Necesita privilegios administrativos para instalar el operador de MTC en los clústeres de origen y destino.
- El DevOps equipo necesita formación para utilizar la herramienta MTC y realizar migraciones.

Ejecute tareas de Amazon ECS en Amazon WorkSpaces con Amazon ECS Anywhere

Akash Kumar, Amazon Web Services

Resumen

Amazon Elastic Container Service (Amazon ECS) Anywhere permite la implementación de tareas de Amazon ECS en cualquier entorno, incluida la infraestructura administrada por Amazon Web Services (AWS) y la infraestructura administrada por el cliente. Esto se puede hacer al tiempo que se utiliza un plano de control totalmente administrado por AWS que se ejecuta en la nube y que está siempre actualizado.

Las empresas suelen utilizar Amazon WorkSpaces para desarrollar aplicaciones basadas en contenedores. Para ello, se necesitó Amazon Elastic Compute Cloud (Amazon EC2) o AWS Fargate con un clúster de Amazon ECS para probar y ejecutar las tareas de ECS. Ahora, con Amazon ECS Anywhere, puede añadir Amazon WorkSpaces como instancias externas directamente a un clúster de ECS y ejecutar sus tareas directamente. Esto reduce el tiempo de desarrollo, ya que puede probar su contenedor con un clúster de ECS localmente en Amazon WorkSpaces. También puede ahorrar el costo de usar EC2 instancias de Fargate para probar sus aplicaciones de contenedores.

Este patrón muestra cómo implementar tareas de ECS en Amazon WorkSpaces con Amazon ECS Anywhere. Configura el clúster de ECS y utiliza AWS Directory Service Simple AD para lanzar el WorkSpaces. A continuación, la tarea ECS de ejemplo lanza NGINX en. WorkSpaces

Requisitos previos y limitaciones

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de AWS (AWS CLI)
- Credenciales de AWS configuradas en su máquina

Arquitectura

Pila de tecnología de destino

- Una nube privada virtual (VPC)
- Clúster de Amazon ECS
- Amazon WorkSpaces

- AWS Directory Service con AD Connector

Arquitectura de destino

La arquitectura incluye los siguientes servicios y recursos:

- Un clúster de ECS con subredes públicas y privadas en una VPC personalizada
- Simple AD en la VPC para proporcionar a los usuarios acceso a Amazon WorkSpaces
- Amazon WorkSpaces aprovisionó en la VPC mediante Simple AD
- AWS Systems Manager activado para añadir Amazon WorkSpaces como instancias gestionadas
- Con Amazon ECS y AWS Systems Manager Agent (SSM Agent), Amazon WorkSpaces agregó a Systems Manager y al clúster de ECS
- Un ejemplo de tarea de ECS para ejecutar WorkSpaces en el clúster de ECS

Tools (Herramientas)

- AWS Directory Service Simple Active Directory (Simple AD) es un directorio administrado de manera autónoma que utiliza tecnología de un servidor compatible con Active Directory de Samba 4. Simple AD ofrece un subconjunto de las funciones que ofrece AWS Managed Microsoft AD, incluida la capacidad de gestionar los usuarios y conectarse de forma segura a las EC2 instancias de Amazon.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores escalable y rápido que ayuda a ejecutar, detener y administrar contenedores en un clúster.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Systems Manager le permite administrar las aplicaciones y la infraestructura que se ejecutan en la nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo requerido para detectar y resolver problemas operativos y ayuda a utilizar y administrar los recursos de AWS a escala de manera segura.
- Amazon le WorkSpaces ayuda a aprovisionar escritorios Microsoft Windows o Amazon Linux virtuales basados en la nube para sus usuarios, conocidos como WorkSpaces. WorkSpaces elimina la necesidad de adquirir e implementar hardware o instalar software complejo.

Epics

Configurar el clúster de ECS

Tarea	Descripción	Habilidades requeridas
Crear y configurar el clúster de ECS.	Para crear el clúster de ECS, siga las instrucciones que figuran en la Documentación de AWS, que incluyen los siguientes pasos: • En Seleccione la compatibilidad de clústeres, elija Solo redes, que admitirá Amazon WorkSpace como instancia externa al clúster de ECS. • Elija crear una nueva VPC.	Arquitecto de la nube

Lanza Amazon WorkSpaces

Tarea	Descripción	Habilidades requeridas
Configura Simple AD y lanza Amazon WorkSpaces.	Para aprovisionar un directorio de Simple AD para su VPC recién creada e iniciar Amazon WorkSpaces, siga las instrucciones de la documentación de AWS.	Arquitecto de la nube

Configuración de AWS Systems Manager para entornos híbridos

Tarea	Descripción	Habilidades requeridas
Descargar los scripts adjuntos.	En su máquina local, descargue los archivos `ssm-`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	`trust-policy.json` y `ssm-activation.json` que se encuentran en la sección Archivos adjuntos.	

Agregar el rol de IAM.	Añada variables de entorno en función de los requisitos de su empresa.
	`export AWS_DEFAULT_REGION=${AWS_REGION_ID}`
	`export ROLE_NAME=${ECS_TASK_ROLE}`
	`export CLUSTER_NAME=${ECS_CLUSTER_NAME}`
	`export SERVICE_NAME=${ECS_CLUSTER_SERVICE_NAME}`
	Ejecutar el siguiente comando.
	`aws iam create-role --role-name $ROLE_NAME --assume-role-policy-document file://ssm-trust-policy.json`
		Arquitecto de la nube

Añade la SSMManaged InstanceCore política de Amazon a la función de IAM.	Ejecutar el siguiente comando. `aws iam attach-role-policy --role-name $ROLE_NAME --policy-arn arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Añada la política de Amazon EC2 ContainerServicefor EC2 Role al rol de IAM.	Ejecutar el siguiente comando. `aws iam attach-role-policy --role-name $ROLE_NAME --policy-arn arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`	Arquitecto de la nube
Comprobar el rol de IAM.	Para verificar el rol de IAM, ejecute el siguiente comando. `aws iam list-attached-role-policies --role-name $ROLE_NAME`	Arquitecto de la nube
Activar Systems Manager.	Ejecutar el siguiente comando. `aws ssm create-activation --iam-role $ROLE_NAME | tee ssm-activation.json`	Arquitecto de la nube

WorkSpaces Añádala al clúster de ECS

Tarea	Descripción	Habilidades requeridas
Conéctese a su WorkSpaces.	Para conectarse a sus Workspaces y configurarlos, siga las instrucciones que figuran en la Documentación de AWS.	Desarrollador de aplicaciones
Descargar el script de instalación ecs-anywhere.	En el símbolo del sistema, ejecute el siguiente comando.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`curl -o "ecs-anywhere-install.sh" "https://amazon-ecs-agent-packages-preview.s3.us-east-1.amazonaws.com/ecs-anywhere-install.sh" && sudo chmod +x ecs-anywhere-install.sh`	
Comprobar la integridad del script del intérprete de comandos.	Ejecutar el siguiente comando (opcional). `curl -o "ecs-anywhere-install.sh.sha256" "https://amazon-ecs-agent-packages-preview.s3.us-east-1.amazonaws.com/ecs-anywhere-install.sh.sha256" && sha256sum -c ecs-anywhere-install.sh.sha256`	Desarrollador de aplicaciones
Agregar un repositorio EPEL en Amazon Linux.	Para agregar un repositorio Extra Packages for Enterprise Linux (EPEL), ejecute el comando `sudo amazon-linux-extras install epel -y`.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Instalar Amazon ECS Anywhere.	Para ejecutar el script de instalación, utilice el siguiente comando. `sudo ./ecs-anywhere-install.sh --cluster $CLUSTER_NAME --activation-id $ACTIVATION_ID --activation-code $ACTIVATION_CODE --region $AWS_REGION`	
Comprobar la información de la instancia desde el clúster de ECS.	Para comprobar la información de las instancias del clúster de Systems Manager y ECS y validar las que WorkSpaces se agregaron al clúster, ejecute el siguiente comando desde su máquina local. `aws ssm describe-instance-information" && "aws ecs list-container-instances --cluster $CLUSTER_NAME`	Desarrollador de aplicaciones

Agregue una tarea de ECS para el WorkSpaces

Tarea	Descripción	Habilidades requeridas
Para crear un rol de IAM de ejecución de tareas.	Descargue `task-execution-assume-role.json` y `external-task-`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	`definition.json` desde la sección Archivos adjuntos. Ejecute el siguiente comando en su equipo local. `aws iam --region $AWS_DEFAULT_REGION create-role --role-name $ECS_TASK_EXECUTION_ROLE --assume-role-policy-document file://task-execution-assume-role.json`	
Agregue la política al rol de ejecución.	Ejecutar el siguiente comando. `aws iam --region $AWS_DEFAULT_REGION attach-role-policy --role-name $ECS_TASK_EXECUTION_ROLE --policy-arn arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Crear un rol de tarea.	Ejecutar el siguiente comando. `aws iam --region $AWS_DEFAULT_REGION create-role --role-name $ECS_TASK_EXECUTION_ROLE --assume-role-policy-document file://task-execution-assume-role.json`	Arquitecto de la nube
Registrar la definición de tareas en el clúster.	Ejecute el siguiente comando en su equipo local. `aws ecs register-task-definition --cli-input-json file://external-task-definition.json`	Arquitecto de la nube
Ejecutar la tarea.	Ejecute el siguiente comando en su equipo local. `aws ecs run-task --cluster $CLUSTER_NAME --launch-type EXTERNAL --task-definition nginx`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas

Validar el estado de ejecución de la tarea.	Para obtener el ID de la tarea, ejecute el siguiente comando.
	`export TEST_TASKID= $(aws ecs list-tasks -- cluster $CLUSTER_NAME | jq -r '.taskArns[0]')`
	Ejecute el siguiente comando con el ID de la tarea.
	`aws ecs describe-tasks --cluster $CLUSTER_ NAME --tasks ${TEST_TA SKID}`
		Arquitecto de la nube

Compruebe la tarea en WorkSpace.	Para comprobar que NGINX se está ejecutando en WorkSpace, ejecute el comando. `curl http://lo calhost:8080`	Desarrollador de aplicaciones

Recursos relacionados

- Clúster de ECS
- Configurar un entorno híbrido
- Amazon WorkSpaces
- AD sencillo

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Ejecute un contenedor Docker de la API web de ASP.NET Core en una instancia de Amazon Linux EC2

Vijai Anand Ramalingam y Sreelaxmi Pai, Amazon Web Services

Resumen

Este patrón es para personas que están empezando a colocar en contenedores sus aplicaciones en la nube de Amazon Web Services (AWS). Cuando empiezaa a colocar aplicaciones en contenedores en la nube, normalmente no hay ninguna plataforma de orquestación de contenedores configurada. Este patrón le ayuda a configurar rápidamente la infraestructura en AWS para probar sus aplicaciones en contenedores sin necesidad de una infraestructura compleja de orquestación de contenedores.

El primer paso en el proceso de modernización es transformar la aplicación. Si se trata de una aplicación antigua de .NET Framework, primero debe cambiar el tiempo de ejecución a ASP.NET Core. A continuación, proceda del modo siguiente:

- Cree la imagen del contenedor de Docker
- Ejecute el contenedor de Docker con la imagen compilada
- Valide la aplicación antes de implementarla en cualquier plataforma de orquestación de contenedores, como Amazon Elastic Container Service (Amazon ECS) o Amazon Elastic Kubernetes Service (Amazon EKS).

Este patrón cubre los aspectos de creación, ejecución y validación del desarrollo de aplicaciones modernas en una instancia Linux de Amazon Elastic Compute Cloud (Amazon EC2).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa
- Un rol de AWS Identity and Access Management (IAM) con acceso suficiente para crear recursos de AWS para este patrón
- Se descargó e instaló Visual Studio Community 2022 o posterior
- Un proyecto de .NET Framework modernizado a ASP.NET Core
- Un GitHub repositorio

Versiones de producto

- Visual Studio Community 2022 o posterior

Arquitectura

Arquitectura de destino

Este patrón utiliza una CloudFormation plantilla de AWS para crear la arquitectura de alta disponibilidad que se muestra en el siguiente diagrama. Se lanza una instancia de Amazon EC2 Linux en una subred privada. El administrador de sesiones de AWS Systems Manager se utiliza para acceder a la instancia privada de Amazon EC2 Linux y para probar la API que se ejecuta en el contenedor de Docker.

1. Acceso a la instancia de Linux a través de Session Manager

Tools (Herramientas)

Servicios de AWS

- Interfaz de la línea de comandos de AWS: la Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos. Con una configuración mínima, puede utilizar comandos de CLI de AWS que implementen una funcionalidad equivalente a la que ofrece la consola de administración de AWS basada en navegador.
- Consola de administración de AWS: la consola de administración de AWS es una aplicación web que engloba y hace referencia a un amplio conjunto de consolas de servicios para la administración de recursos de AWS. La primera vez que inicie sesión, verá la página de inicio de la consola. La página de inicio proporciona acceso a la consola de cada servicio y ofrece un único lugar para acceder a la información que necesita para realizar sus tareas relacionadas con AWS.
- Administrador de sesiones de AWS Systems Manager: el administrador de sesiones es una funcionalidad de AWS Systems Manager totalmente gestionada. Con Session Manager, puede gestionar sus instancias de Amazon Elastic Compute Cloud (Amazon EC2). El administrador de sesiones proporciona una administración de nodos segura y auditable sin necesidad de abrir puertos de entrada, mantener los hosts bastiones ni administrar las claves SSH.

Otras herramientas

- Visual Studio 2022: Visual Studio 2022 es un entorno de desarrollo integrado (IDE).
- Docker: Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización a nivel del sistema operativo para entregar software en contenedores.

Código

```
FROM mcr.microsoft.com/dotnet/aspnet:5.0 AS base
 WORKDIR /app
EXPOSE 80
EXPOSE 443

FROM mcr.microsoft.com/dotnet/sdk:5.0 AS build
WORKDIR /src
COPY ["DemoNetCoreWebAPI/DemoNetCoreWebAPI.csproj", "DemoNetCoreWebAPI/"]
RUN dotnet restore "DemoNetCoreWebAPI/DemoNetCoreWebAPI.csproj"
COPY . .
WORKDIR "/src/DemoNetCoreWebAPI"
RUN dotnet build "DemoNetCoreWebAPI.csproj" -c Release -o /app/build

FROM build AS publish
RUN dotnet publish "DemoNetCoreWebAPI.csproj" -c Release -o /app/publish

FROM base AS final
WORKDIR /app
COPY --from=publish /app/publish .
ENTRYPOINT ["dotnet", "DemoNetCoreWebAPI.dll"]
```

Epics

Desarrollar la API web de ASP.NET Core

Tarea	Descripción	Habilidades requeridas
Cree un ejemplo de API web de ASP.NET Core con Visual Studio.	Para crear una API web de ASP.NET Core de ejemplo, haga lo siguiente: 1. Open Visual Studio 2022.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	2. Elija Crear un proyecto nuevo.
	3. Seleccione la plantilla de proyecto de la API web de ASP.NET Core y elija Siguiente.
	4. Para el nombre del proyecto, ingresa DemoNetCoreWebAPI y selecciona Siguiente.
	5. Seleccione Crear.
	6. Para ejecutar el proyecto localmente, presione F5.
	7. Compruebe que el punto final de la WeatherFo recastAPI predeterminado devuelva los resultados mediante Swagger.
	8. Abra la línea de comandos, vaya a la carpeta del proyecto .csproj y ejecute los siguientes comandos para enviar la nueva API web a su repositorio. GitHub
	`git add --all`
	`git commit -m "Initial Version"`
	`git push`	

Tarea	Descripción	Habilidades requeridas
Cree un Dockerfile.	Para crear un archivo Dockerfile, realice una de las siguientes acciones: • Cree el archivo Dockerfile manualmente usando el Dockerfile de ejemplo de la sección Código. Según los requisitos, seleccione la imagen base de .NET adecuada. Para obtener información sobre las imágenes relacionadas con .NET y ASP.NET Core, consulte Centro Docker. • Cree el archivo Dockerfile con Visual Studio y Escritorio Docker. En el explorador de soluciones, haga clic con el botón derecho del proyecto y seleccione Agregar -> Soporte Docker. Para OS de destino, seleccione Linux. Asegúrese de que el nuevo Dockerfile esté en la misma ruta que el archivo de la solución (.sln). Para enviar los cambios a tu GitHub repositorio, ejecuta el siguiente comando. `git add --all`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`git commit -m "Dockerfile added"` `git push`	

Configurar la instancia de Amazon EC2 Linux

Tarea	Descripción	Habilidades requeridas
Configure la infraestructura.	Lance la CloudFormation plantilla de AWS para crear la infraestructura, que incluye lo siguiente: • Una nube privada virtual (VPC), que utiliza la Introducción a VPC de AWS, con dos subredes públicas y dos subredes privadas que abarcan dos zonas de disponibilidad. • El rol de IAM necesario para habilitar AWS Systems Manager. • En una de las subredes privadas, una instancia de demostración de Amazon Linux 2 con el agente SSM más reciente. Aunque esta instancia no tiene conectividad directa desde Internet, se puede acceder a ella de forma segura mediante el administrador de sesiones de AWS Systems Manager	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	sin necesidad de un host bastión. **Note** Se acerca el fin de la compatibilidad de Amazon Linux 2. Para obtener más información, consulte Amazon Linux 2 FAQs. Para obtener más información sobre cómo acceder a una EC2 instancia privada de Amazon mediante el Administrador de sesiones sin necesidad de un host bastión, consulta la entrada del blog Hacia un mundo sin bastiones.	

Tarea	Descripción	Habilidades requeridas
Inicie sesión en la instancia de Amazon EC2 Linux.	Para conectarse a la instancia de Amazon EC2 Linux en la subred privada, haga lo siguiente: 1. Abre la EC2 consola de Amazon. 2. En el panel de navegación, seleccione Instances (Instancias). 3. Seleccione la instancia de demostración de Amazon Linux 2 y elija Conectarse. **Note** Se acerca el fin de la compatibilidad de Amazon Linux 2. Para obtener más información, consulte Amazon Linux 2 FAQs. 4. Elija Session Manager. 5. Elija Conectarse para abrir una nueva ventana de terminal. 6. Ejecute el comando siguiente. `sudo su`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Instale e inicie Docker.	Para instalar e iniciar Docker en la instancia de Amazon EC2 Linux, haga lo siguiente:
	1. Para instalar Docker, ejecute el siguiente comando.
	`yum install -y docker`
	2. Para iniciar el servicio Docker, ejecute el comando siguiente.
	`service docker start`
	3. Para verificar la instalación de Docker, ejecute el siguiente comando.
	`docker info`
		Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas

Instale GitHub y clone el repositorio.	Para instalar Git en la instancia de Amazon EC2 Linux y clonar el repositor io desde GitHub ella, haz lo siguiente.
	1. Para instalar Git, ejecute el siguiente comando.
	`yum install git -y`
	2. Para clonar el repositor io, ejecute el siguiente comando.
	`git clone https://g ithub.com/<usernam e>/<repo-name>.git`
	3. Para ir al Dockerfile, ejecute el siguiente comando.
	`cd <repo-name>/DemoNe tCoreWebAPI/`
		Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas

Cree y ejecute el contenedor de Docker.	Para compilar la imagen de Docker y ejecutar el contenedor dentro de la instancia de Amazon EC2 Linux, haga lo siguiente:
	1. Para crear la imagen de Docker, ejecute el siguiente comando.
	`docker build -t aspnetcorewebapiimage -f Dockerfile .`
	2. Para ver todas las imágenes de Docker, ejecute el siguiente comando.
	`docker images`
	3. Para crear y ejecutar el contenedor, ejecute el siguiente comando.
	`docker run -d -p 80:80 --name aspnetcorewebapicontainer aspnetcorewebapiimage`
		Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Pruebe la API web

Tarea	Descripción	Habilidades requeridas
Pruebe la API web con el comando curl.	Para probar la API web, ejecute el siguiente comando. `curl -X GET "http://localhost/WeatherForecast" -H "accept: text/plain"` Verifique la respuesta de la API. **Note** Si usa Swagger de forma local, puede obtener los comandos curl de cada punto de conexión.	Desarrollador de aplicaciones

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Elimine todos los recursos.	Eliminar la pila para eliminar todos los recursos. Esto asegura que no se le cobre por ningún servicio que no utilice.	Administrador de AWS, AWS DevOps

Recursos relacionados

- Conectarse a la instancia de Linux desde Windows mediante PuTTY

- Crear una API web con ASP.NET Core
- Toward a bastion-less world

Ejecutar cargas de trabajo con estado y almacenamiento de datos persistente mediante Amazon EFS en Amazon EKS con AWS Fargate

Ricardo Morais, Rodrigo Bersa y Lucio Pereira, Amazon Web Services

Resumen

Este patrón proporciona orientación para habilitar Amazon Elastic File System (Amazon EFS) como dispositivo de almacenamiento para contenedores que usan Amazon Elastic Kubernetes Service (Amazon EKS), mediante AWS Fargate para aprovisionar sus recursos de computación.

La configuración descrita en este patrón sigue las prácticas recomendadas de seguridad y proporciona seguridad en reposo y seguridad en tránsito de forma predeterminada. Para cifrar su sistema de archivos Amazon EFS, utiliza una clave de AWS Key Management Service (AWS KMS), pero también puede especificar un alias de clave que gestione el proceso de creación de una clave de KMS.

Puede seguir los pasos de este patrón para crear un espacio de nombres y un perfil de Fargate para una aplicación proof-of-concept (PoC), instalar el controlador Amazon EFS Container Storage Interface (CSI) que se utiliza para integrar el clúster de Kubernetes con Amazon EFS, configurar la clase de almacenamiento e implementar la aplicación PoC. Estos pasos dan como resultado un sistema de archivos Amazon EFS que se comparte entre varias cargas de trabajo de Kubernetes y se ejecuta en Fargate. El patrón va acompañado de scripts que automatizan estos pasos.

Puede utilizar este patrón si quiere garantizar la persistencia de los datos en sus aplicaciones contenerizadas y evitar la pérdida de datos en las operaciones de escalado. Por ejemplo:

- DevOps herramientas: un escenario habitual es desarrollar una herramienta de integración y entrega continuas. CI/CD) strategy. In this case, you can use Amazon EFS as a shared file system to store configurations among different instances of the CI/CD tool or to store a cache (for example, an Apache Maven repository) for pipeline stages among different instances of the CI/CD
- Servidores web: un escenario habitual es utilizar Apache como servidor web HTTP. Puede utilizar Amazon EFS como un sistema de archivos compartidos para almacenar archivos estáticos que se comparten entre distintas instancias del servidor web. En este escenario de ejemplo, las modificaciones se aplican directamente al sistema de archivos en lugar de incluir los archivos estáticos en una imagen de Docker.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un clúster de Amazon EKS existente con la versión 1.17 o posterior de Kubernetes (probado hasta la versión 1.27)
- Un sistema de archivos Amazon EFS existente para vincular un Kubernetes StorageClass y aprovisionar sistemas de archivos de forma dinámica
- Permisos de administración de clústeres
- El contexto está configurado para apuntar al clúster de Amazon EKS deseado

Limitaciones

- Hay algunas limitaciones que se deben tener en cuenta al utilizar Amazon EKS con Fargate. Por ejemplo, no se admite el uso de algunas construcciones de Kubernetes, como los contenedores DaemonSets privilegiados. Para obtener más información sobre las limitaciones de Fargate, consulte Consideraciones sobre AWS Fargate en la documentación de Amazon EKS.
- El código que se proporciona con este patrón es compatible con estaciones de trabajo que ejecutan Linux o macOS.

Versiones de producto

- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2 o posterior
- La versión 1.0 o posterior del controlador de CSI de Amazon EFS (probado hasta la versión 2.4.8)
- La versión 0.24.0 o posterior de eksctl (probado hasta la versión 0.158.0)
- La versión 1.6 o posterior de jq
- La versión 1.17 o posterior de kubectl (probado hasta la versión 1.27)
- La versión 1.17 o posterior de Kubernetes (probado hasta la versión 1.27)

Arquitectura

La arquitectura de destino consta de la siguiente infraestructura:

- Una nube privada virtual (VPC)
- Dos zonas de disponibilidad.
- Una subred pública con una puerta de enlace de NAT que proporciona acceso a Internet.
- Una subred privada con un clúster de Amazon EKS y destinos de montaje de Amazon EFS (también conocidos como puntos de montaje)
- Amazon EFS para VPC

La siguiente es la infraestructura del entorno del clúster de Amazon EKS:

- Perfiles de AWS Fargate que admitan los constructos de Kubernetes en el espacio de nombres.
- Un espacio de nombres de Kubernetes con lo siguiente:
  - Dos pods de aplicaciones distribuidos en las zonas de disponibilidad.
  - Una solicitud de volumen persistente (PVC) vinculada a un volumen persistente (PV) en el clúster.
- Un PV de todo el clúster que esté enlazado a la PVC del espacio de nombres y que apunte a los destinos de montaje de Amazon EFS en la subred privada, fuera del clúster.

Tools (Herramientas)

Servicios de AWS

- Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que puede usar para interactuar con los servicios de AWS desde la línea de comandos.
- Amazon Elastic File System (Amazon EFS) le ayuda a crear y configurar sistemas de archivos compartidos en la nube de AWS. Siguiendo este patrón, proporciona un sistema de archivos simple, escalable, completamente administrado y compartido para su uso con Amazon EKS.
- Amazon Elastic Kubernetes Service (Amazon EKS) le permite poner en marcha Kubernetes en AWS sin necesidad de instalar ni operar sus propios clústeres.
- AWS Fargate es un motor de computación sin servidor para Amazon EKS. Crea y administra recursos de computación para sus aplicaciones de Kubernetes.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.

Otras herramientas

- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización a nivel del sistema operativo para entregar software en contenedores.
- eksctl: es una utilidad sencilla de línea de comandos para crear y administrar clústeres de Kubernetes en Amazon EKS.
- kubectl: una interfaz de la línea de comandos que le ayuda en la ejecución de comandos en clústeres de Kubernetes.
- jq es una herramienta de línea de comandos para analizar JSON.

Código

El código de este patrón se proporciona en la configuración de GitHub persistencia con Amazon EFS en Amazon EKS mediante el repositorio de AWS Fargate. Los scripts están organizados por epic, en las carpetas desde `epic01` hasta `epic06`, según el orden de la sección Epics de este patrón.

Prácticas recomendadas

La arquitectura de destino incluye los siguientes servicios y componentes, y sigue las prácticas recomendadas de Marco de AWS Well-Architected:

- Amazon EFS, que proporciona un sistema de archivos NFS elástico, simple, escalable y completamente administrado. Se utiliza como un sistema de archivos compartido entre todas las replicaciones de la aplicación PoC que se ejecutan en pods, que se distribuyen en las subredes privadas del clúster de Amazon EKS elegido.
- Un destino de montaje de Amazon EFS para cada subred privada. Esto proporciona redundancia por zona de disponibilidad dentro de la nube privada virtual (VPC) del clúster.
- Amazon EKS, que ejecuta las cargas de trabajo de Kubernetes. Debe aprovisionar un clúster de Amazon EKS antes de utilizar este patrón, tal y como se describe en la sección Requisitos previos.
- AWS KMS, que proporciona cifrado en reposo para el contenido almacenado en el sistema de archivos Amazon EFS.
- Fargate, que administra los recursos informáticos de los contenedores para que pueda centrarse en los requisitos empresariales y no en la carga de la infraestructura. El perfil de Fargate se crea para todas las subredes privadas. Esto proporciona redundancia por zona de disponibilidad dentro de la nube privada virtual (VPC) del clúster.
- Los pods de Kubernetes permiten validar que distintas instancias de una aplicación puedan compartir, consumir y escribir contenido.

Epics

Aprovisionamiento de un clúster de Amazon EKS (opcional)

Tarea	Descripción	Habilidades requeridas
Cree un clúster de Amazon EKS.	**Note** Si ya dispone de un clúster, continúe con la siguiente epic. Cree un clúster de Amazon EKS en su cuenta de AWS. En el GitHub directorio, utilice uno de los patrones para implementar un clúster de Amazon EKS mediante Terraform o eksctl. Para obtener más información, consulte Creación de un clúster de Amazon EKS en la documentación de Amazon EKS. En el patrón de Terraform, también hay ejemplos que muestran cómo: vincular los perfiles de Fargate a su clúster de Amazon EKS, crear un sistema de archivos de Amazon EFS e implementar el	Administrador de AWS, administrador de Terraform o eksctl, administrador de Kubernetes

Tarea	Descripción	Habilidades requeridas
	controlador de CSI de Amazon EFS en su clúster de Amazon EKS.	

Tarea	Descripción	Habilidades requeridas

Exporte variables de entorno.	Use el script env.sh. Esto proporciona la información necesaria en los siguientes pasos.
	
	`source ./scripts/env.sh`
	`Inform the AWS Account ID:`
	`<13-digit-account-id>`
	`Inform your AWS Region:`
	`<aws-Region-code>`
	`Inform your Amazon EKS Cluster Name:`
	`<amazon-eks-cluster-name>`
	`Inform the Amazon EFS Creation Token:`
	`<self-genereated-uuid>`
	
	Si aún no lo ha indicado, puede obtener toda la información solicitada anteriormente con los siguientes comandos de CLI.
	
	`# ACCOUNT ID`
	`aws sts get-caller-identity --query "Account" --output text`
	
	`# REGION CODE`
	`aws configure get region`
	
	`# CLUSTER EKS NAME`
		Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas

	`aws eks list-clusters --query "clusters" --output text`
	
	`# GENERATE EFS TOKEN uuidgen`	

Crear un espacio de nombres de Kubernetes y un perfil de Fargate vinculado

Tarea	Descripción	Habilidades requeridas
Cree un espacio de nombres de Kubernetes y perfil de Fargate para las cargas de trabajo de las aplicaciones.	Cree un espacio de nombres para recibir las cargas de trabajo de las aplicacio nes que interactúan con Amazon EFS. Ejecute el script `create-k8s-ns-and-linked-fargate-pro file.sh` . Puede elegir usar un nombre para el espacio de nombres personalizado o el espacio de nombres proporcio nado por defecto `poc-efs-e ks-fargate` . Con un nombre para el espacio de nombres de la aplicación personalizado: `export $APP_NAME SPACE=<CUSTOM_NAME> ./scripts/epic01/ create-k8s-ns-and -linked-fargate-pr ofile.sh \`	Usuario de Kubernetes con permisos concedidos

Tarea	Descripción	Habilidades requeridas

	`-c "$CLUSTER_NAME" -n "$APP_NAMESPACE"`
	
	Sin un nombre para el espacio de nombres de la aplicación personalizado:
	
	`./scripts/epic01/create-k8s-ns-and-linked-fargate-profile.sh \ -c "$CLUSTER_NAME"`
	
	donde `$CLUSTER_NAME` es el nombre de su clúster de Amazon EKS. El parámetro `-n <NAMESPACE>` es opcional; si no se indica, se proporcionará un nombre para el espacio de nombres generado por defecto.	

Crear un sistema de archivos de Amazon EFS

Tarea	Descripción	Habilidades requeridas
Genere un token único.	Amazon EFS requiere la creación de un token para garantizar la operación de idempotencia (llamar a la operación con el mismo token de creación no tiene ningún efecto). Para cumplir con este requisito, debe generar un token único mediante	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	una técnica disponible. Por ejemplo, puede generar un identificador único universal (UUID) para usarlo como token de creación.	

Tarea	Descripción	Habilidades requeridas
Crear un sistema de archivos de Amazon EFS.	Cree el sistema de archivos para recibir los archivos de datos que leen y escriben las cargas de trabajo de la aplicación. Puede crear un sistema de archivos cifrado o no cifrado. (Como práctica recomendada, el código de este patrón crea un sistema cifrado para habilitar el cifrado en reposo de forma predeterminada). Puede utilizar una clave de AWS KMS simétrica y única para cifrar su sistema de archivos. Si no se especifica, se utiliza una clave administr ada de AWS. Utilice el script create-efs.sh para crear un sistema de archivos Amazon EFS cifrado o no cifrado, después de generar un token único para Amazon EFS. Con el cifrado en reposo, sin clave KMS: `./scripts/epic02/c reate-efs.sh \ -c "$CLUSTER_NAME" \ -t "$EFS_CRE ATION_TOKEN"`	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas

	donde `$CLUSTER_NAME` es el nombre de su clúster de Amazon EKS y `$EFS_CREATION_TOKEN` es un token de creación único para el sistema de archivos.
	
	Con el cifrado en reposo, con una clave KMS:
	
	`./scripts/epic02/create-efs.sh \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN" \ -k "$KMS_KEY_ALIAS"`
	
	donde `$CLUSTER_NAME` es el nombre de su clúster de Amazon EKS, `$EFS_CREATION_TOKEN` es un token de creación único para el sistema de archivos y `$KMS_KEY_ALIAS` es el alias para la clave KMS.
	
	Sin cifrado:
	
	`./scripts/epic02/create-efs.sh -d \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN"`	

Tarea	Descripción	Habilidades requeridas
	donde `$CLUSTER_NAME` es el nombre de su clúster de Amazon EKS, `$EFS_CREATION_TOKEN` es un token de creación único para el sistema de archivos y `–d` deshabilita el cifrado en reposo.	
Crear un grupo de seguridad.	Cree un grupo de seguridad para permitir al clúster de Amazon EKS acceder al sistema de archivos de Amazon EFS.	Administrador de sistemas de AWS
Actualizar la regla de entrada del grupo de seguridad.	Actualice las reglas de entrada del grupo de seguridad para permitir el tráfico entrante para las siguientes configuraciones: • Protocolo TCP: puerto 2049 • Origen: rangos de bloques de CIDR para las subredes privadas de la VPC que contiene el clúster de Kubernetes	Administrador de sistemas de AWS
Agregar un destino de montaje para cada subred privada.	Para cada subred privada del clúster de Kubernetes, cree un destino de montaje para el sistema de archivos y el grupo de seguridad.	Administrador de sistemas de AWS

Instalar los componentes de Amazon EFS en el clúster de Kubernetes

Tarea	Descripción	Habilidades requeridas
Implementar el controlador de CSI de Amazon EFS.	Implemente el controlador de CSI de Amazon EFS en el clúster. El controlador aprovisiona el almacenamiento de acuerdo con las demandas de volumen persistentes creadas por las aplicaciones. Use el script `create-k8s-efs-csi-sc.sh` para implementar el controlador de CSI de Amazon EFS y la clase de almacenamiento en el clúster: `./scripts/epic03/create-k8s-efs-csi-sc.sh` Este script usa la utilidad `kubectl`, así que asegúrese de que el contexto se haya configurado y que apunte al clúster de Amazon EKS deseado.	Usuario de Kubernetes con permisos concedidos
Implementar la clase de almacenamiento.	Implemente la clase de almacenamiento en el clúster del aprovisionador de Amazon EFS (efs.csi.aws.com).	Usuario de Kubernetes con permisos concedidos

Instalear la aplicación PoC en el clúster de Kubernetes

Tarea	Descripción	Habilidades requeridas
Implementar el volumen persistente.	Implemente el volumen persistente y vincúlelo a la clase de almacenamiento creada y al ID del sistema de archivos Amazon EFS. La aplicación utiliza el volumen persistente para leer y escribir contenido. Puede especific ar cualquier tamaño para el volumen persistente en el campo de almacenam iento. Kubernetes requiere este campo, pero dado que Amazon EFS es un sistema de archivos elástico, no aplica ningún límite de capacidad del sistema de archivos. Puede implementar el volumen persistente con o sin cifrado. (El controlador CSI de Amazon EFS habilita el cifrado de forma predeterminada, como práctica recomenda da). Use el script `deploy-po c-app.sh` para implement ar el volumen persistente, la demanda de volumen persistente y las dos cargas de trabajo. Con cifrado en tránsito:	Usuario de Kubernetes con permisos concedidos

Tarea	Descripción	Habilidades requeridas

	`./scripts/epic04/deploy-poc-app.sh \ -t "$EFS_CREATION_TOKEN"`
	
	donde `$EFS_CREATION_TOKEN` es el token de creación único para el sistema de archivos.
	
	Sin cifrado en tránsito:
	
	`./scripts/epic04/deploy-poc-app.sh -d \ -t "$EFS_CREATION_TOKEN"`
	
	donde `$EFS_CREATION_TOKEN` es el token de creación único para el sistema de archivos y `-d` desactiva el cifrado en tránsito.	

Tarea	Descripción	Habilidades requeridas
Implementar la demanda de volumen persistente solicitada por la aplicación.	Implemente la demanda de volumen persistente solicitada por la aplicación y vincúlela a la clase de almacenamiento. Utilice el mismo modo de acceso que el volumen persistente que creó anteriormente. Puede especificar cualquier tamaño para la demanda de volumen persistente en el campo de almacenamiento. Kubernetes requiere este campo, pero dado que Amazon EFS es un sistema de archivos elástico, no aplica ningún límite de capacidad del sistema de archivos.	Usuario de Kubernetes con permisos concedidos
Implementar la carga de trabajo 1.	Implemente el pod que representa la carga de trabajo 1 de la aplicación. Esta carga de trabajo escribe el contenido en el archivo `/data/out1.txt` .	Usuario de Kubernetes con permisos concedidos
Implementar la carga de trabajo 2.	Implemente el pod que representa la carga de trabajo 2 de la aplicación. Esta carga de trabajo escribe el contenido en el archivo `/data/out2.txt` .	Usuario de Kubernetes con permisos concedidos

Validar la persistencia, durabilidad y compartibilidad del sistema de archivos

Tarea	Descripción	Habilidades requeridas
Compruebe el estado de `PersistentVolume` .	Ingrese el siguiente comando para verificar el estado de `PersistentVolume` . `kubectl get pv` Para obtener un ejemplo de salida, consulte la sección Información adicional.	Usuario de Kubernetes con permisos concedidos
Compruebe el estado de `PersistentVolumeClaim` .	Ingrese el siguiente comando para verificar el estado de `PersistentVolumeClaim` . `kubectl -n poc-efs-eks-fargate get pvc` Para obtener un ejemplo de salida, consulte la sección Información adicional.	Usuario de Kubernetes con permisos concedidos
Validar que la carga de trabajo 1 pueda escribir en el sistema de archivos.	Ingrese el siguiente comando para validar que la carga de trabajo 1 esté escribiendo en `/data/out1.txt` . `kubectl exec -ti poc-app1 -n poc-efs-eks-fargate -- tail -f /data/out1.txt` Los resultados son similares a los siguientes:	Usuario de Kubernetes con permisos concedidos

Tarea	Descripción	Habilidades requeridas
	``` ... Thu Sep 3 15:25:07 UTC 2023 - PoC APP 1 Thu Sep 3 15:25:12 UTC 2023 - PoC APP 1 Thu Sep 3 15:25:17 UTC 2023 - PoC APP 1 ... ```	
Validar que la carga de trabajo 2 pueda escribir en el sistema de archivos.	Ingrese el siguiente comando para validar que la carga de trabajo 2 esté escribiendo en `/data/out2.txt` . ``` kubectl -n $APP_NAME SPACE exec -ti poc-app2 -- tail -f /data/out 2.txt ``` Los resultados son similares a los siguientes: ``` ... Thu Sep 3 15:26:48 UTC 2023 - PoC APP 2 Thu Sep 3 15:26:53 UTC 2023 - PoC APP 2 Thu Sep 3 15:26:58 UTC 2023 - PoC APP 2 ... ```	Usuario de Kubernetes con permisos concedidos

Tarea	Descripción	Habilidades requeridas

Validar que la carga de trabajo 1 pueda leer el archivo escrito por la carga de trabajo 2.	Ingrese el siguiente comando para validar que la carga de trabajo 1 pueda leer el archivo `/data/out2.txt` escrito por la carga de trabajo 2.
	`kubectl exec -ti poc-app1 -n poc-efs-eks-fargate -- tail -n 3 /data/out2.txt`
	Los resultados son similares a los siguientes:
	`... Thu Sep 3 15:26:48 UTC 2023 - PoC APP 2 Thu Sep 3 15:26:53 UTC 2023 - PoC APP 2 Thu Sep 3 15:26:58 UTC 2023 - PoC APP 2 ...`
		Usuario de Kubernetes con permisos concedidos

Tarea	Descripción	Habilidades requeridas

Validar que la carga de trabajo 2 pueda leer el archivo escrito por la carga de trabajo 1.	Ingrese el siguiente comando para validar que la carga de trabajo 2 pueda leer el archivo `/data/out1.txt` escrito por la carga de trabajo 1.
	`kubectl -n $APP_NAMESPACE exec -ti poc-app2 -- tail -n 3 /data/out1.txt`
	Los resultados son similares a los siguientes:
	`... Thu Sep 3 15:29:22 UTC 2023 - PoC APP 1 Thu Sep 3 15:29:27 UTC 2023 - PoC APP 1 Thu Sep 3 15:29:32 UTC 2023 - PoC APP 1 ...`
		Usuario de Kubernetes con permisos concedidos

Tarea	Descripción	Habilidades requeridas

Validar que los archivos se conserven después de eliminar los componentes de la aplicación.	A continuación, utilice un script para eliminar los componentes de la aplicación (volumen persistente, solicitud de volumen persistente y pods) y comprobar que los archivos `/data/out1.txt` y `/data/out2.txt` se retienen en el sistema de archivos. Ejecute el script `validate-efs-content.sh` mediante el comando siguiente.
	`./scripts/epic05/validate-efs-content.sh \`
	`-t "$EFS_CREATION_TOKEN"`
	donde `$EFS_CREATION_TOKEN` es el token de creación único para el sistema de archivos.
	Los resultados son similares a los siguientes:
	`pod/poc-app-validation created`
	`Waiting for pod get Running state...`
	`Waiting for pod get Running state...`
	`Waiting for pod get Running state...`
		Usuario de Kubernetes con permisos concedidos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas

	`Results from execution of 'find /data' on validation process pod:`
	`/data`
	`/data/out2.txt`
	`/data/out1.txt`	

Operaciones de supervisión

Tarea	Descripción	Habilidades requeridas
Supervisar los registros de aplicación.	Como parte de una operación de dos días, envía los registros de la aplicación a Amazon CloudWatch para que los supervisen.	Administrador de sistemas de AWS, usuario de Kubernetes con permisos concedidos
Supervisar contenedores de Amazon EKS y de Kubernetes con Container Insights.	Como parte de una operación de dos días, supervise los sistemas Amazon EKS y Kubernetes mediante Amazon Container Insights. CloudWatch Esta herramienta recopila, agrega y resume métricas de aplicaciones en contenedores en diferentes niveles y dimensiones. Para obtener más información, consulte la sección Recursos relacionados.	Administrador de sistemas de AWS, usuario de Kubernetes con permisos concedidos
Supervise Amazon EFS con CloudWatch.	Como parte de una operación de dos días, supervise los sistemas de archivos con Amazon CloudWatch, que	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	recopila y procesa datos sin procesar de Amazon EFS para convertirlos en métricas legibles y prácticamente en tiempo real. Para obtener más información, consulte la sección Recursos relacionados.	

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Limpiar todos los recursos creados para el patrón.	Tras completar este patrón, limpie todos los recursos para evitar incurrir en cargos de AWS. Use el script `clean-up-resources.sh` para eliminar todos los recursos una vez que haya terminado de usar la aplicación PoC. Complete una de las siguientes opciones: Con el cifrado en reposo, con una clave KMS: `./scripts/epic06/clean-up-resources.sh \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN" \ -k "$KMS_KEY_ALIAS"`	Usuario de Kubernetes con permisos concedidos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	donde `$CLUSTER_NAME` es el nombre de su clúster de Amazon EKS, `$EFS_CREATION_TOKEN` es un token de creación único para el sistema de archivos y `$KMS_KEY_ALIAS` es el alias para la clave KMS. Sin cifrado en reposo: `./scripts/epic06/clean-up-resources.sh \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN"` donde `$CLUSTER_NAME` es el nombre de su clúster de Amazon EKS y `$EFS_CREATION_TOKEN` es un token de creación único para el sistema de archivos.	

Recursos relacionados

Referencias

- AWS Fargate for Amazon EKS now supports Amazon EFS (anuncio)
- Cómo capturar los registros de las aplicaciones al usar Amazon EKS en AWS Fargate (entrada del blog)
- Uso de Container Insights (CloudWatch documentación de Amazon)

- Configuración de Container Insights en Amazon EKS y Kubernetes (documentación de Amazon) CloudWatch
- Métricas de Amazon EKS y Kubernetes Container Insights (documentación de Amazon) CloudWatch
- Supervisión de Amazon EFS con Amazon CloudWatch (documentación de Amazon EFS)

GitHub tutoriales y ejemplos

- Aprovisionamiento estático
- Cifrado en tránsito
- Acceder al sistema de archivos desde varios pods
- Consumir Amazon EFS en StatefulSets
- Montaje de subrutas
- Uso de puntos de acceso de Amazon EFS
- Amazon EKS Blueprints for Terraform

Herramientas necesarias

- Instalación de la versión 2 de la AWS CLI
- Instalación de eksctl
- Instalación de kubectl
- Instalación de jq

Información adicional

A continuación, se muestra un ejemplo de la salida del comando `kubectl get pv`.

```
NAME         CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM
            STORAGECLASS   REASON   AGE
poc-app-pv   1Mi        RWX            Retain           Bound    poc-efs-eks-fargate/
poc-app-pvc   efs-sc                  3m56s
```

A continuación, se muestra un ejemplo de la salida del comando `kubectl -n poc-efs-eks-fargate get pvc`.

```
NAME          STATUS   VOLUME       CAPACITY   ACCESS MODES   STORAGECLASS   AGE
poc-app-pvc   Bound    poc-app-pv   1Mi        RWX            efs-sc         4m34s
```

Configuración del escalado automático basado en eventos en Amazon EKS mediante Amazon EKS Pod Identity y KEDA

Dipen Desai, Abhay Diwan, Kamal Joshi y Mahendra Revanasiddappa, Amazon Web Services

Resumen

Las plataformas de orquestación, como Amazon Elastic Kubernetes Service (Amazon EKS), han simplificado la administración del ciclo de vida de las aplicaciones basadas en contenedores. Esto ayuda a las organizaciones a centrarse en crear, proteger, operar y mantener aplicaciones basadas en contenedores. A medida que las implementaciones basadas en eventos se vuelven más comunes, las organizaciones escalan con mayor frecuencia las implementaciones de Kubernetes en función de diversos orígenes de eventos. Este método, combinado con el escalado automático, puede generar importantes ahorros de costos al proporcionar recursos de cómputo bajo demanda y un escalado eficiente que se adapta a la lógica de la aplicación.

KEDA es un escalador automático basado en eventos que se basa en Kubernetes. KEDA lo ayuda a escalar cualquier contenedor de Kubernetes en función de la cantidad de eventos que deben procesarse. Es ligero y se integra con cualquier clúster de Kubernetes. También funciona con componentes estándar de Kubernetes, como el escalado automático de pods horizontales (HPA). KEDA también ofrece una TriggerAuthenticationfunción que le ayuda a delegar la autenticación. Permite describir los parámetros de autenticación que están separados del contenedor de despliegue ScaledObject y del contenedor de despliegue.

AWS proporciona funciones AWS Identity and Access Management (IAM) que admiten diversas opciones de implementación de Kubernetes, incluidas Amazon EKS, Amazon EKS Anywhere Red Hat OpenShift Service en AWS (ROSA) y clústeres de Kubernetes autogestionados en Amazon Elastic Compute Cloud (Amazon). EC2 Estas funciones utilizan estructuras de IAM, como los proveedores de identidad de OpenID Connect (OIDC) y las políticas de confianza de IAM, para funcionar en diferentes entornos sin depender directamente de los servicios de Amazon EKS o. APIs Para obtener más información, consulte Roles de IAM para cuentas de servicio en la documentación de Amazon EKS.

Amazon EKS Pod Identity simplifica el proceso para que las cuentas de servicio de Kubernetes asuman roles de IAM sin necesidad de proveedores de OIDC. Ofrece la posibilidad de administrar las credenciales de sus aplicaciones. En lugar de crear y distribuir tus AWS credenciales a los contenedores o usar el rol de la EC2 instancia de Amazon, asocias un rol de IAM a una cuenta de servicio de Kubernetes y configuras tus Pods para que usen la cuenta de servicio. Esto lo ayuda

a utilizar un rol de IAM en varios clústeres y simplifica la administración de políticas al permitir la reutilización de las políticas de permisos en todos los roles de IAM.

Al implementar KEDA con Amazon EKS Pod Identity, las empresas pueden lograr un escalado automático eficiente basado en eventos y una administración de credenciales simplificada. Las aplicaciones se escalan en función de la demanda, lo que optimiza la utilización de los recursos y reduce los costos.

Este patrón lo ayuda a integrar Amazon EKS Pod Identity con KEDA. Muestra cómo puede utilizar la cuenta de servicio `keda-operator` y delegar la autenticación con `TriggerAuthentication`. También describe cómo configurar una relación de confianza entre un rol de IAM para el operador de KEDA y un rol de IAM para la aplicación. Esta relación de confianza permite a KEDA supervisar los mensajes de las colas de eventos y ajustar la escala de los objetos de Kubernetes de destino.

Requisitos previos y limitaciones

Requisitos previos

- AWS Command Line Interface (AWS CLI) versión 2.13.17 o posterior, instalada
- La versión 3.11.5 o posterior de Python instalada
- AWS SDK para Python (Boto3) versión 1.34.135 o posterior, instalada
- La versión 3.12.3 o posterior de Helm instalada
- La versión 1.25.1 o posterior de kubectl instalada
- La versión 26.1.1 o posterior de Docker Engine instalada
- Un clúster de Amazon EKS (versión 1.24 o posterior) creado
- Se cumplen los requisitos previos para crear el agente de Amazon EKS Pod Identity

Limitaciones

- Es necesario establecer una relación de confianza entre los roles `keda-operator` y `keda-identity`. Las instrucciones se proporcionan en la sección Epics de este patrón.

Arquitectura

En este patrón, se crean los siguientes recursos: AWS

- Repositorio de Amazon Elastic Container Registry (Amazon ECR): en este patrón, este repositorio se denomina `keda-pod-identity-registry`. Este repositorio privado se usa para almacenar imágenes de Docker de la aplicación de muestra.
- Cola de Amazon Simple Queue Service (Amazon SQS): en este patrón, esta cola se denomina `event-messages-queue`. La cola actúa como un búfer de mensajes que recopila y almacena los mensajes entrantes. KEDA supervisa las métricas de la cola, como el recuento de mensajes o la longitud de la cola, y escala automáticamente la aplicación en función de estas métricas.
- Rol de IAM para la aplicación: en este patrón, este rol se denomina `keda-identity`. El rol `keda-operator` asume este rol. Este rol permite tener acceso a la cola de Amazon SQS.
- Rol de IAM para el operador KEDA: en este patrón, este rol se denomina `keda-operator`. El operador KEDA usa esta función para realizar las llamadas a la AWS API necesarias. Este rol concede permisos para asumir el rol `keda-identity`. Debido a la relación de confianza entre los roles `keda-operator` y `keda-identity`, el rol `keda-operator` tiene permisos de Amazon SQS.

A través de los recursos personalizados `TriggerAuthentication` y `ScaledObject` de Kubernetes, el operador usa el rol `keda-identity` para conectarse con una cola de Amazon SQS. En función del tamaño de la cola, KEDA escala automáticamente la implementación de la aplicación. Añade 1 pod por cada 5 mensajes no leídos de la cola. En la configuración predeterminada, si no hay mensajes sin leer en la cola de Amazon SQS, la aplicación se reduce verticalmente a 0 pods. El operador de KEDA supervisa la cola en un intervalo especificado.

La siguiente imagen muestra cómo se utiliza Amazon EKS Pod Identity para proporcionar al rol `keda-operator` un acceso seguro a la cola de Amazon SQS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El agente Amazon EKS Pod Identity se instala en el clúster de Amazon EKS.
2. El operador de KEDA se implementa en el espacio de nombres de KEDA del clúster de Amazon EKS.
3. Los roles `keda-operator` y de `keda-identity` IAM se crean en el destino. Cuenta de AWS
4. Se establece una relación de confianza entre los roles de IAM.
5. La aplicación se implementa en el espacio de nombres `security`.

6. El operador de KEDA sondea los mensajes de una cola de Amazon SQS.
7. KEDA inicia HPA, que escala automáticamente la aplicación en función del tamaño de la cola.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar AWS Kubernetes sin necesidad de instalar o mantener su propio plano de control o nodos de Kubernetes.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.

Otras herramientas

- KEDA es un escalador automático basado en eventos que se basa en Kubernetes.

Repositorio de código

El código de este patrón está disponible en el escalado GitHub automático basado en eventos mediante EKS Pod Identity y el repositorio KEDA.

Prácticas recomendadas

Recomendamos que siga las siguientes prácticas recomendadas:

- Prácticas recomendadas de Amazon EKS
- Security best practices in IAM (Prácticas recomendadas de seguridad en IAM)
- Prácticas recomendadas de Amazon SQS

Epics

Cree recursos AWS

Tarea	Descripción	Habilidades requeridas
Cree el rol de IAM del operador de KEDA.	1. Inicie sesión en la consola de IAM y Consola de administración de AWS, a continuación, ábrala. 2. Seleccione Roles en el panel de navegación. 3. Elija Crear rol. 4. Elija el tipo de rol Custom trust policy (Política de confianza personalizada). 5. En la sección Política de confianza personalizada, ingrese la política de confianza personalizada para este rol: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "pods.eks.amazonaws.com" }, "Action": [ "sts:AssumeRole",`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	<pre>"sts:TagSession"
	            ]
	        }
	    ]
	}</pre>
	6. En la página Agregar permisos, elija Siguiente . No se agrega ninguna política a este rol.
	7. En Role name (Nombre del rol), introduzca `keda-operator` .
	8. Elija Create role (Crear rol).	

Tarea	Descripción	Habilidades requeridas
Cree un rol de IAM para la aplicación de muestra.	1. En el panel de navegación de la consola de IAM, elija Roles. 2. Seleccione Crear rol. 3. Elija el tipo de rol Custom trust policy (Política de confianza personalizada). 4. En la sección Política de confianza personalizada, ingrese la política de confianza personalizada para este rol. Sustituya `<account number>` por el número de su cuenta de destino: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "pods.eks.amazonaws.com", "AWS": "arn:aws:iam::<account number>:role/keda-operator" }, "Action": [ "sts:AssumeRole",`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	<pre>"sts:TagSession"
	]
	}
	]
	}</pre>
	5. En la página Añadir permisos, añada las siguientes políticas AWS gestionadas al rol:
	• `AmazonSQSReadOnlyAccess`
	• `AWSLambdaSQSQueueExecutionRole`
	6. Elija Siguiente.
	7. En Role name (Nombre del rol), introduzca `keda-identity` .
	8. Elija Create role (Crear rol).	

Crear una cola de Amazon SQS.	1. Abra la consola de Amazon SQS. 2. Elige Crear cola. 3. En Tipo, seleccione Estándar. 4. En la página Crear cola, en Nombre, introduzca `event-messages-queue` . 5. Elige Crear cola. No cambie la configuración predeterminada de esta cola.	AWS general

Tarea	Descripción	Habilidades requeridas
Cree un repositorio de Amazon ECR.	1. Abra la consola de Amazon ECR. 2. Elija Create repository. 3. En Nombre del repositorio, introduzca `keda-pod-identity-registry` . 4. Elija Create repository. No cambie la configuración predeterminada de este repositorio.	AWS general

Configuración de un clúster de Amazon EKS

Tarea	Descripción	Habilidades requeridas
Implemente el agente Amazon EKS Pod Identity.	Para el clúster de Amazon EKS, configure el agente Amazon EKS Pod Identity. Siga las instrucciones de Configuración del agente Amazon EKS Pod Identity en la documentación de Amazon EKS.	AWS DevOps

Implemente KEDA.	1. Introduzca los siguientes comandos para implementar KEDA en el clúster de Amazon EKS de destino:
	`# Add Helm Repo for Keda`
	`helm repo add kedacore https://kedacore.github.io/charts`
	`# Update Helm repo`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	`helm repo update`
	`# Install Keda`
	`helm install keda kedacore/keda --namespace keda --create-namespace`
	
	Para obtener más información, consulte Implementación de Helm en la documentación de KEDA.
	
	2. Tras una implementación correcta, en el resultado, valide que se hayan creado tres implementaciones para el operador de KEDA. A continuación, se muestra un ejemplo de la salida:
	
	`NAME READY UP-TO-DATE AVAILABLE AGE`
	`keda-admission-webhooks 1/1 1 1 89s`
	`keda-operator 1/1 1 1 89s`
	`keda-operator-metrics-apiserver 1/1 1 1 89s`	

Tarea	Descripción	Habilidades requeridas
Asigne el rol de IAM a la cuenta de servicio de Kubernetes.	Siga las instrucciones de Asignación de un rol de IAM a una cuenta de servicio de Kubernetes en la documentación de Amazon EKS. Use los siguientes valores: • Para el rol de IAM, introduzca `keda-operator` . • Para el espacio de nombres de Kubernetes, introduzca `keda`. • Para la cuenta de servicio de Kubernetes, introduzca `keda-operator` .	AWS DevOps
Creación de un espacio de nombres de .	Introduzca el siguiente comando para crear un espacio de nombres `security` en el clúster de Amazon EKS de destino: `kubectl create ns security`	DevOps ingeniero

Implemente la aplicación de muestra.

Tarea	Descripción	Habilidades requeridas
Clone los archivos de la aplicación.	Introduzca el siguiente comando para clonar el autoescalado basado en eventos mediante EKS Pod	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Identity y el repositorio KEDA desde: GitHub `git clone https://github.com/aws-samples/event-driven-autoscaling-using-podidentity-and-keda.git`	

Cree la imagen de Docker.	1. Introduzca el siguiente comando para ir al repositorio clonado:
	`cd event-driven-autoscaling-using-podidentity-and-keda`
	2. Introduzca el siguiente comando para crear la imagen de Docker para la aplicación de muestra:
	`docker build -t keda-pod-identity-registry .`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Envíe la imagen de Docker a Amazon ECR.	1. En el terminal en el que creó la imagen de Docker, introduzca el siguiente comando para iniciar sesión en Amazon ECR. Sustituya <AWS_REGION> y <AWS_ACCOUNT_ID> con los valores de su AWS entorno:
	`aws ecr get-login-password \ --region <AWS_REGION> | docker login \ --username AWS \ --password-stdin <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com`
	2. Introduzca el siguiente comando para etiquetar la imagen. Reemplace <AWS_REGION> y <AWS_ACCOUNT_ID> con valores de su AWS entorno:
	`docker tag keda-pod-identity-registry:latest <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com/keda-pod-identity-registry:latest`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	3. Introduzca el siguiente comando para insertar la imagen en Amazon ECR. Reemplace `<AWS_REGION>` y `<AWS_ACCOUNT_ID>` con valores de su AWS entorno: `docker push <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com/keda-pod-identity-registry:latest` **Note** Para encontrar los comandos de inserción, vaya a la página del repositorio de Amazon ECR y, a continuación, seleccione Ver comandos de inserción.	

Tarea	Descripción	Habilidades requeridas
Implemente la aplicación de muestra.	1. En el repositorio clonado, abra el archivo deploy.yaml. 2. Sustituya <AWS_ACCOUNT_ID> y <AWS_REGION> por los valores correspondientes al entorno. 3. Guarde y cierre el archivo deploy.yaml. 4. Introduzca los siguientes comandos para implementar la misma aplicación en el clúster de Amazon EKS de destino: `kubectl apply -f deploy.yaml` Este comando crea una cuenta de implementación y servicio en el clúster.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Asigne el rol de IAM a la cuenta de servicio de la aplicación.	Realice una de las siguientes acciones para asociar el rol de IAM `keda-identity` a la cuenta de servicio de la aplicación de ejemplo:
	• Siga las instrucciones de Asignación de un rol de IAM a una cuenta de servicio de Kubernetes en la documentación de Amazon EKS. Use los siguientes valores:
	  • Para el rol de IAM, introduzca `keda-identity` .
	  • Para el espacio de nombres de Kubernetes, introduzca `security`.
	  • Para la cuenta de servicio de Kubernetes, introduzca `my-sqs-read-msgs` .
	• Introduzca el siguiente AWS CLI comando. Sustituya `<cluster-name>` por el nombre del clúster de Amazon EKS de destino y `<role-ARN>` por el nombre de recurso de Amazon (ARN) del rol `keda-identity` :
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`aws eks create-pod-identity-association \ --cluster-name <cluster-name> \ --role-arn <role-ARN> \ --namespace security \ --service-account my-sqs-read-msgs`	

Tarea	Descripción	Habilidades requeridas
Implemente `ScaledObject` y `TriggerAuthentication` .	1. En el repositorio clonado, abra el archivo keda.yaml. 2. `{{AWS_ACCOUNT_ID}}` Sustitúyalo por el ID de tu objetivo Cuenta de AWS. 3. `{{AWS_REGION}}` Sustitúyalo por tu objetivo Región de AWS. 4. (Opcional) En las líneas 21 a 24, actualice los parámetros de la política de escalado `ScaledObject` . Para obtener más información acerca del uso de estos parámetros, consulte lo siguiente: • pollingInterval • cooldownPeriod • idleReplicaCount • minReplicaCount 5. Guarde y cierre el archivo keda.yaml. 6. Ingrese el comando siguiente para implementar los recursos `ScaledObject` y `TriggerAuthentication` . `kubectl -n security apply -f keda.yaml`	DevOps ingeniero

Prueba de escalado automático

Tarea	Descripción	Habilidades requeridas

Envíe mensajes a la cola de Amazon SQS.	1. Introduzca el siguiente comando para ir al repositorio clonado:
	`cd event-driven-autoscaling-using-podidentity-and-keda`
	2. Introduzca el siguiente comando para enviar mensajes de prueba a la cola de Amazon SQS:
	`python sqs_send_msg.py`
	El script sqs_send_msg.py actúa como una aplicación que genera mensajes para probar el escalado automático.
	Note
	Si está ejecutando Python 3, use `python3 sqs_send_msg.py .`
		DevOps ingeniero

Supervise los pods de aplicaciones.	1. En un terminal diferente, introduzca el siguiente comando para supervisar los pods:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	`kubectl -n security get po`
	2. Por cada 5 mensajes no leídos de la cola de Amazon SQS, KEDA añade un pod. En el resultado del comando anterior, confirme que se están añadiendo nuevos pods. A continuación, se muestra un ejemplo de la salida:
	`kubectl -n security get po`
	`NAME READY STATUS RESTARTS AGE`
	`q-read-797f4c7589-2bj76 1/1 Running 0 2s`
	`q-read-797f4c7589-4zxph 1/1 Running 0 49s`
	`q-read-797f4c7589-cg9dt 1/1 Running 0 18s`
	`q-read-797f4c7589-slc69 1/1 Running 0 33s`
	3. Cuando finalice las pruebas, en el terminal original, introduzca CTRL	

Tarea	Descripción	Habilidades requeridas
	+ C (Windows) o CMD + C (macOS). Esta acción detiene el script python sqs_send_msg.py.	

Resolución de problemas

Problema	Solución

El operador de KEDA no puede escalar la aplicación.	Introduzca el siguiente comando para comprobar los registros del rol de IAM `keda-operator` :
	`kubectl logs -n keda -l app=keda-operator -c keda-operator`
	
	Si hay un código de respuesta`HTTP 403`, la aplicación y el escalador de KEDA no tienen permisos suficientes para acceder a la cola de Amazon SQS. Realice los siguientes pasos:
	1. Consulte las instrucciones y políticas de IAM del rol `keda-identity` para confirmar que se concede el acceso de lectura a la cola.
	2. Valide la relación de confianza entre los roles de IAM. A continuación, se muestra un ejemplo:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow",`

Problema	Solución
	<pre> "Principal": { "Service": "pods.eks .amazonaws.com" }, "Action": ["sts:AssumeRole", "sts:TagSession"] }] }</pre> Si se produce un error `Assume-Role` , el rol de IAM de un nodo de Amazon EKS no puede asumir el rol de IAM que está definido para `TriggerAuthentication` . Realice los siguientes pasos: 1. Introduzca el siguiente comando para eliminar el pod `keda-operator` y crear uno nuevo: <pre>kubectl delete pod keda-operator- <alphenumeric-value> --namespace keda</pre> 2. Introduzca el siguiente comando para comprobar la identidad que asume el pod: <pre>kubectl describe pod <keda-operator- pod-name> --namespace keda</pre> 3. Cuando el pod se reinicie correctamente, confirme que se hayan añadido las dos variables siguientes a la descripción del pod: • `AWS_CONTAINER_CREDENTIALS_F ULL_URI`

Problema	Solución
	• `AWS_CONTAINER_AUTHORIZATION_TOKEN_FILE`

Recursos relacionados

- Configuración del agente Amazon EKS Pod Identity (documentación de Amazon EKS)
- Implementación de KEDA (documentación de KEDA)
- ScaledObject especificación (documentación de KEDA)
- Autenticación con TriggerAuthentication (documentación de KEDA)

Simplificación de las implementaciones de PostgreSQL en Amazon EKS mediante PGO

Shalaka Dengale, Amazon Web Services

Resumen

Este patrón integra el operador de Postgres de Crunchy Data (PGO) con Amazon Elastic Kubernetes Service (Amazon EKS) para agilizar las implementaciones de PostgreSQL en entornos nativos en la nube. PGO proporciona automatización y escalabilidad para administrar bases de datos de PostgreSQL en Kubernetes. Al combinar PGO con Amazon EKS, se forma una plataforma sólida para implementar, administrar y escalar bases de datos de PostgreSQL de manera eficiente.

Esta integración proporciona las ventajas clave siguientes:

- Implementación automatizada: simplifica la implementación y la administración de clústeres de PostgreSQL.
- Definiciones de recursos personalizadas (CRDs): utiliza primitivas de Kubernetes para la administración de PostgreSQL.
- Alta disponibilidad: admite la conmutación por error automática y la replicación sincrónica.
- Copias de seguridad y restauraciones automatizadas: simplifica los procesos para hacer copias de seguridad y restauraciones.
- Escalado horizontal: permite el escalado dinámico de los clústeres de PostgreSQL.
- Actualizaciones de versión: facilita las actualizaciones sucesivas con un tiempo de inactividad mínimo.
- Seguridad: aplica el cifrado, los controles de acceso y los mecanismos de autenticación.

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2, instalada y configurada en Linux, macOS o Windows.
- AWS CLI Config, para conectar AWS los recursos desde la línea de comandos.
- eksctl instalado y configurado en Linux, macOS o Windows.

- `kubectl`, instalado y configurado para acceder a los recursos de su clúster de Amazon EKS. Para más información, consulte Configuración de kubectl y eksctl en la documentación de Amazon EKS.
- Su terminal de equipo está configurado para acceder al clúster de Amazon EKS. Para obtener más información, consulte Configuración del equipo para que se comunique con el clúster en la documentación de Amazon EKS.

Versiones de producto

- Kubernetes, versiones 1.21 a 1.24 o posteriores (consulte la documentación de PGO).
- PostgreSQL, versión 10 y posterior. Este patrón utiliza PostgreSQL, versión 16.

Limitaciones

- Algunos Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

Pila de tecnología de destino

- Amazon EKS
- Amazon Virtual Private Cloud (Amazon VPC)
- Amazon Elastic Compute Cloud (Amazon EC2)

Arquitectura de destino

Este patrón crea una arquitectura que contiene un clúster de Amazon EKS con tres nodos. Cada nodo se ejecuta en un conjunto de instancias de EC2 en el backend. Esta configuración de PostgreSQL sigue una arquitectura de réplica principal, que resulta especialmente eficaz en casos de uso con lectura intensiva. La arquitectura incluye los siguientes componentes:

- El contenedor de base de datos principal (pg-primary) aloja la instancia principal de PostgreSQL a la que se dirigen todas las operaciones de escritura.
- Los contenedores de réplicas secundarios (pg-replica) alojan las instancias de PostgreSQL que replican los datos de la base de datos principal y gestionan las operaciones de lectura.
- PgBounceres un agrupador de conexiones ligero para bases de datos PostgreSQL que se incluye en PGO. Se encuentra entre el cliente y el servidor PostgreSQL y actúa como intermediario para las conexiones de las bases de datos.
- PGO automatiza la implementación y la administración de los clústeres de PostgreSQL en este entorno de Kubernetes.
- Patroni es una herramienta de código abierto que administra y automatiza las configuraciones de alta disponibilidad para PostgreSQL. Se incluye con PGO. Cuando utiliza Patroni con PGO en Kubernetes, desempeña un papel crucial a la hora de garantizar la resiliencia y la tolerancia a errores de un clúster de PostgreSQL. Para más información, consulte la documentación de Patroni.

En el flujo de trabajo se incluyen estos pasos:

- Implemente el operador de PGO. El operador de PGO se implementa en el clúster de Kubernetes que se ejecuta en Amazon EKS. Esto se puede hacer mediante manifiestos de Kubernetes o gráficos de Helm. Este patrón utiliza los manifiestos de Kubernetes.
- Defina las instancias de PostgreSQL. Cuando el operador está en ejecución, se crean recursos personalizados (CRs) para especificar el estado deseado de las instancias de PostgreSQL. Esto incluye configuraciones como el almacenamiento, la replicación y la alta disponibilidad.
- Administración de operadores. Se interactúa con el operador a través de objetos de la API de Kubernetes, por ejemplo, CRs para crear, actualizar o eliminar instancias de PostgreSQL.
- Supervisión y mantenimiento. Puede supervisar el estado y el rendimiento de las instancias de PostgreSQL que se ejecutan en Amazon EKS. Los operadores suelen proporcionar métricas y registros con fines de supervisión. Puede hacer tareas de mantenimiento de rutina, como actualizaciones y aplicación de revisiones, según sea necesario. Para más información, consulte Supervisión del rendimiento de un clúster y visualización de registros en la documentación de Amazon EKS.
- Escalado y copia de seguridad: puede utilizar las características proporcionadas por el operador para escalar las instancias de PostgreSQL y administrar las copias de seguridad.

Este patrón no cubre las operaciones de supervisión, mantenimiento y copia de seguridad.

Automatización y escala

- Puede utilizarlos para automatizar la creación de CloudFormation la infraestructura. Para más información, consulte Creación de recursos de Amazon EKS con CloudFormation en la documentación de Amazon EKS.
- Puede usar GitVersion los números de compilación de Jenkins para automatizar la implementación de instancias de bases de datos.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar AWS Kubernetes sin necesidad de instalar o mantener su propio plano de control o nodos de Kubernetes.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar mediante los comandos de su consola de línea de comandos. Servicios de AWS

Otras herramientas

- eksctl es una herramienta sencilla de línea de comandos para crear clústeres de Amazon EKS.
- kubectl: es una utilidad de línea de comandos para la ejecución de comandos en clústeres de Kubernetes.
- PGO automatiza y escala la administración de las bases de datos de PostgreSQL en Kubernetes.

Prácticas recomendadas

Siga estas prácticas recomendadas para garantizar una implementación eficiente y sin problemas:

- Proteja el clúster de EKS. Implemente las mejores prácticas de seguridad para su clúster de EKS, como el uso de funciones AWS Identity and Access Management (IAM) para las cuentas de servicio (IRSA), las políticas de red y los grupos de seguridad de VPC. Limite el acceso al servidor de API del clúster de EKS y cifre las comunicaciones entre los nodos y el servidor de API mediante TLS.
- Asegúrese de la compatibilidad de versiones entre PGO y Kubernetes que se ejecutan en Amazon EKS. Algunas características de PGO pueden requerir versiones específicas de

Kubernetes o introducir limitaciones de compatibilidad. Para más información, consulte Components and Compatibility en la documentación de PGO.

- Planifique la asignación de recursos para la implementación de PGO, lo que incluye la CPU, la memoria y el almacenamiento. Tenga en cuenta los requisitos de recursos de las instancias de PGO y PostgreSQL que administra. Supervise el uso de los recursos y escálelos según sea necesario.
- Diseñe para una alta disponibilidad. Diseñe la implementación de PGO para una alta disponibilidad a fin de minimizar el tiempo de inactividad y garantizar la fiabilidad. Implemente varias réplicas de PGO en varias zonas de disponibilidad para la tolerancia a errores.
- Implemente procedimientos de copia de seguridad y restauración para las bases de datos de PostgreSQL que administra PGO. Utilice las características que ofrece PGO o las soluciones de copia de seguridad de terceros que sean compatibles con Kubernetes y Amazon EKS.
- Configure la supervisión y el registro de la implementación de PGO para hacer un seguimiento del rendimiento, del estado y de los eventos. Utilice herramientas como Prometheus para supervisar las métricas y Grafana para la visualización. Configure el registro para capturar los registros de PGO para la solución de problemas y la auditoría.
- Configure las redes de manera correcta para permitir las comunicaciones entre instancias de PGO, PostgreSQL y otros servicios del clúster de Kubernetes. Utilice las características de red de Amazon VPC y los complementos de red de Kubernetes, como Calico o CNI de Amazon VPC, para aplicar las políticas de red y aislar el tráfico.
- Elija las opciones de almacenamiento adecuadas para las bases de datos de PostgreSQL. Tenga en cuenta factores como el rendimiento, la durabilidad y la escalabilidad. Utilice los volúmenes de Amazon Elastic Block Store (Amazon EBS) AWS o los servicios de almacenamiento gestionado para el almacenamiento persistente. Para más información, consulte el tema sobre almacenamiento de volúmenes de Kubernetes con Amazon EBS en la documentación de Amazon EKS.
- Utilice herramientas de infraestructura como código (IaC) CloudFormation para automatizar la implementación y la configuración de PGO en Amazon EKS. Defina los componentes de la infraestructura, tales como el clúster de EKS, las redes y los recursos de PGO, como código para garantizar la coherencia, la repetibilidad y el control de versiones.

Epics

Creación de un rol de IAM

Tarea	Descripción	Habilidades requeridas
Crear un rol de IAM.	1. Cree un rol de IAM con el comando siguiente en la AWS CLI: `aws iam create-role \ --role-name {YourRoleName} \ --assume-role-policy-document '{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principal": { "Service": "eks.amazonaws.com" }, "Action": "sts:AssumeRole" }] }' && \ aws iam attach-role-policy \ --role-name {YourRoleName}\ --policy-arn arn:aws:iam::aws:policy/AmazonEKSClusterPolicy && \`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	`aws iam attach-role-policy \ --role-name {YourRoleName}\ --policy-arn arn:aws:iam::aws:policy/AmazonEKSServicePolicy && \ aws iam attach-role-policy \ --role-name {YourRoleName}\ --policy-arn arn:aws:iam::aws:policy/CloudWatchFullAccess`
	2. Revise el rol en la Consola de administración de AWS:
	a. Abra la consola de IAM.
	b. Elija Roles y busque el nombre del rol que creó.
	c. Valide que se adjunten las políticas siguientes:
	`AmazonEKSClusterPolicy`
	`AmazonEKSServicePolicy`
	`CloudWatchFullAccess`	

Crear un clúster de Amazon EKS

Tarea	Descripción	Habilidades requeridas
Cree un clúster de Amazon EKS.	Si ya implementó un clúster, omita este paso. De lo contrario, implemente un clúster de Amazon EKS en su clúster actual Cuenta de AWS mediante `eksctl` Terraform o CloudFormation. Este patrón utiliza `eksctl` para la implementación de clústeres. **Note** Este patrón utiliza Amazon EC2 como grupo de nodos para Amazon EKS. Si quiere usarlo AWS Fargate, consulte la `managedNodeGroups` configuración en la documentación de eksctl. 1. Utilice el archivo siguiente de entrada `eksctl` para generar el clúster. `sample-cluster.yaml` : `apiVersion: eksctl.io/v1alpha5`	Administrador de AWS, administrador de Terraform o eksctl, administrador de Kubernetes

Tarea	Descripción	Habilidades requeridas

	<pre>kind: ClusterConfig
	metadata:
	  name: postgresql
	  region: us-east-1
	  version: "1.29"
	accessConfig:
	  authenticationMode
	: API_AND_C
	ONFIG_MAP
	availabilityZones:
	- us-east-1a
	- us-east-1b
	- us-east-1c
	nodeGroups:
	  - name: ng-1
	  instanceType:
	 m5.16xlarge
	  desiredCapacity:
	 2
	  - name: ng-2
	  instanceType:
	 m5.16xlarge
	  desiredCapacity:
	 2
	  - name: ng-3
	  instanceType:
	 m5.16xlarge
	  desiredCapacity:
	 2
	vpc:
	  cidr: 192.168.0
	.0/16
	  clusterEndpoints:
	  publicAccess:
	 true
	  nat:
	  gateway: HighlyAva
	ilable
	iamIdentity
	Mappings:
	  - arn: arn:aws:i
	am::<account-id>:r</pre>	

Tarea	Descripción	Habilidades requeridas

	<pre>ole/<role-name> # update the IAM role ARN created in step 1
	    username: <user-name> # Enter the user name per your choice
	    noDuplicateARNs: false</pre>
	2. Ejecute el comando siguiente para crear el clúster (proporcione la ruta del archivo `sample-cluster.yaml`):
	<pre>eksctl create cluster -f sample-cluster.yaml</pre>	

Valide el estado del clúster.	Ejecute el comando siguiente para ver el estado actual de los nodos del clúster: <pre>kubectl get nodes</pre> Si encuentra errores, consulte la sección de resolución de problemas de la documentación de Amazon EKS.	Administrador de AWS, administrador de Terraform o eksctl, administrador de Kubernetes

Creación de un proveedor de identidad de OIDC

Tarea	Descripción	Habilidades requeridas
Habilite el proveedor de OIDC de IAM.	Como requisito previo para el controlador de la interfaz de almacenamiento de contenedores (CSI) de Amazon EBS, debe tener un proveedor de IAM OpenID Connect (OIDC) existente para el clúster. Habilite el proveedor de IAM OIDC mediante el comando siguiente: `eksctl utils associate -iam-oidc-provider --region={region} --cluster={YourClusterNameHere} --approve` Para más información acerca de este paso, consulte la documentación de Amazon EKS.	Administrador de AWS
Cree un rol de IAM para el controlador de CSI de Amazon EBS	Utilice el comando siguiente `eksctl` para crear el rol de IAM para el controlador de la CSI: `eksctl create iamserviceaccount \ --region {RegionName} \ --name ebs-csi-controller-sa \`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	`--namespace kube-system \`
	`--cluster {YourClusterNameHere} \`
	`--attach-policy-arn arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy \`
	`--approve \`
	`--role-only \`
	`--role-name AmazonEKS_EBS_CSI_DriverRole`
	
	Si utiliza controladores de Amazon EBS cifrados, debe configurar la política con mayor detalle. Para obtener instrucciones, consulte la documentación de controladores de la SCI de Amazon EBS.	

Tarea	Descripción	Habilidades requeridas
Agregue el controlador de CSI de Amazon EBS.	Utilice el comando siguiente `eksctl` para agregar el controlador de CSI de Amazon EBS: `eksctl create addon \ --name aws-ebs-csi-driver \ --cluster <YourClusterName> service-account-role-arn arn:aws:iam::$(aws sts get-caller-identity \ --query Account \ --output text):role/AmazonEKS_EBS_CSI_DriverRole \ --force`	Administrador de AWS

Instalación de PGO

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de PGO.	Clona el GitHub repositorio para PGO: `git clone https://github.com/CrunchyData/postgres-operator-examples.git`	AWS DevOps
Proporcione los detalles del rol para crear la cuenta de servicio.	Para conceder al clúster de Amazon EKS acceso a los AWS recursos necesarios, especifique el nombre del recurso de Amazon (ARN) del	Administrador de AWS, administrador de Kubernetes

Tarea	Descripción	Habilidades requeridas

	rol OIDC que creó anteriormente en el `service_account.yaml` archivo que se encuentra en. GitHub
	`cd postgres-operator-examples`
	`--- metadata: annotations: eks.amazonaws.com/role-arn: arn:aws:iam::<accountId>:role/<role_name> # Update the OIDC role ARN created earlier`	

Tarea	Descripción	Habilidades requeridas

Cree el espacio de nombres y los requisitos previos de PGO.	1. Ejecute el siguiente comando para crear el espacio de nombres :
	`kubectl apply -k kustomize/install/namespace`
	Esto establece un espacio de nombres dedicado para PGO. Si es necesario, puede modificar el archivo `namespace.yml` y asignar un nombre distinto al espacio de nombres.
	2. Ejecute el comando siguiente para aplicar la configuración predeterminada al clúster:
	`kubectl apply --server-side -k kustomize/install/default`
	`kustomize/install/default` proporciona la configuración predeterminada para el control de acceso basado en roles (RBAC) de Kubernetes, la definición de recursos personalizados (CRD) y los archivos de Kubernetes Manager.
		Administrador de Kubernetes

Tarea	Descripción	Habilidades requeridas
Verifique la creación de los pods.	Compruebe que se hayan creado el espacio de nombres y la configuración predeterminada: `kubectl get pods -n postgres-operator`	Administrador de AWS, administrador de Kubernetes
Verificar PVCs.	Usa el siguiente comando para verificar las notificaciones de volumen persistentes (PVCs): `kubectl describe pvc -n postgres-operator`	Administrador de AWS, administrador de Kubernetes

Creación e implementación de un operador

Tarea	Descripción	Habilidades requeridas

Cree un operador.	Revise el contenido del archivo ubicado en `/kustomize/postgres/postgres.yaml` para que coincida con lo siguiente:
	`spec:`
	`  instances:`
	`  - name: pg-1`
	`  replicas: 3`
	`  patroni:`
	`  dynamicConfiguration:`
	`  postgresql:`
	`  pg_hba:`
		Administrador de AWS, DBA, administrador de Kubernetes

Tarea	Descripción	Habilidades requeridas

	<pre>- "host all all 0.0.0.0/0 trust"
	# this line enabled logical replication with programmatic access
	- "host all postgres 127.0.0.1/32 md5"
	synchronous_mode: true
	users:
	- name: replicator
	databases:
	- testdb
	options: "REPLICATION"</pre>
	Estas actualizaciones hacen lo siguiente:
	• Ajuste los valores de configuración de PostgreSQL para facilitar el acceso a la instancia de PostgreSQL.
	• Incluya configuraciones para el usuario de replicación, el usuario de la base de datos y el superusuario para permitir la replicación en streaming, el acceso a la base de datos y la administración de clústeres.	

Tarea	Descripción	Habilidades requeridas
Implemente el operador.	Implemente el operador de PGO para permitir la administración y el uso simplificados de las bases de datos de PostgreSQL en entornos de Kubernetes: `kubectl apply -k kustomize/postgres`	Administrador de AWS, DBA, administrador de Kubernetes

Tarea	Descripción	Habilidades requeridas

Comprobar la implementación.	1. Valide que el operador se haya implementado:
	`kubectl get pods -n postgres-operator --selector=postgres-operator.crunchydata.com/instance-set \ -L postgres-operator.crunchydata.com/role`
	2. Verifique que se haya creado el recurso de servicio asociado al pod del operador:
	`kubectl get svc -n postgres-operator`
	En el resultado del comando, anote la réplica principal (`primary_pod_name`) y lea la réplica (`read_pod_name`). Los utilizará en los pasos próximos.
		Administrador de AWS, DBA, administrador de Kubernetes

Verificación de replicación de flujos

Tarea	Descripción	Habilidades requeridas
Escriba los datos en la réplica principal.	Utilice los comandos siguientes para conectarse a la réplica principal de PostgreSQL y	Administrador de AWS, administrador de Kubernetes

Tarea	Descripción	Habilidades requeridas

	escribir datos en la base de datos:
	
	`kubectl exec -it <primary_pod_name> bash -n postgres-operator`
	
	`psql`
	
	`CREATE TABLE customers (firstname text, customer_id serial, date_created timestamp );`
	`\dt`	

Confirme que la réplica de lectura tiene los mismos datos.	Conéctese a la réplica de lectura de PostgreSQL y compruebe si la replicación de streaming funciona correctamente:
	
	`kubectl exec -it {read_pod_name} bash -n postgres-operator`
	
	`psql`
	
	`\dt`
	
	La réplica de lectura debe tener la tabla que creó en la réplica principal en el paso anterior.
		Administrador de AWS, administrador de Kubernetes

Resolución de problemas

Problema	Solución

El pod no se inicia.	• Utilice el comando siguiente para inspeccionar el estado del pod:
	`kubectl get pods -n your-namespace`
	• Inspeccione los registros para detectar errores:
	`kubectl logs your-pod-name -n your-namespace`
	• Verifique los eventos de los pods para ver si hay eventos anormales relacionados con los pods:
	`kubectl describe pod your-pod-name -n your-namespace`

Las réplicas están muy atrasadas con respecto a la base de datos principal.	• Compruebe el retraso de la replicación:
	`SELECT * FROM pg_stat_replication;`
	• Asegúrese de que las réplicas tengan recursos suficientes de CPU y memoria. Compruebe los límites de los recursos:
	`kubectl describe pod your-replica-pod -n your-namespace`
	• Verifique que el backend de almacenamiento funcione de manera óptima. Un disco lento I/O puede provocar un retraso en la replicación.

Problema	Solución
No tiene visibilidad del rendimiento y el estado del clúster de PostgreSQL.	• Activa Amazon CloudWatch Logs y asegúrate de que los registros se envíen a Amazon CloudWatch para su análisis. Para obtener más información, consulte la documentación de Amazon EKS. • Compruebe **`pg_stat_activity`** : `SELECT * FROM pg_stat_activity;`

La replicación no funciona.	• Verifique la configuración principal y consulte la configuración de la replicación en `postgresql.conf` :
	`wal_level = replica`
	`max_wal_senders = 10`
	`wal_keep_size = 64  # or wal_keep_segments in older versions`
	• Verifique que `pg_hba.conf` incluye los permisos de replicación:
	`host replication replica_user all md5`
	• Verifique la configuración de la replicación. Asegúrese de que los valores de `recovery.conf` o una equivalente (`standby.signal` y `primary_conninfo`) estén configurados correctamente en las réplicas.

Recursos relacionados

- Amazon Elastic Kubernetes Service (documento técnico Overview of Deployment Options on AWS)
- CloudFormation (documento técnico Overview of Deployment Options on AWS)
- Introducción a Amazon EKS: eksctl (Guía de usuario de Amazon EKS)
- Configuración de kubectl y eksctl (Guía de usuario de Amazon EKS)
- Creación de un rol para una federación de OpenID Connect (Guía de usuario de IAM)
- Configuración de los ajustes de la AWS CLI (Guía AWS CLI del usuario)
- Documentación de Crunchy Postgres for Kubernetes
- Crunch & Learn: Crunchy Postgres for Kubernetes 5,0 (video)

Simplificación de la autenticación de aplicaciones con TLS mutuo en Amazon ECS mediante el equilibrador de carga de aplicación

Olawale Olaleye y Shamanth Devagari, Amazon Web Services

Resumen

Este patrón le permite simplificar la autenticación de sus aplicaciones y a reducir las cargas de seguridad con el TLS mutuo en Amazon Elastic Container Service (Amazon ECS) mediante el equilibrador de carga de aplicación (ALB). Con ALB, puede autenticar los certificados de cliente X.509 desde. AWS Private Certificate Authority Esta eficiente combinación ayuda a lograr una comunicación segura entre sus servicios, lo que reduce la necesidad de mecanismos de autenticación complejos en las aplicaciones. Además, el patrón utiliza Amazon Elastic Container Registry (Amazon ECR) para almacenar imágenes de contenedor.

En el ejemplo de este patrón se utilizan imágenes de Docker de una galería pública para crear las cargas de trabajo de muestra desde un inicio. Posteriormente, se crean nuevas imágenes de Docker para almacenarlas en Amazon ECR. Para la fuente, considere un sistema basado en Git como GitHub GitLab, o Bitbucket, o utilice Amazon Simple Storage Service Amazon S3 (Amazon S3). Para crear las imágenes de Docker, considere utilizarlas AWS CodeBuild para las imágenes siguientes.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS con acceso a las pilas de despliegue AWS CloudFormation . Asegúrese de tener permisos de usuario o rol AWS Identity and Access Management (de IAM) para realizar la implementación. CloudFormation
- AWS Command Line Interface (AWS CLI) instalado. Configure sus AWS credenciales en su máquina local o en su entorno utilizando AWS CLI o configurando las variables de entorno del `~/.aws/credentials` archivo.
- OpenSSL instalado.
- Docker instalado.
- Familiaridad con lo Servicios de AWS descrito en Herramientas.
- Conocimientos de Docker y NGINX.

Limitaciones

- La TLS mutua para el equilibrador de carga de aplicación solo admite certificados de cliente X.509v3. No se admiten los certificados de cliente X.509v1.
- La CloudFormation plantilla que se proporciona en el repositorio de código de este patrón no incluye el aprovisionamiento de un CodeBuild proyecto como parte de la pila.
- Algunas Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- La versión 27.3.1 o posterior de Docker
- AWS CLI versión 2.14.5 o posterior

Arquitectura

En el diagrama siguiente se muestran los componentes de la arquitectura de este patrón.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Cree un repositorio de Git y confirme el código de la aplicación en el repositorio.
2. Cree una autoridad de certificación (CA) privada en. AWS Private CA
3. Cree un CodeBuild proyecto. CodeBuildproject Se activa mediante cambios de confirmación y crea la imagen de Docker y publica la imagen creada en Amazon ECR.
4. Copie la cadena del certificado y el cuerpo del certificado de la autoridad de certificación y cargue la agrupación de certificados en Amazon S3.
5. Cree un almacén de confianza con la agrupación de CA que cargó en Amazon S3. Asocie el almacén de confianza a los oyentes de la TLS mutua del equilibrador de carga de aplicación (ALB).
6. Utilice la CA privada para emitir certificados de cliente para las cargas de trabajo del contenedor. Cree también un certificado TLS privado utilizando. AWS Private CA
7. Importe el certificado TLS privado a AWS Certificate Manager (ACM) y utilícelo con el ALB.

8. La carga de trabajo del contenedor en `ServiceTwo` utiliza el certificado de cliente emitido para autenticarse con el equilibrador de carga de aplicación cuando se comunica con la carga de trabajo del contenedor en `ServiceOne`.
9. La carga de trabajo del contenedor en `ServiceOne` utiliza el certificado de cliente emitido para autenticarse con el equilibrador de carga de aplicación cuando se comunica con la carga de trabajo del contenedor en `ServiceTwo`.

Automatización y escala

Este patrón se puede automatizar por completo mediante el uso CloudFormation de operaciones de API desde un SDK para aprovisionar los recursos. AWS Cloud Development Kit (AWS CDK) AWS

Se puede utilizar AWS CodePipeline para implementar una canalización de integración e implementación continuas (CI/CD) CodeBuild para automatizar el proceso de creación de imágenes de contenedores y la implementación de nuevas versiones en los servicios de clúster de Amazon ECS.

Tools (Herramientas)

Servicios de AWS

- AWS Certificate Manager (ACM) le ayuda a crear, almacenar y renovar claves y certificados SSL/TLS X.509 públicos y privados que protegen sus AWS sitios web y aplicaciones.
- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todo el territorio y. Cuentas de AWS Regiones de AWS
- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores altamente escalable y rápido que permite ejecutar, detener y administrar contenedores en un clúster. Puede ejecutar sus tareas y servicios en una infraestructura sin servidores gestionada por AWS Fargate. Como alternativa, para tener más control sobre su infraestructura, puede ejecutar sus tareas y servicios en un clúster de instancias de Amazon Elastic Compute Cloud (Amazon EC2) que administre.

- Amazon ECS Exec le permite interactuar de manera directa con los contenedores sin necesidad de interactuar primero con el sistema operativo del contenedor host, abrir puertos entrantes o administrar claves SSH. Puedes usar ECS Exec para ejecutar comandos u obtener un shell para un contenedor que se ejecute en una EC2 instancia de Amazon o en AWS Fargateél.
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos. Por ejemplo, puede distribuir el tráfico entre EC2 instancias, contenedores y direcciones IP de Amazon, en una o más zonas de disponibilidad. ELB supervisa el estado de los destinos registrados y enruta el tráfico solo a los destinos con un estado correcto. ELB escala el equilibrador de carga a medida que el tráfico entrante va cambiando con el tiempo. Puede escalarse automáticamente para adaptarse a la mayoría de las cargas de trabajo.
- AWS Fargatele ayuda a ejecutar contenedores sin necesidad de gestionar servidores o EC2 instancias de Amazon. Fargate es compatible tanto con Amazon ECS como con Amazon Elastic Kubernetes Service (Amazon EKS). Puede ejecutar las tareas y servicios de Amazon ECS con el tipo de lanzamiento de Fargate o con un proveedor de capacidad de Fargate. Todo lo que tiene que hacer es empaquetar su aplicación en contenedores, especificar los requisitos de CPU y de memoria, definir las políticas de IAM y de redes, y lanzar la aplicación. Cada tarea de Fargate tiene su propio límite de aislamiento y no comparte el kernel subyacente, los recursos de CPU, los recursos de memoria ni la interfaz de red elástica con otra tarea.
- AWS Private Certificate Authoritypermite la creación de jerarquías de autoridades de certificación (CA) privadas, incluidas las principales y las subordinadas CAs, sin los costes de inversión y mantenimiento que implica operar una CA local.

Otras herramientas

- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización a nivel del sistema operativo para entregar software en contenedores.
- GitHubGitLab, y Bitbucket son algunos de los sistemas de control de código fuente basados en Git más utilizados para realizar un seguimiento de los cambios en el código fuente.
- NGINX Open Source es un equilibrador de carga, caché de contenido y servidor web de código abierto. Este patrón lo utiliza como servidor web.
- OpenSSL es una biblioteca de código abierto que proporciona servicios que utilizan las implementaciones OpenSSL de TLS y CMS.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub MTLS-with-Application-Load-Balancer-in-Amazon-ECS.

Prácticas recomendadas

- Utilice Amazon ECS Exec para ejecutar comandos en un contenedor u obtener un intérprete de comandos en un contenedor que se ejecute en Fargate. Puede también utilizar ECS Exec como ayuda para recopilar información de diagnóstico para la depuración.
- Utilice grupos de seguridad y listas de control de acceso a la red () para controlar el tráfico entrante y saliente entre los servicios. ACLs Las tareas de Fargate reciben una dirección IP de la subred configurada en la nube privada virtual (VPC).

Epics

Creación de repositorio

Tarea	Descripción	Habilidades requeridas
Descargue el código fuente.	Para descargar el código fuente de este patrón, bifurque o clone el repositorio GitHub MTLS-with-Application-Load-Balancer-in-Amazon-ECS.	DevOps ingeniero
Cree un repositorio de Git.	Para crear un repositorio de Git que contenga el Dockerfile y los archivos `buildspec.yaml` , haga lo siguiente: 1. Cree una carpeta en su entorno virtual. Póngale el nombre del proyecto. 2. Abra un terminal en la máquina local y vaya a la carpeta. 3. Para clonar el repositorio MTLS-with-Application-	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Load-Balancer-in-Amazon-ECS en el directorio de su proyecto, introduzca el comando siguiente: `git clone https://github.com/aws-samples/mTLS-with-Application-Load-Balancer-in-Amazon-ECS.git`	

Creación de una CA y generación de certificados

Tarea	Descripción	Habilidades requeridas
Cree una CA privada en AWS Private CA.	Para crear una autoridad de certificación (CA) privada, ejecute los siguientes comandos en su terminal. Sustituya los valores de las variables de ejemplo por sus propios valores. `export AWS_DEFAULT_REGION="us-west-2"` `export SERVICES_DOMAIN="www.example.com"` `export ROOT_CA_ARN=`aws acm-pca create-certificate-authority \` `--certificate-authority-type ROOT \`	DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`--certificate-authority-configuration \`
	`"KeyAlgorithm=RSA_2048,`
	`SigningAlgorithm=SHA256WITHRSA,`
	`Subject={`
	`Country=US,`
	`State=WA,`
	`Locality=Seattle,`
	`Organization=Build on AWS,`
	`OrganizationalUnit=mTLS Amazon ECS and ALB Example,`
	`CommonName=${SERVICES_DOMAIN}}" \`
	`--query CertificateAuthorityArn --output text`
	
	Para obtener más información, consulte Crear una CA privada AWS Private CA en la AWS documentación.	

Tarea	Descripción	Habilidades requeridas

Cree e instale su certificado CA privado.	Para crear e instalar un certificado para su CA raíz privada, ejecute los comandos siguientes en su terminal:
	
	1. Genere una solicitud de firma de certificado (CSR).
	
	```ROOT_CA_CSR=`aws acm-pca get-certificate-authority-csr \ --certificate-authority-arn ${ROOT_CA_ARN} \ --query Csr --output text````
	
	2. Emita el certificado raíz.
	
	``AWS_CLI_VERSION=$(aws --version 2>&1 | cut -d/ -f2 | cut -d. -f1) [[${AWS_CLI_VERSION} -gt 1]] && ROOT_CA_CSR="$(echo ${ROOT_CA_CSR} | base64)"
	
	ROOT_CA_CERT_ARN= `aws acm-pca issue-certificate \ --certificate-authority-arn ${ROOT_CA_ARN} \ --template-arn arn:aws:acm-pca:::template/RootCACertificate/V1 \```
		AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`--signing-algorithm SHA256WITHRSA \` `--validity Value=10,Type=YEARS \` `--csr "${ROOT_CA_CSR}" \` `--query CertificateArn --output text` 3. Recupere el certificado de raíz. `ROOT_CA_CERT=`aws acm-pca get-certificate \` `--certificate-arn ${ROOT_CA_CERT_ARN} \` `--certificate-authority-arn ${ROOT_CA_ARN} \` `--query Certificate --output text`  `# store for later use` `aws acm-pca get-certificate \` `--certificate-arn ${ROOT_CA_CERT_ARN} \` `--certificate-authority-arn ${ROOT_CA_ARN} \` `--query Certificate --output text > ca-cert.pem`	

Tarea	Descripción	Habilidades requeridas

	4. Importe el certificado de CA raíz para instalarlo en la CA.
	
	`[[ ${AWS_CLI_VERSION} -gt 1 ]] && ROOT_CA_CERT="$(echo ${ROOT_CA_CERT} | base64)"`
	
	`aws acm-pca import-certificate-authority-certificate \ --certificate-authority-arn $ROOT_CA_ARN \ --certificate "${ROOT_CA_CERT}"`
	
	Para obtener más información, consulte Instalación del certificado de CA en la AWS documentación.	

Tarea	Descripción	Habilidades requeridas
Solicite un certificado administrado.	Para solicitar un certifica do privado AWS Certifica te Manager para usarlo con su ALB privado, utilice el siguiente comando: `export TLS_CERTI FICATE_ARN=`aws acm request-certificate \ --domain-name "*. ${DOMAIN_DOMAIN}" \ --certificate-auth ority-arn ${ROOT_CA _ARN} \ --query Certifica teArn --output text``	DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas

Utilice la CA privada para emitir un certificado de cliente.	• Para crear una solicitud de firma de certificado (CSR) para los dos servicios, utilice el siguiente AWS CLI comando:
	
	`openssl req -out client_csr1.pem -new -newkey rsa:2048 -nodes -keyout client_private-key 1.pem`
	
	`openssl req -out client_csr2.pem -new -newkey rsa:2048 -nodes -keyout client_private-key 2.pem`
	
	Este comando devuelve la CSR y la clave privada de los dos servicios.
	
	• Para emitir un certificado para los servicios, ejecute los comandos siguientes para utilizar la CA privada que creó:
	
	`SERVICE_ONE_CERT_ARN=`aws acm-pca issue-certificate \`
		DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`--certificate-authority-arn ${ROOT_CA_ARN} \` `--csr fileb://client_csr1.pem \` `--signing-algorithm "SHA256WITHRSA" \` `--validity Value=5,Type="YEARS" --query CertificateArn --output text` `echo "SERVICE_ONE_CERT_ARN: ${SERVICE_ONE_CERT_ARN}"` `aws acm-pca get-certificate \` `--certificate-authority-arn ${ROOT_CA_ARN} \` `--certificate-arn ${SERVICE_ONE_CERT_ARN} \` `| jq -r '.Certificate' > client_cert1.cert` `SERVICE_TWO_CERT_ARN=`aws acm-pca issue-certificate \` `--certificate-authority-arn ${ROOT_CA_ARN} \` `--csr fileb://client_csr2.pem \` `--signing-algorithm "SHA256WITHRSA" \` `--validity Value=5,Type="YEARS" --query CertificateArn --output text`	

Tarea	Descripción	Habilidades requeridas

	``
	echo "SERVICE_TWO_CERT_
	ARN: ${SERVICE
	_TWO_CERT_ARN}"
	
	aws acm-pca get-certi
	ficate \
	    --certificate-auth
	ority-arn ${ROOT_CA
	_ARN} \
	    --certificate-arn
	 ${SERVICE_TWO_CERT
	_ARN} \
	     | jq -r '.Certifi
	cate' > client_ce
	rt2.cert
	``
	
	Para obtener más información, consulte Emitir certificados de entidades finales privadas en la AWS documentación.	

Aprovisionamiento de servicios de AWS

Tarea	Descripción	Habilidades requeridas
Servicios de AWS Aprovisione con la CloudFormation plantilla.	Para aprovisionar la nube privada virtual (VPC), el clúster de Amazon ECS, los servicios de Amazon ECS, Application Load Balancer y Amazon Elastic Container Registry (Amazon ECR), utilice la plantilla. CloudFormation	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Obtenga las variables.	Verifique que tiene un clúster de Amazon ECS con dos servicios en ejecución. Para recuperar los detalles del recurso y almacenarlos como variables, utilice los comandos siguientes:
	
	`export LoadBalancerDNS=$(aws cloudformation describe-stacks --stack-name ecs-mtls \ --output text \ --query 'Stacks[0].Outputs[?OutputKey==`LoadBalancerDNS`].OutputValue')`
	
	`export ECRRepositoryUri=$(aws cloudformation describe-stacks --stack-name ecs-mtls \ --output text \ --query 'Stacks[0].Outputs[?OutputKey==`ECRRepositoryUri`].OutputValue')`
	
	`export ECRRepositoryServiceOneUri=$(aws cloudformation describe-stacks --stack-name ecs-mtls \ --output text \ --query 'Stacks[0].Outputs[?OutputKey==`ECRRepository`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	ServiceOneUri`].Ou tputValue')  export ECRReposi toryServiceTwoUri= $(aws cloudformation  describe-stacks -- stack-name ecs-mtls \ --output text \ --query 'Stacks[0 ].Outputs[?OutputK ey==`ECRRepository ServiceTwoUri`].Ou tputValue')  export ClusterName= $(aws cloudformation  describe-stacks -- stack-name ecs-mtls \ --output text \ --query 'Stacks[0 ].Outputs[?OutputK ey==`ClusterName`] .OutputValue')  export BucketName= $(aws cloudformation  describe-stacks -- stack-name ecs-mtls \ --output text \ --query 'Stacks[0 ].Outputs[?OutputK ey==`BucketName`]. OutputValue') export Service1L istenerArn=$(aws cloudformation describe-stacks -- stack-name ecs-mtls \ --output text \	

Tarea	Descripción	Habilidades requeridas

	`--query 'Stacks[0 ].Outputs[?OutputK ey==`Service1Liste nerArn`].OutputVal ue')`
	
	`export Service2L istenerArn=$(aws cloudformation describe-stacks -- stack-name ecs-mtls \ --output text \ --query 'Stacks[0 ].Outputs[?OutputK ey==`Service2Liste nerArn`].OutputVal ue')`	

Tarea	Descripción	Habilidades requeridas
Crea un CodeBuild proyecto.	Para usar un CodeBuild proyecto para crear las imágenes de Docker para sus servicios de Amazon ECS, haga lo siguiente: 1. Inicie sesión en y abra Consola de administración de AWS la CodeBuild consola en https://console.aws.amazon.com/codesuite/codebuild/. 2. Cree un nuevo proyecto de . En Origen, elija el repositorio de Git que creó. Para obtener información sobre los distintos tipos de integración de repositorios de Git, consulta Cómo trabajar con conexiones en la AWS documentación. 3. Confirme que el modo con privilegios esté habilitado. Este modo es necesario para crear imágenes de Docker. De lo contrario, la imagen no se compilará correctamente. 4. Utilice el archivo personalizado `buildspec.yaml` que se comparte para cada servicio.	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	5. Proporcione valores para el nombre y la descripción del proyecto. Para obtener más información, consulta Cómo crear un proyecto de compilación AWS CodeBuild en la AWS documentación.	

Tarea	Descripción	Habilidades requeridas

Cree las imágenes de Docker.	Se puede utilizar CodeBuild para realizar el proceso de creación de imágenes. CodeBuild necesita permisos para interactuar con Amazon ECR y trabajar con Amazon S3.
	
	Como parte del proceso, la imagen de Docker se compila y envía al registro de Amazon ECR. Para obtener informaci ón sobre la plantilla y el código, consulte Información adicional.
	
	(Opcional) Para compilar localmente con fines de prueba, utilice el siguiente comando:
	
	`# login to ECR`
	`aws ecr get-login`
	`-password | docker`
	`login --username`
	`AWS --password-stdin`
	`$ECRRepositoryUri`
	
	`# build image for`
	`service one`
	`cd /service1`
	`aws s3 cp s3://$Buc`
	`ketName/serviceone/`
	`service1/ --recursive`
	`docker build -t`
	`$ECRRepositoryServ`
	`iceOneUri .`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	`docker push $ECRRepositoryServiceOneUri`
	
	`# build image for service two`
	`cd ../service2`
	`aws s3 cp s3://$BucketName/servicetwo/service2/ --recursive`
	`docker build -t $ECRRepositoryServiceTwoUri .`
	`docker push $ECRRepositoryServiceTwoUri`	

Cómo inhabilitar la TLS mutua

Tarea	Descripción	Habilidades requeridas
Cargue el certificado CA en Amazon S3.	Para cargar el certificado CA en el bucket de Amazon S3, utilice el comando de ejemplo siguiente: `aws s3 cp ca-cert.pem s3://$BucketName/acm-trust-store/`	AWS DevOps, DevOps ingeniero
Cree un almacén de confianza .	Para crear el almacén de confianza, utilice el comando de ejemplo siguiente: `TrustStoreArn=`aws elbv2 create-trust-store --name acm-pca-trust-certs \`	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`--ca-certificates-bundle-s3-bucket $BucketName \ --ca-certificates-bundle-s3-key acm-trust-store/ca-cert.pem --query 'TrustStores[].TrustStoreArn' --output text`	

Cargue los certificados de cliente.	Para cargar los certificados de cliente en Amazon S3 para las imágenes de Docker, utilice el comando de ejemplo siguiente :
	
	`# for service one aws s3 cp client_cert1.cert s3://$BucketName/serviceone/ aws s3 cp client_private-key1.pem s3://$BucketName/serviceone/`
	
	`# for service two aws s3 cp client_cert2.cert s3://$BucketName/servicetwo/ aws s3 cp client_private-key2.pem s3://$BucketName/servicetwo/`
		AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Modifique el oyente.	Para habilitar el TLS mutuo en el ALB, modifique los oyentes HTTPS con los comandos siguientes:
	
	`aws elbv2 modify-listener \`
	`  --listener-arn $Service1ListenerArn \`
	`  --certificates CertificateArn=$TLS_CERTIFICATE_ARN_TWO \`
	`  --ssl-policy ELBSecurityPolicy-2016-08 \`
	`  --protocol HTTPS \`
	`  --port 8080 \`
	`  --mutual-authentication Mode=verify,TrustStoreArn=$TrustStoreArn,IgnoreClientCertificateExpiry=false`
	
	`aws elbv2 modify-listener \`
	`  --listener-arn $Service2ListenerArn \`
	`  --certificates CertificateArn=$TLS_CERTIFICATE_ARN_TWO \`
	`  --ssl-policy ELBSecurityPolicy-2016-08 \`
	`  --protocol HTTPS \`
	`  --port 8090 \`
		AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`--mutual-authentication Mode=verify,TrustStoreArn=$TrustStoreArn,IgnoreClientCertificateExpiry=false` Para obtener más información, consulte Configuración del TLS mutuo en un Application Load Balancer en AWS la documentación.	

Actualización de los servicios

Tarea	Descripción	Habilidades requeridas
Actualice la definición de tareas de Amazon ECS.	Para actualizar la definición de tareas de Amazon ECS, modifique el parámetro `image` en la revisión nueva. Para obtener los valores de los servicios respectivos, actualice las definiciones de tareas con la nueva URI de imágenes de Docker que creó en los pasos anteriores: `echo $ECRRepositoryServiceOneUri` o `echo $ECRRepositoryServiceTwoUri` `"containerDefinitions": [`	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	<pre>{
	"name":
	"nginx",
	"image":
	"public.ecr.aws/ng
	inx/nginx:latest",
	# <----- change to new
	Uri
	"cpu": 0,</pre>
	Para obtener más información, consulte Actualización de una definición de tarea de Amazon ECS mediante la consola en la AWS documentación.	

Tarea	Descripción	Habilidades requeridas
Actualice el servicio Amazon ECS.	Actualice el servicio con la última definición de tareas. Esta definición de tareas es el esquema de las imágenes de Docker recién creadas y contiene el certificado de cliente que se requiere para la autenticación de TLS mutua. Para actualizar el servicio, proceda de la manera siguiente: 1. Abra la consola Amazon ECS en la https://console.aws.amazon.com/ecs/versión 2. 2. En la página Clusters (Clústeres), elija el clúster. 3. En la página de detalles del clúster, en la sección Servicios, seleccione la casilla situada junto al servicio y, a continuación, elija Actualizar. 4. Para que su servicio inicie una nueva implementación, seleccione Force new deployment (Forzar una nueva implementación). 5. En Definición de tareas, elija la familia y la última revisión de definiciones de tareas.	Administrador de AWS DevOps, DevOps ingeniero de AWS

Tarea	Descripción	Habilidades requeridas
	6. Elija Actualizar. Repita los pasos para el otro servicio.	

Acceda a la aplicación

Tarea	Descripción	Habilidades requeridas
Copie la URL de la aplicación.	Utilice la consola de Amazon ECS para ver la tarea. Cuando el estado de la tarea se haya actualizado a En ejecución , seleccione la tarea. En la sección Tarea, copie el ID de la tarea.	Administrador de AWS, AWS DevOps

Pruebe su aplicación.	Para probar la aplicación, utilice ECS Exec para acceder a las tareas.
	
	1. Para el servicio uno, utilice el comando siguiente:
	
	`container="nginx"`
	
	`ECS_EXEC_TASK_ARN ="<TASK ARN>" aws ecs execute-c ommand --cluster $ClusterName \ --task $ECS_EXEC _TASK_ARN \ --container $container \ --interactive \`
		Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`--command "/bin/bash"`
	2. En el contenedor de la tarea del servicio uno, utilice el comando siguiente para introducir el equilibrador de carga interno `url` y el puerto del oyente que apunta al servicio dos. A continuación, especifique la ruta al certificado del cliente para probar la aplicación:
	`curl -kvs https://<internal-alb-url>:8090 --key /usr/local/share/ca-certificates/client.key --cert /usr/local/share/ca-certificates/client.crt`
	3. En el contenedor de la tarea del servicio dos, utilice el comando siguiente para introducir el equilibrador de carga interno `url` y el puerto del oyente que apunta al servicio uno. A continuación, especifique la ruta al certificado del cliente para probar la aplicación:
	`curl -kvs https://<internal-alb-url>:8080 --key /usr/local/share/ca-certifi`	

Tarea	Descripción	Habilidades requeridas
	`cates/client.key --cert /usr/local/share/ca-certificates/client.crt` **Note** El indicador `-k` de los comandos curl (como parte de `-kvs`) inhabilita la validación del certificado SSL. Puede eliminar este indicador cuando utilice un certificado SSL que coincida con el nombre de su dominio, lo que permitirá una validación adecuada del certificado.	

Recursos relacionados

Documentación de Amazon ECS

- Creación de una definición de tarea de Amazon ECS mediante la consola
- Creación de una imagen de contenedor para su uso en Amazon ECS
- Clústeres de Amazon ECS
- Amazon ECS para AWS Fargate
- Mejores prácticas de redes de Amazon ECS
- Parámetros de definición del servicio Amazon ECS

Otros AWS recursos

- ¿Cómo uso una CA AWS privada para configurar los mTLS en el Application Load Balancer? ()AWS re:Post

Información adicional

Edición del Dockerfile

El siguiente código muestra los comandos que edita en el Dockerfile para el servicio 1:

```
FROM public.ecr.aws/nginx/nginx:latest
WORKDIR /usr/share/nginx/html
RUN echo "Returning response from Service 1: Ok" > /usr/share/nginx/html/index.html
ADD client_cert1.cert client_private-key1.pem /usr/local/share/ca-certificates/
RUN chmod -R 400 /usr/local/share/ca-certificates/
```

El siguiente código muestra los comandos que edita en el Dockerfile para el servicio 2:

```
FROM public.ecr.aws/nginx/nginx:latest
WORKDIR /usr/share/nginx/html
RUN echo "Returning response from Service 2: Ok" > /usr/share/nginx/html/index.html
ADD client_cert2.cert client_private-key2.pem /usr/local/share/ca-certificates/
RUN chmod -R 400 /usr/local/share/ca-certificates/
```

Si está creando las imágenes de Docker CodeBuild, el `buildspec` archivo utiliza el número de CodeBuild compilación para identificar de forma exclusiva las versiones de las imágenes como un valor de etiqueta. Puede cambiar el archivo `buildspec` para adaptarlo a sus necesidades, como se muestra en el código personalizado `buildspec` :

```
version: 0.2

phases:
  pre_build:
    commands:
      - echo Logging in to Amazon ECR...
      - aws ecr get-login-password --region $AWS_DEFAULT_REGION | docker login --
username AWS --password-stdin $ECR_REPOSITORY_URI
      - COMMIT_HASH=$(echo $CODEBUILD_RESOLVED_SOURCE_VERSION | cut -c 1-7)
      - IMAGE_TAG=${COMMIT_HASH:=latest}
  build:
```

```
    commands:
        # change the S3 path depending on the service
      - aws s3 cp s3://$YOUR_S3_BUCKET_NAME/serviceone/ $CodeBuild_SRC_DIR/ --
recursive
      - echo Build started on `date`
      - echo Building the Docker image...
      - docker build -t $ECR_REPOSITORY_URI:latest .
      - docker tag $ECR_REPOSITORY_URI:latest $ECR_REPOSITORY_URI:$IMAGE_TAG
  post_build:
    commands:
      - echo Build completed on `date`
      - echo Pushing the Docker images...
      - docker push $ECR_REPOSITORY_URI:latest
      - docker push $ECR_REPOSITORY_URI:$IMAGE_TAG
      - echo Writing image definitions file...
      # for ECS deployment reference
      - printf '[{"name":"%s","imageUri":"%s"}]' $CONTAINER_NAME $ECR_REPOSITORY_URI:
$IMAGE_TAG > imagedefinitions.json

artifacts:
  files:
    - imagedefinitions.json
```

Más patrones

- Automatice la eliminación de AWS CloudFormation pilas y recursos asociados
- Automatice la gestión dinámica de canalizaciones para implementar soluciones de hotfix en entornos de Gitflow mediante el uso y AWS Service Catalog AWS CodePipeline
- Cree CI/CD canalizaciones y clústeres de Amazon ECS de forma automática para microservicios mediante AWS CDK
- Cree e inserte imágenes de Docker en Amazon ECR mediante GitHub Actions y Terraform
- Almacenamiento en contenedores de las cargas de trabajo de mainframe que Blu Age ha modernizado
- Crear un analizador de registros personalizado para Amazon ECS mediante un enrutador de registros Firelens
- Implementación de sistemas de agentes en Amazon Bedrock con el marco CrewAI mediante Terraform
- Implementar un entorno para aplicaciones de Blu Age en contenedores mediante Terraform
- Implemente la lógica de preprocesamiento en un modelo de aprendizaje automático en un único punto final mediante una canalización de inferencias en Amazon SageMaker
- Implemente cargas de trabajo desde DevOps canalizaciones de Azure a clústeres privados de Amazon EKS
- Implementación de diagnósticos y solución de problemas de Kubernetes con tecnología de IA con la integración de K8sGPT y Amazon Bedrock
- Gestione blue/green las implementaciones de microservicios en varias cuentas y regiones mediante los servicios de código de AWS y las claves multirregionales de AWS KMS
- Gestión de las aplicaciones de contenedores en las instalaciones mediante la configuración de Amazon ECS Anywhere con AWS CDK
- Migre de Oracle WebLogic a Apache Tomcat (ToMEE) en Amazon ECS
- Supervise los repositorios de Amazon ECR en busca de permisos comodín mediante AWS y AWS Config CloudFormation
- Supervise la actividad de las aplicaciones mediante CloudWatch Logs Insights
- Configure una CI/CD canalización para cargas de trabajo híbridas en Amazon ECS Anywhere mediante AWS CDK y GitLab
- Configure el end-to-end cifrado para aplicaciones en Amazon EKS mediante cert-manager y Let's Encrypt

- Simplificación de la implementación de aplicaciones multiusuario de Amazon EKS mediante Flux
- Optimice los flujos de trabajo de aprendizaje automático desde el desarrollo local hasta los experimentos escalables mediante el uso de SageMaker IA e Hydra
- Estructure un proyecto de Python en una arquitectura hexagonal con AWS Lambda
- Pruebe AWS la infraestructura mediante LocalStack Terraform Tests
- Coordine la dependencia de los recursos y la ejecución de tareas mediante la construcción AWS Fargate WaitCondition hook
- Uso de agentes de Amazon Bedrock para automatizar la creación de controles de entrada de acceso en Amazon EKS mediante peticiones basadas en texto

Sin servidor

Temas

- Cree una aplicación móvil React Native sin servidor con AWS Amplify
- Administrar los inquilinos de varios productos SaaS en un único plano de control
- Consolidación de la generación de URL prefirmadas y las descargas de objetos de Amazon S3 mediante un punto de conexión asociado a direcciones IP estáticas
- Crear una EventBridge conexión entre cuentas de Amazon en una organización
- Entregue registros de DynamoDB a Amazon S3 mediante Kinesis Data Streams y Firehose con AWS CDK
- Implementación del control de versiones de API basado en rutas mediante dominios personalizados en Amazon API Gateway
- Importe la biblioteca psycopg2 para interactuar con su base de AWS Lambda datos PostgreSQL
- Integre Amazon API Gateway con Amazon SQS para gestionar el REST asíncrono APIs
- Procesamiento de eventos de forma asíncrona con Amazon API Gateway y AWS Lambda
- Procesamiento de eventos de forma asíncrona con Amazon API Gateway y Amazon DynamoDB Streams
- Procesamiento de eventos de forma asíncrona con Amazon API Gateway, Amazon SQS y AWS Fargate
- Puesta en marcha de las tareas de Automatización de AWS Systems Manager de forma sincrónica desde AWS Step Functions
- Ejecute lecturas paralelas de objetos S3 mediante Python en una AWS Lambda función
- Envíe datos de telemetría desde y AWS Lambda OpenSearch para análisis y visualización en tiempo real
- Configuración de un router de celdas sin servidor para una arquitectura basada en celdas
- Configuración del acceso privado a un bucket de Amazon S3 a través de un punto de conexión de VPC
- Solucione problemas de estados AWS Step Functions mediante Amazon Bedrock
- Más patrones

Cree una aplicación móvil React Native sin servidor con AWS Amplify

Deekshitulu Pentakota, Amazon Web Services

Resumen

Este patrón muestra cómo crear un backend sin servidor para una aplicación móvil React Native mediante AWS Amplify y los siguientes servicios de AWS:

- AWS AppSync
- Amazon Cognito
- Amazon DynamoDB

Tras configurar e implementar el backend de la aplicación mediante Amplify, Amazon Cognito autentica a los usuarios y los autoriza a acceder a la aplicación. AppSync A continuación, AWS interactúa con la aplicación de interfaz y con una tabla de DynamoDB de backend para crear y obtener datos.

> **Note**
>
> En este patrón se utiliza una sencilla aplicación «ToDoList» como ejemplo, pero puede utilizar un procedimiento similar para crear cualquier aplicación móvil de React Native.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de Amplify (Amplify CLI) instalada y configurada
- XCode (cualquier versión)
- Microsoft Visual Studio (cualquier versión, cualquier editor de código, cualquier editor de texto)
- Familiaridad con Amplify
- Familiaridad con Amazon Cognito
- Familiaridad con AWS AppSync

- Familiaridad con DynamoDB
- Familiaridad con Node.js
- Familiarización con npm
- Familiaridad con React y React Native
- Familiaridad con JavaScript y (ECMAScript 6) ES6
- Familiaridad con GraphQL

Arquitectura

El siguiente diagrama muestra un ejemplo de arquitectura para ejecutar el backend de una aplicación móvil React Native en la nube de AWS:

En el siguiente diagrama se muestra la arquitectura:

1. Amazon Cognito autentica a los usuarios y los autoriza a acceder a la aplicación.
2. Para crear y obtener datos, AWS AppSync utiliza una API de GraphQL para interactuar con la aplicación de frontend y una tabla de DynamoDB de backend.

Tools (Herramientas)

Servicios de AWS

- AWS Amplify es un conjunto de herramientas y características diseñadas específicamente que permiten a los desarrolladores web y móviles de frontend crear aplicaciones de pila completa en AWS de manera rápida.
- AWS AppSync proporciona una interfaz GraphQL escalable que ayuda a los desarrolladores de aplicaciones a combinar datos de varias fuentes, incluidas Amazon DynamoDB, AWS Lambda y HTTP. APIs
- Amazon Cognito ofrece autenticación, autorización y administración de usuarios para aplicaciones móviles y web.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.

Código

El código de la aplicación de muestra que se utiliza en este patrón está disponible en el repositorio -. GitHub aws-amplify-react-native ios-todo-app Para usar los archivos de ejemplo, siga las instrucciones de la sección Épica de este patrón.

Epics

Cree y ejecute su aplicación React Native

Tarea	Descripción	Habilidades requeridas
Configure un entorno de desarrollo React Native.	Para obtener instrucciones, consulte Configurar el entorno de desarrollo en la documentación de React Native.	Desarrollador de aplicaciones

Cree y ejecute la aplicación móvil ToDoList React Native en el simulador de iOS.	1. Cree un nuevo directorio de proyecto de aplicación móvil React Native en su entorno local ejecutando el siguiente comando en una nueva ventana de terminal:
	`npx react-native init ToDoListAmplify`
	2. Navegue hasta el directorio raíz del proyecto ejecutando el siguiente comando:
	`cd ToDoListAmplify`
	3. Ponga en marcha la aplicación ejecutando el siguiente comando:
	`npx react-native run-ios`
		Desarrollador de aplicaciones

Inicialice un nuevo entorno backend para la aplicación

Tarea	Descripción	Habilidades requeridas

Cree los servicios de backend necesarios para respaldar la aplicación en Amplify.	1. En tu entorno local, ejecuta el siguiente comando desde el directorio raíz del proyecto (ToDoListAmplify):
	`amplify init`
	2. Aparecerá un mensaje solicitando informaci ón sobre la aplicación. Introduzca la información requerida en función del caso de uso. A continuac ión, pulse Intro.
	
	Para la configuración de la ToDoList aplicación utilizada en este patrón, aplique la siguiente configuración de ejemplo.
	
	Ejemplo de ajustes de configuración de aplicación React Native en Amplify
	`? Name: ToDoListAmplify`
	`? Environment: dev`
	`? Default editor: Visual Studio Code`
	`? App type: javascript`
	`? Javascript framework : react-native`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	? Source Directory Path: src ? Distribution Directory Path: / ? Build Command: npm run-script build ? Start Command: npm run-script start ? Select the authentic ation method you want to use: AWS profile ? Please choose the profile you want to use: default Para obtener más informaci ón, consulte Crear un nuevo backend de Amplify en la documentación de Amplify Dev Center. **Note** El `amplify init` comando aprovisio na los siguientes recursos mediante AWS CloudForm ation:	

Tarea	Descripción	Habilidades requeridas
	• Roles de AWS Identity and Access Management (IAM) para usuarios autenticados y no autenticados (rol Auth y rol Unauth) • Un bucket de Amazon Simple Storage Service (Amazon S3) para implementación (para la aplicación de ejemplo de este patrón, Amplify-meta.json. • Un entorno de backend en Amplify Hosting	

Añada la autenticación de Amazon Cognito a su aplicación React Native de Amplify

Tarea	Descripción	Habilidades requeridas
Cree un servicio de autenticación de Amazon Cognito.	1. En su entorno local, ejecute el siguiente comando desde el directorio raíz del proyecto (ToDoListAmplify): `amplify add auth` 2. Aparecerá un mensaje solicitando información sobre los ajustes de configuración del servicio de autenticación. Introduzca la información requerida en función del caso de uso. A continuación, pulse Intro.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	Para la configuración de la ToDoList aplicación utilizada en este patrón, aplique la siguiente configuración de ejemplo.
	
	Ejemplo de ajustes de configuración del servicio de autenticación
	
	`? Do you want to use the default authentication and security configuration? \`
	`Default configuration`
	
	`? How do you want users to be able to sign in? \`
	`Username`
	
	`? Do you want to configure advanced settings? \`
	`No, I am done`
	
	Note
	El comando `amplify add auth` crea las carpetas, archivos y archivos de dependencia necesarios en una carpeta local (amplify) dentro del directorio raíz del proyecto. Para	

Tarea	Descripción	Habilidades requeridas
	la configuración de la ToDoList aplicación utilizada en este patrón, se crea el archivo aws-exports.js con este fin.	

Implemente el servicio de Amazon Cognito en la nube de AWS.	1. Desde el directorio raíz del proyecto, ejecute el siguiente comando en la CLI de Amplify:
	`amplify push`
	2. Aparecerá un mensaje para confirmar la implementación. Introduzca Sí. A continuación, pulse Intro.
	Note
	Para ver los servicios implementados en su proyecto, acceda a la consola de Amplify ejecutando el siguiente comando:
	`amplify console`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Instala las bibliotecas Amplify necesarias para React Native y las CocoaPods dependencias para iOS.	1. Instale las bibliotecas cliente de código abierto de Amplify necesarias ejecutando el siguiente comando desde el directorio raíz del proyecto:
	`npm install aws-amplify aws-amplify-react-native \ amazon-cognito-identity-js @react-native-community/netinfo \ @react-native-async-storage/async-storage`
	2. Instala CocoaPods las dependencias necesarias para iOS ejecutando el siguiente comando:
	`npx pod-install`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Importe y configure el servicio Amplify.	En el archivo de punto de entrada de la aplicación (por ejemplo, App.js), importe y cargue el archivo de configuración del servicio Amplify introduciendo las siguientes líneas de código:
	`import Amplify from 'aws-amplify'`
	`import config from './src/aws-exports'`
	`Amplify.configure(config)`
	Note
	Si recibe un error después de importar el servicio Amplify en el archivo de punto de entrada de la aplicación, deténgala. A continuación, abre XCode y selecciona el ToDoListAmplifyarchivo.xcworkspace de la carpeta iOS del proyecto y ejecuta la aplicación.
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Actualice el archivo de punto de entrada de la aplicación para usar el componente de orden superior (HOC) withAuthenticator.	**Note** El HOC `withAuthenticator` proporciona flujos de trabajo para iniciar sesión, registrarse y recuperar contraseñas en su aplicación con unas pocas líneas de código. Para obtener más información, consulte Opción 1: usar componentes de interfaz de usuario precompilados en Amplify Dev Center. También puede consultar Componentes de orden superior en la documentación de React. 1. En el archivo de punto de entrada de la aplicación (por ejemplo,App.js), importe el HOC `withAuthenticator` introduciendo las siguientes líneas de código: `import { withAuthenticator } from`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	`'aws-amplify-react-native'`
	2. Exporte el HOC withAuthenticator introduciendo el siguiente código:
	`export default withAuthenticator(App)`
	
	Ejemplo de código de HOC withAuthenticator
	
	`import Amplify from 'aws-amplify'`
	`import config from './src/aws-exports'`
	`Amplify.configure(config)`
	`import { withAuthenticator } from 'aws-amplify-react-native';`
	
	`const App = () => {`
	`  return null;`
	`};`
	
	`export default withAuthenticator(App);`
	
	Note
	En el simulador de iOS, la aplicación muestra la pantalla de	

Tarea	Descripción	Habilidades requeridas
	inicio de sesión que proporciona el servicio Amazon Cognito.	
Pruebe la configuración del servicio de autenticación.	En el simulador de iOS, haga lo siguiente: 1. Cree una cuenta nueva en la aplicación con una dirección de correo electrónico real. Se enviará un código de verificación al correo electrónico registrado. 2. Verifique la cuenta configurada con el código que ha recibido en el correo electrónico de verificación. 3. Introduzca el nombre de usuario y la contraseña que ha creado. A continuación, seleccione Iniciar sesión. Aparecerá una pantalla de bienvenida. **Note** También puede abrir la consola de Amazon Cognito y comprobar si se ha creado un nuevo usuario en el grupo de identidades.	Desarrollador de aplicaciones

Conectar una AppSync API de AWS y una base de datos de DynamoDB a la aplicación

Tarea	Descripción	Habilidades requeridas
Cree una AppSync API de AWS y una base de datos de DynamoDB.	1. Añada una AppSync API de AWS a su aplicación y aprovisione automátic amente una base de datos de DynamoDB mediante la ejecución del siguiente comando de Amplify CLI desde el directorio raíz del proyecto: `amplify add api` 2. Aparecerá un aviso que le pedirá información sobre la API y los ajustes de configuración de la base de datos. Introduzca la información requerida en función del caso de uso. A continuación, pulse Intro. La CLI de Amplify abre el archivo de esquema de GraphQL en su editor de texto. Para la configuración de la ToDoList aplicación utilizada en este patrón, aplique la siguiente configuración de ejemplo. Ejemplo de ajustes de configuración de API y base de datos	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	? Please select from one of the below mentioned services: \ GraphQL ? Provide API name: todolistamplify ? Choose the default authorization type for the API \ Amazon Cognito User Pool Do you want to use the default authentication and security configura tion ? Default configuration How do you want users to be able to sign in? \ Username Do you want to configure advanced settings? \ No, I am done. ? Do you want to configure advanced settings for the GraphQL API \ No, I am done. ? Do you have an annotated GraphQL schema? \ No ? Choose a schema template: \	

Tarea	Descripción	Habilidades requeridas

	Single object with fields (e.g., "Todo" with ID, name, description)
	
	? Do you want to edit the schema now? \
	Yes
	
	Ejemplo de esquema de GraphQL
	
	type Todo @model {
	id: ID!
	name: String!
	description: String
	}	

Tarea	Descripción	Habilidades requeridas
Implemente la AppSync API de AWS.	1. Desde el directorio raíz del proyecto, ejecute el siguiente comando en la CLI de Amplify: `amplify push` 2. Aparecerá un aviso que le pedirá más información sobre la API y los ajustes de configuración de la base de datos. Introduzca la información requerida en función del caso de uso. A continuación, pulse Intro. Su aplicación ahora puede interactuar con la AppSync API de AWS. Para la configuración de la ToDoList aplicación utilizada en este patrón, aplique la siguiente configuración de ejemplo. Ejemplo de ajustes de configuración AppSync de la API de AWS **Note** La siguiente configuración crea la API GraphQL en AWS	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	AppSync y una tabla Todo en Dynamo DB. ? Are you sure you want to continue? Yes ? Do you want to generate code for your newly created GraphQL API Yes ? Choose the code generation language target javascript ? Enter the file name pattern of graphql queries, mutations and subscriptions src/graphql/**/*.js ? Do you want to generate/update all possible GraphQL operations - \ queries, mutations and subscriptions Yes ? Enter maximum statement depth \ [increase from default if your schema is deeply nested] 2	

Tarea	Descripción	Habilidades requeridas
Conecta la interfaz de la aplicación a la AppSync API de AWS.	Para usar la ToDoList aplicación de ejemplo que se proporciona en este patrón, copie el código del archivo App.js del ios-todo-app GitHub repositorio aws-amplify-react-native-. A continuación, integre el código de ejemplo en su entorno local. El código de ejemplo proporcionado en el archivo App.js del repositorio hace lo siguiente: • Muestra el formulario para crear un ToDo elemento con los campos de título y descripción • Muestra la lista de tareas pendientes (Título y Descripción) • Publica y recupera datos mediante métodos de `aws-amplify`	Desarrollador de aplicaciones

Recursos relacionados

- AWS Amplify
- Amazon Cognito
- AWS AppSync
- Amazon DynamoDB
- React (documentación de React)

Administrar los inquilinos de varios productos SaaS en un único plano de control

Ramanna Avancha, Kishan Kavala, Anusha Mandava y Jenifer Pascal, Amazon Web Services

Resumen

Este patrón muestra cómo gestionar los ciclos de vida de los inquilinos en varios productos de software como servicio (SaaS) en un único plano de control en la nube de AWS. La arquitectura de referencia proporcionada puede ayudar a las organizaciones a reducir la implementación de características redundantes y compartidas en sus productos SaaS individuales y a proporcionar eficiencias de gobierno a escala.

Las grandes empresas pueden tener varios productos SaaS en varias unidades de negocio. A menudo, estos productos deben aprovisionarse para que los utilicen inquilinos externos con diferentes niveles de suscripción. Sin una solución de usuario común, los administradores de TI deben dedicar tiempo a administrar funciones indiferenciadas en varios APIs SaaS, en lugar de centrarse en el desarrollo de las funciones principales del producto.

La solución de inquilino común que se proporciona en este patrón puede ayudar a centralizar la administración de muchas de las características de los productos SaaS compartidos de una organización, incluidas las siguientes:

- Seguridad
- Aprovisionamiento de inquilinos
- Almacenamiento de datos del inquilino
- Comunicaciones con los inquilinos
- Gestión de productos
- Registro y supervisión de métricas

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Conocimiento de Amazon Cognito o de un proveedor de identidades (IdP) externo

- Conocimiento de Amazon API Gateway
- Conocimiento de AWS Lambda
- Conocimiento de Amazon DynamoDB
- Conocimientos de AWS Identity and Access Management (IAM)
- Conocimiento de AWS Step Functions
- Conocimientos de AWS CloudTrail y Amazon CloudWatch
- Conocimiento de las bibliotecas y el código de Python
- Conocimiento del SaaS APIs, incluidos los diferentes tipos de usuarios (organizaciones, inquilinos, administradores y usuarios de aplicaciones), los modelos de suscripción y los modelos de aislamiento de inquilinos
- Conocimiento de los requisitos de SaaS multiproducto y de las suscripciones multiusuario de su organización

Limitaciones

- Las integraciones entre la solución de inquilino común y los productos SaaS individuales no se incluyen en este patrón.
- Este patrón implementa el servicio Amazon Cognito únicamente en una sola región de AWS.

Arquitectura

Pila de tecnología de destino

- Amazon API Gateway
- Amazon Cognito
- AWS CloudTrail
- Amazon CloudWatch
- Amazon DynamoDB
- IAM
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon Simple Notification Service (Amazon SNS)
- AWS Step Functions

Arquitectura de destino

El siguiente diagrama muestra un ejemplo de flujo de trabajo para administrar los ciclos de vida de los inquilinos en varios productos SaaS en un único plano de control en la nube de AWS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario de AWS inicia el aprovisionamiento de inquilinos, el aprovisionamiento de productos o las acciones relacionadas con la administración mediante una llamada a un punto de conexión de API Gateway.
2. El usuario se autentica mediante un token de acceso que se recupera de un grupo de usuarios de Amazon Cognito o de otro IdP.
3. Las tareas individuales de aprovisionamiento o administración se ejecutan mediante funciones de Lambda que se integran con los puntos de conexión de API de API Gateway.
4. La administración APIs de la solución Common Tenant (para inquilinos, productos y usuarios) recopila todos los parámetros de entrada, encabezados y símbolos necesarios. A continuación, la administración APIs invoca las funciones Lambda asociadas.
5. El servicio de IAM valida los permisos de IAM tanto para la administración APIs como para las funciones de Lambda.
6. Las funciones de Lambda almacenan y recuperan datos de los catálogos (para inquilinos, productos y usuarios) en DynamoDB y Amazon S3.
7. Una vez validados los permisos, se invoca un flujo de trabajo de AWS Step Functions para realizar una tarea específica. El ejemplo del diagrama muestra un flujo de trabajo de aprovisionamiento de inquilinos.
8. Las tareas individuales del flujo de trabajo de AWS Step Functions se ejecutan en un flujo de trabajo predeterminado (máquina de estado).
9. Todos los datos esenciales necesarios para ejecutar la función de Lambda asociada a cada tarea del flujo de trabajo se recuperan de DynamoDB o Amazon S3. Es posible que sea necesario aprovisionar otros recursos de AWS mediante una CloudFormation plantilla de AWS.
10. Si es necesario, el flujo de trabajo envía una solicitud para aprovisionar recursos de AWS adicionales para un producto SaaS específico a la cuenta de AWS de ese producto.
11. Cuando la solicitud se realiza correctamente o no, el flujo de trabajo publica la actualización de estado como un mensaje en un tema de Amazon SNS.
12. Amazon SNS está suscrito al tema Amazon SNS del flujo de trabajo Step Functions.

13 A continuación, Amazon SNS envía la actualización del estado del flujo de trabajo al usuario de AWS.

14 Los registros de las acciones de cada servicio de AWS, incluida una pista de auditoría de las llamadas a la API, se envían a CloudWatch. Se pueden configurar reglas y alarmas específicas CloudWatch para cada caso de uso.

15 Los registros se archivan en buckets de Amazon S3 para fines de auditoría.

Automatización y escala

Este patrón utiliza una CloudFormation plantilla para ayudar a automatizar la implementación de la solución Common Tenant. La plantilla también puede ayudarlo a escalar o reducir verticalmente los recursos asociados con rapidez.

Para obtener más información, consulte Trabajar con CloudFormation plantillas de AWS en la Guía del CloudFormation usuario de AWS.

Tools (Herramientas)

Servicios de AWS

- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket APIs a cualquier escala.
- Amazon Cognito ofrece autenticación, autorización y administración de usuarios para aplicaciones móviles y web.
- AWS le CloudTrail ayuda a auditar la gobernanza, el cumplimiento y el riesgo operativo de su cuenta de AWS.
- Amazon le CloudWatch ayuda a monitorizar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de Lambda AWS y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial.

Prácticas recomendadas

La solución de este patrón utiliza un único plano de control para gestionar la incorporación de varios inquilinos y proporcionar acceso a varios productos de SaaS. El plano de control ayuda a los usuarios administrativos a gestionar otros cuatro planos con características específicas:

- Plano de seguridad
- Plano de flujo de trabajo
- Plano de comunicación
- Plano de registro y monitoreo

Epics

Configuración del plano de seguridad

Tarea	Descripción	Habilidades requeridas
Establezca los requisitos para su plataforma SaaS multiusuario.	Establezca requisitos detallados para lo siguiente: • Inquilinos • Users • Roles • Productos SaaS de • Suscripciones • Intercambios de perfiles	Arquitecto de la nube, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
Configure el servicio de Amazon Cognito.	Siga las instrucciones de Introducción a Amazon Cognito de la Guía para desarrolladores de Amazon Cognito.	Arquitecto de la nube
Configure las políticas de IAM necesarias.	Cree las políticas de IAM necesarias para su caso de uso. A continuación, asigne las políticas a los roles de IAM en Amazon Cognito. Para obtener más información, consulte Administrar el acceso mediante políticas y Control de acceso basado en roles en la Guía para desarrolladores de Amazon Cognito.	Administrador de la nube, arquitecto de la nube, seguridad de AWS IAM
Configure los permisos de API necesarios.	Configure los permisos de acceso a API Gateway mediante roles y políticas de IAM y autorizadores Lambda. Para obtener instrucciones, consulte las secciones siguientes de la Guía de desarrolladores de Amazon API Gateway: • Control del acceso a una API con permisos de IAM • Uso de autorizadores Lambda de API Gateway	Administrador de la nube, arquitecto de la nube

Configuración del plano de datos

Tarea	Descripción	Habilidades requeridas
Cree los catálogos de datos necesarios.	1. Cree tablas de DynamoDB para almacenar los datos de los catálogos de usuarios. Asegúrese de incluir los atributos y funciones de los usuarios. Además, asegúrese de modelar los datos en las tablas del catálogo para mantener los atributos obligatorios y opcionales de cada usuario y función. 2. Cree tablas de DynamoDB para almacenar los datos de los catálogos de productos. Asegúrese de modelar los casos de uso específicos para sus productos SaaS. 3. Cree tablas de DynamoDB para almacenar los datos de los catálogos de inquilinos. Asegúrese de configurar los modelos de suscripción para los inquilinos, los productos y las licencias para las suscripciones multiSaaS y las etiquetas. Para obtener más informaci ón, consulte Configuración de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.	

Configuración del plano de control

Tarea	Descripción	Habilidades requeridas
Cree funciones Lambda y API Gateway APIs para ejecutar las tareas necesarias del plano de control.	Cree funciones Lambda y API Gateway independientes APIs para añadir, eliminar y gestionar lo siguiente: • Users • Inquilinos • Productos Para obtener más información, consulte Uso de AWS Lambda con Amazon API Gateway en la Guía para desarrolladores de AWS Lambda.	Desarrollador de aplicaciones

Configuración del plano de flujo de trabajo

Tarea	Descripción	Habilidades requeridas
Identifique las tareas que deben ejecutar los flujos de trabajo de AWS Step Functions.	Identifique y documente los requisitos detallados del flujo de trabajo de AWS Step Functions para lo siguiente: • Users	Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	• Inquilinos • Productos **Important** Asegúrese de que las partes interesadas clave aprueben los requisitos.	

Tarea	Descripción	Habilidades requeridas
Cree los flujos de trabajo de AWS Step Functions necesarios.	1. Cree los flujos de trabajo necesarios para los usuarios, inquilinos y productos en AWS Step Functions. Para obtener más información, consulte la Guía para desarrolladores de AWS Step Functions. 2. Identifique los mecanismos de reintentos y gestión de errores. Para obtener más información, consulte Gestión de errores, reintentos y añadir alertas a las máquinas de estado de Step Function en el blog de AWS. 3. Implemente los pasos del flujo de trabajo mediante funciones de Lambda. Para obtener instrucciones, consulte Creación de una máquina de estado de Step Functions que utilice Lambda en la Guía para desarrolladores de AWS Step Functions. 4. Integre cualquier servicio externo con AWS Step Functions según sea necesario. 5. Mantenga el estado de cada flujo de trabajo en	Desarrollador de aplicaciones, responsable de compilación

Tarea	Descripción	Habilidades requeridas
	una tabla de DynamoDB y comunique el estado de cada flujo de trabajo mediante Amazon SNS.	

Configuración del plano de comunicación

Tarea	Descripción	Habilidades requeridas
Crear temas de Amazon SNS.	Cree temas de Amazon SNS para recibir notificaciones sobre lo siguiente: • Estados del flujo de trabajo • Errores • Reintentos Para obtener más informaci ón, consulte Creación de un tema de SNS en la Guía para desarrolladores de Amazon SNS.	Propietario de la aplicación, arquitecto de la nube
Suscribir puntos de conexión a cada tema de Amazon SNS.	Para recibir los mensajes publicados en un tema de Amazon SNS, tiene que suscribirse a un punto de conexión en cada tema. Para obtener más información, consulte el tema Suscripción a un tema de Amazon SNS en la Guía para desarrolladores de Amazon SNS.	Desarrollador de aplicaciones, arquitecto de la nube

Configuración del plano de registro y supervisión

Tarea	Descripción	Habilidades requeridas
Active el registro para cada componente de la solución común para inquilinos.	Active el registro a nivel de componente para cada recurso de la solución de inquilino común que haya creado. Para obtener instrucciones, consulte lo siguiente: • ¿Cómo activo CloudWatch los registros para solucionar problemas con mi API REST o WebSocket API de API Gateway? (Centro de conocimientos de AWS) • Registro mediante CloudWatch registros (guía para desarrolladores de AWS Step Functions) • Registro de funciones de AWS Lambda en Python (Guía para desarrolladores de AWS Lambda) • Registro y supervisión en Amazon Cognito (Guía para desarrolladores de Amazon Cognito) • Supervisión con Amazon CloudWatch (Guía para desarrolladores de Amazon DynamoDB)	Administrador de sistemas de AWS, desarrollador de aplicaciones, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	Note Puede consolidar los registros de cada recurso en una cuenta de registro centraliz ada mediante las políticas de IAM. Para obtener más informaci ón, consulte Registro centralizado y barreras de protección para varias cuentas.	

Aprovisionar e implementar la solución de inquilino común

Tarea	Descripción	Habilidades requeridas
Cree plantillas CloudForm ation .	Automatice la implement ación y el mantenimiento de la solución Common Tenant completa y todos sus componentes mediante el uso de CloudFormation plantillas. Para obtener más informaci ón, consulte la Guía del CloudFormation usuario de AWS.	Desarrollador, DevOps ingeniero y CloudFormation desarrollador de aplicaciones

Recursos relacionados

- Control del acceso a una API de REST con grupos de usuarios de Amazon Cognito como autorizador (Guía para desarrolladores de Amazon API Gateway)
- Uso de autorizadores Lambda de API Gateway (Guía para desarrolladores de Amazon API Gateway)
- Grupos de usuarios de Amazon Cognito (Guía para desarrolladores de Amazon Cognito)
- CloudWatch Consola multicuentas entre regiones (Guía del CloudWatch usuario de Amazon)

Consolidación de la generación de URL prefirmadas y las descargas de objetos de Amazon S3 mediante un punto de conexión asociado a direcciones IP estáticas

Song Jin, Eunhye Jo y Jun Soung Lee, Amazon Web Services

Resumen

Este patrón simplifica el acceso a Amazon Simple Storage Service (Amazon S3) al crear descargas de objetos seguras y URLs prefirmadas personalizadas. La solución proporciona un único punto de conexión con un dominio único y direcciones IP estáticas. Está diseñado para los clientes que requieren la consolidación de la API y los puntos de conexión de Amazon S3 en un dominio unificado con direcciones IP estáticas. El caso de uso implica que los usuarios sigan una política de firewall de listas de direcciones IP y dominios permitidos, lo que limita el acceso de la API a dominios y direcciones IP específicos.

La arquitectura emplea claves Servicios de AWS AWS Global Accelerator, como Amazon API Gateway AWS Lambda, Application Load Balancer y Amazon S3. AWS PrivateLink Este diseño centraliza la API para generar el punto final prefirmado URLs y el punto final de Amazon S3 en un único dominio, vinculado a un acelerador con dos direcciones IP estáticas. En consecuencia, los usuarios pueden solicitar URLs y descargar objetos de Amazon S3 prefirmados sin esfuerzo a través de un punto de enlace de dominio unificado con direcciones IP estáticas.

Esta arquitectura es especialmente beneficiosa para los clientes con políticas o requisitos de conformidad estrictos, como los de los sectores público, médico y financiero.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Una zona alojada pública de su dominio personalizado
- Un dominio importado en AWS Certificate Manager (ACM) Región de AWS de su elección

Limitaciones

- El nombre del bucket de Amazon S3 debe coincidir con el nombre de dominio del punto de conexión. Este requisito es para garantizar que el punto de conexión de Amazon S3 se pueda atender a través del punto de conexión de API único.
- El nombre de dominio personalizado utilizado en API Gateway debe coincidir con el nombre de dominio del único punto de conexión de la API.
- Algunos Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

En el siguiente diagrama se muestran los componentes de la arquitectura de destino y el flujo de trabajo de este patrón.

El diagrama ilustra el siguiente concepto y flujo de trabajo:

1. Un usuario inicia una solicitud para generar una URL prefirmada mediante el punto de enlace personalizado a través del cual se sirve AWS Global Accelerator, utilizando el nombre de dominio personalizado y las direcciones IP asociadas.
2. Una función de Lambda genera la URL prefirmada y apunta al punto de conexión personalizado. Responde con una redirección 301 que contiene la URL prefirmada generada. A través de la URL prefirmada redirigida, el usuario descarga el objeto automáticamente mediante el punto de conexión personalizado ofrecido a través de Global Accelerator.

Los componentes de la arquitectura general para la generación de URL prefirmadas y el flujo de trabajo de descarga de objetos son los siguientes:

- Aprovisionamiento de direcciones IP estáticas por parte de Global Accelerator.
- Registro del alias del acelerador como registro A en la zona alojada pública de Amazon Route 53 con el nombre de dominio personalizado.
- Creación de un bucket de Amazon S3 con un nombre de bucket que coincida con el nombre de dominio personalizado registrado.
- Creación de puntos de enlace de VPC para API Gateway y el servicio Amazon S3.

- Configuración de un equilibrador de carga de aplicación interno para conectarse a Global Accelerator.
- Asignación de un nombre de dominio personalizado para API Gateway con un certificado ACM adjunto.
- Implementación de una API Gateway privada integrada con una función de Lambda.
- La función Lambda está equipada con un rol AWS Identity and Access Management (IAM) adjunto (con GetObjectpermisos).

Tools (Herramientas)

Servicios de AWS

- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket APIs a cualquier escala.
- Los balanceadores de carga de aplicaciones distribuyen el tráfico de aplicaciones entrante entre varios destinos, como las instancias de Amazon Elastic Compute Cloud (Amazon EC2), en varias zonas de disponibilidad.
- AWS Certificate Manager (ACM) le ayuda a crear, almacenar y renovar claves y certificados SSL/TLS X.509 públicos y privados que protegen sus AWS sitios web y aplicaciones.
- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir y aprovisionar la Nube de AWS infraestructura en código.
- AWS Global Accelerator es un servicio global que admite puntos de conexión en varias Regiones de AWS. Puede crear aceleradores que dirijan el tráfico a puntos finales óptimos a través de la red AWS global. De este modo, se mejora la disponibilidad y el rendimiento de las aplicaciones de Internet destinadas al público general.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS PrivateLinkle ayuda a crear conexiones unidireccionales y privadas desde sus nubes privadas virtuales (VPCs) a servicios externos a la VPC.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.

Repositorio de código

Puede implementar este patrón utilizando Terraform AWS CDK o Terraform según sus preferencias. La sección Epics contiene instrucciones para ambos métodos de implementación. El código de este patrón está disponible en los siguientes GitHub repositorios:

- AWS CDK— s3- presignedurl-staticips-endpoint-with -cdk
- Terraforma — s3 - -terraforma presignedurl-staticips-endpoint-with

Prácticas recomendadas

- Para mejorar la seguridad en el entorno de producción, es crucial implementar mecanismos de autorización, como Amazon Cognito, para restringir el acceso a la API de generación `PresignedUrl`.
- Siga el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Prepare el entorno

Tarea	Descripción	Habilidades requeridas
Decida un nombre de dominio.	Elija un nombre de dominio público para el punto de conexión unificado de Amazon S3. El nombre del dominio	Administrador de AWS, administrador de red

Tarea	Descripción	Habilidades requeridas
	también se usa como el nombre del bucket de Amazon S3.	
Creación de una zona alojada pública.	Cree una zona alojada pública en Amazon Route 53. Su nombre de dominio debe coincidir con el nombre de dominio que se usa en API Gateway.	Administrador de AWS, administrador de red
Prepare un certificado SSL.	Utilice AWS Certificate Manager (ACM) para solicitar o importar un certificado SSL para el dominio de su aplicación web.	Administrador de AWS, administrador de red

Implementación del patrón con Terraform

Tarea	Descripción	Habilidades requeridas
Configure el entorno de desarrollo de Terraform.	Para configurar el entorno de desarrollo, haga lo siguiente: 1. Instale Terraform versión 1.0 o posterior. 2. Clone el repositorio GitHub s3- presignedurl-staticips-endpoint-with -terraform ejecutando el siguiente comando en una ventana de terminal: `git clone https://github.com/aws-samp`	Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	`les/s3-presignedurl-staticips-endpoint-with-terraform.git`	

Tarea	Descripción	Habilidades requeridas

Modifique los archivos `.tfvars` y `provider.tf` .	1. Cree los archivos `.tfvars` necesarios: cree archivos `apg.tfvars` en los directorios `1.vpc_alb_ga` y `2.apigw_s3_lambda` . Estos archivos contendrán los valores de las variables específicos de su entorno.
	• Para `1.vpc_alb_ga/apg.tfvars` , cree un archivo con la siguiente plantilla:
	`hcl`
	`environment_name = "test"`
	`domain = "your-domain.com"`
	`s3_bucket_prefix = "your-bucket-prefix"`
	`aws_region = "ap-northeast-2"`
	`# Change to your preferred region`
	• Para `2.apigw_s3_lambda/apg.tfvars` , cree un archivo con la siguiente plantilla (tendrá que actualizar `vpc_id` después de completar el paso 1):
	`hcl`
		Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas

	vpc_id = "vpc-xxxxxxxxx" # Update this with the VPC ID output from step 1
	environment_name = "test"
	domain = "your-domain.com"
	s3_bucket_prefix = "your-bucket-prefix"
	aws_region = "ap-northeast-2" # Change to your preferred region
	2. Modifique los **provider.tf** archivos: tanto en la carpeta como en la 1.vpc_alb_ga 2.apigw_s3_lambda carpeta, edite los provider.tf archivos para que coincidan con su configuración local AWS :
	hcl
	provider "aws" {
	region = "ap-northeast-2" # Change to your preferred region
	profile = "apg" # Change to your AWS profile name
	}
	Tenga en cuenta lo siguiente:	

Tarea	Descripción	Habilidades requeridas
	• Sustituya los valores de marcador de posición de los archivos `.tfvars` por los valores reales. • Tras completar la primera implementación de Terraform (`1.vpc_alb_ga`), actualiza el valor `vpc_iden 2.apigw_s3_lambda/apg.tfvars` con el ID de VPC del resultado. • Asegúrese de que el nombre AWS de su perfil en el `provider.tf` archivo coincida con un perfil existente en `~/.aws/credentials` el archivo. • El valor del dominio debe coincidir con el dominio de la zona alojada de Route 53. • El `s3_bucket_prefix` combinado con el dominio formará el nombre de su bucket de Amazon S3 (por ejemplo, `your-bucket-prefix.your-domain.com`). • Si cambia `aws_region` , es posible que también tenga que actualizar las zonas de disponibilidad codificadas de los	

Tarea	Descripción	Habilidades requeridas
	archivos `main.tf` para que coincidan con las Región de AWS que ha elegido.	

Aprovisione los recursos de red.	Para aprovisionar los recursos de red, ejecute los siguientes comandos:
	`cd ./2.vpc_alb_ga`
	`terraform init`
	`terraform plan --var-file=apg.tfvars`
	`terraform apply --var-file=apg.tfvars`
	Durante la ejecución del comando `apply` , escriba sí cuando se le solicite.
		Administrador de la nube, administrador de AWS

Aprovisione API Gateway, Amazon S3 y Lambda.	Para aprovisionar los recursos de red, use los siguientes comandos:
	`cd ./2.apigw_s3_lambda`
	`terraform init`
	`terraform plan --var-file=apg.tfvars`
	`terraform apply --var-file=apg.tfvars`
		Administrador de la nube, administrador de AWS

Implemente el patrón con AWS CDK

Tarea	Descripción	Habilidades requeridas
Configure el entorno AWS CDK de desarrollo.	Para configurar el entorno de desarrollo, haga lo siguiente:	Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	1. Instale el AWS CDK. 2. Clone el repositorio GitHub s3- presignedurl-staticips-endpoint-with -cdk ejecutando el siguiente comando en una ventana de terminal: `git clone https://github.com/aws-samples/s3-presignedurl-staticips-endpoint-with-cdk.git`	

Tarea	Descripción	Habilidades requeridas
Configure los ajustes del dominio en el archivo `config/index.ts` .	Para editar las opciones de la variable constante, utilice los siguientes comandos: `export const options = { certificateArn: '{arn of the acm which created before}', dnsAttr: { zoneName: '{public hosted zone name}', hostedZoneId: 'hosted zone Id', }, domainNamePrefix: '{Prefix for the domain}', presignPath: 'presign', objectsPath: 'objects', };` En los comandos, reemplace cada marcador de posición con su propia información: • Sustituya `'{arn of the acm which created before}'` por el nombre de recurso de Amazon (ARN) del certificado de ACM. • Sustituya `'{public hosted zone name}'` por su nombre de dominio.	Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	• Sustituya `'hosted zone Id'` por el ID de zona alojada de Route 53. • Sustituya `'{Prefix for the domain}'` por el prefijo de dominio que desee usar. • Si lo desea, modifique las rutas `'presign'` y `'objects'` si es necesario para su caso de uso específico.	

Implemente las pilas.	Para implementar dos pilas, una para la nube privada virtual (VPC) y otra para la aplicación, utilice el siguiente comando:
	`$ npm install`
	`$ cdk synth`
	`$ cdk deploy --all`
		Administrador de la nube, administrador de AWS

Prueba del patrón

Tarea	Descripción	Habilidades requeridas
Verifique las direcciones IP del punto de conexión.	Para comprobar que el dominio de este patrón tenga direcciones IP estáticas, utilice el siguiente comando: `nslookup ${s3-bucket-prefix}.${domain}`	Administrador de red

Tarea	Descripción	Habilidades requeridas
Cargue un archivo de prueba que pueda descargar más adelante.	Cargue el archivo de prueba en la carpeta `'/objects'` del bucket de Amazon S3.	Administrador de la nube, administrador de AWS
Invoque la API para generar una URL prefirmada.	Para generar una URL prefirmada, llame a la URL desde un navegador o un cliente de API (por ejemplo, Postman) con el siguiente formato: `https://${s3-bucket-prefix}.${domain}/presign/objects/${uploaded-filename}` Sustituya los valores de los marcadores de posición `${s3-bucket-prefix}` y `${domain}` por los valores que configuró en los pasos anteriores.	Propietario de la aplicación
Compruebe el resultado.	El resultado esperado es que reciba un código de estado de redireccionamiento 301 (desplazado permanentemente). Esta respuesta contendrá la URL prefirmada, que debería iniciar automáticamente la descarga del archivo de prueba.	Ingeniero de pruebas

Limpieza con Terraform

Tarea	Descripción	Habilidades requeridas

Destruya los recursos de API Gateway, Amazon S3 y Lambda.	Para eliminar los recursos, use los siguientes comandos:
	`cd ./2.apigw_s3_lambda`
	`terraform init`
	`terraform plan --destroy --var-file=apg.tfvars`
	`terraform destroy --var-file=apg.tfvars`
		Administrador de la nube, administrador de AWS

Destruya los recursos de red.	Para eliminar los recursos de red, use los siguientes comandos:
	`cd ./1.vpc_alb_ga`
	`terraform init`
	`terraform plan --destroy --var-file=apg.tfvars`
	`terraform destroy --var-file=apg.tfvars`
		Administrador de la nube, administrador de AWS

Limpie con AWS CDK

Tarea	Descripción	Habilidades requeridas
Destruya las pilas.	Para destruir las pilas de VPC y de aplicaciones, utilice el siguiente comando: `$ cdk destroy --all`	Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas

Vacíe y elimine los buckets de Amazon S3.	Vacíe y elimine el bucket de Amazon S3 del objeto y el bucket de Amazon S3 de los registros que no se eliminen de forma predeterminada.
	
	Los nombres de los buckets de Amazon S3 son `${s3-bucket-prefix}.${domain}` y `${s3-bucket-prefix}.${domain}-logs`.
	
	Si prefiere usar AWS Command Line Interface (AWS CLI) para eliminar los buckets, utilice los siguientes comandos:
	
	`$ aws s3 rm s3://${s3-bucket-prefix}.${domain} --recursive`
	`$ aws s3 rb s3://${s3-bucket-prefix}.${domain} --force`
	`$ aws s3 rm s3://${s3-bucket-prefix}.${domain}-logs --recursive`
	`$ aws s3 rb s3://${s3-bucket-prefix}.${domain}-logs --force`
	
	Sustituya `${s3-bucket-prefix}` y `${domain}` por los valores que se estableció en los pasos anteriores.
		Administrador de la nube, administrador de AWS

Recursos relacionados

AWS Blogs

- Acceso a una Amazon API Gateway mediante direcciones IP estáticas proporcionadas por AWS Global Accelerator
- Genere una URL prefirmada de forma modular AWS CDK para JavaScript
- Alojamiento de sitios web estáticos HTTPS internos con ALB, S3 y PrivateLink

Crear una EventBridge conexión entre cuentas de Amazon en una organización

Sam Wilson y Robert Stone, Amazon Web Services

Resumen

Los grandes sistemas distribuidos utilizan Amazon EventBridge para comunicar los cambios de estado entre varias cuentas de Amazon Web Services (AWS) de una AWS Organizations organización. Sin embargo, por EventBridge lo general solo puede dirigirse a los puntos finales o a los consumidores de la misma Cuenta de AWS. La excepción es un bus de eventos en una cuenta diferente. Ese bus de eventos es un destino válido. Para consumir eventos de un bus de eventos de otra cuenta, los eventos deben transferirse del bus de eventos de la cuenta de origen al bus de eventos de la cuenta de destino. Para evitar problemas a la hora de gestionar eventos críticos en distintas aplicaciones Cuentas de AWS, utilice el enfoque recomendado que se presenta en este patrón.

Este patrón ilustra cómo implementar una arquitectura basada en eventos EventBridge que involucre a varios miembros de una Cuentas de AWS AWS Organizations organización. El patrón usa AWS Cloud Development Kit (AWS CDK) Toolkit y. AWS CloudFormation

EventBridge ofrece un bus de eventos sin servidor que le ayuda a recibir, filtrar, transformar, enrutar y entregar eventos. Un componente fundamental de las arquitecturas basadas en eventos, EventBridge permite separar entre los productores de mensajes y los consumidores de esos mensajes. En una sola cuenta, esto es sencillo. Una estructura entre cuentas requiere consideraciones adicionales para que los eventos del bus de eventos de una cuenta se consuman en otras cuentas de la misma organización.

Para obtener información sobre las consideraciones específicas de las cuentas para productores y consumidores, consulte la sección de información adicional.

Requisitos previos y limitaciones

Requisitos previos

- Una AWS Organizations organización con al menos dos asociados Cuentas de AWS
- Una función AWS Identity and Access Management (IAM) en ambas Cuentas de AWS que le permita aprovisionar la infraestructura en ambas Cuentas de AWS mediante AWS CloudFormation

- Git instalado localmente
- AWS Command Line Interface (AWS CLI) instalado localmente
- AWS CDK instalado localmente y arrancado en ambos Cuentas de AWS

Versiones de producto

Este patrón se ha creado y probado usando las siguientes herramientas y versiones:

- AWS CDK Kit de herramientas 2.126.0
- Node.js 18.19.0
- npm 10.2.3
- Python 3.12

Este patrón debería funcionar con cualquier versión de AWS CDK v2 o npm. Las versiones 13.0.0 a 13.6.0 de Node.js no son compatibles con AWS CDK.

Arquitectura

Arquitectura de destino

El siguiente diagrama muestra el flujo de trabajo de arquitectura para enviar un evento desde una cuenta y consumirlo en otra cuenta.

El flujo de trabajo consta de los pasos siguientes:

1. La AWS Lambda función Producer de la cuenta Source coloca un evento en el bus de EventBridge eventos de la cuenta.
2. La EventBridge regla de cuentas cruzadas dirige el evento a un bus de EventBridge eventos de la cuenta de destino.
3. El bus de EventBridge eventos de la cuenta de destino tiene una regla Lambda de destino que invoca la función Consumer Lambda.

Una práctica recomendada es utilizar una cola de mensajes fallidos (DLQ) para gestionar las invocaciones fallidas de la función de Lambda de consumidor. Sin embargo, el DLQ se omitió en esta solución para mayor claridad. Para obtener más información sobre cómo implementar una DLQ en

sus flujos de trabajo y mejorar la capacidad de los flujos de trabajo para recuperarse de los errores, consulte la entrada del blog Implementación AWS Lambda de patrones de manejo de errores.

Automatización y escala

AWS CDK aprovisiona automáticamente la arquitectura requerida. EventBridge puede ampliarse a miles de registros por segundo, según el Región de AWS. Para obtener más información, consulta la documentación de EventBridge cuotas de Amazon.

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir y aprovisionar la Nube de AWS infraestructura en el código. Este patrón utiliza el kit de AWS CDK herramientas, un kit de desarrollo en la nube de línea de comandos que te ayuda a interactuar con tu AWS CDK aplicación.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, AWS Lambda funciones, puntos finales de invocación HTTP que utilizan destinos de API o buses de eventos en otros. Cuentas de AWS
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar múltiples cuentas Cuentas de AWS en una organización que puede crear y administrar de forma centralizada.

Otras herramientas

- Node.js es un entorno de JavaScript ejecución basado en eventos diseñado para crear aplicaciones de red escalables.
- npm es un registro de software que se ejecuta en un entorno Node.js y se utiliza para compartir o tomar prestados paquetes y administrar la implementación de paquetes privados.
- Python es un lenguaje de programación informático de uso general.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub cross-account-eventbridge-in-organization.

Prácticas recomendadas

Para conocer las mejores prácticas a la hora de trabajar con EventBridge él, consulta los siguientes recursos:

- Mejores prácticas para los patrones de EventBridge eventos de Amazon
- Mejores prácticas a la hora de definir reglas en Amazon EventBridge

Epics

Prepare su entorno AWS CDK de despliegue local

Tarea	Descripción	Habilidades requeridas
Configure las credenciales locales para la cuenta de origen y la cuenta de destino.	Revise la configuración y las credenciales nuevas y utilice el método de autenticación y credenciales que mejor se adapte a su entorno. ⚠ Important Asegúrese de configurar la autenticación tanto AWS CLI para la cuenta de origen como para la cuenta de destino. Estas instrucciones suponen que ha configurado dos perfiles de AWS de manera	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	local: `sourceAccount` y `destinationAccount` .	

Bootstrap para ambos Cuentas de AWS.	Para arrancar las cuentas, ejecute los siguientes comandos:
	`cdk bootstrap --profile sourceAccount`
	`cdk bootstrap --profile destinationAccount`
		Desarrollador de aplicaciones

Clone el código de patrón.	Para clonar el repositorio, ejecute el siguiente comando:
	`git clone git@github.com:aws-samples/aws-cdk-examples.git`
	A continuación, cambie el directorio a la carpeta del proyecto recién clonada:
	`cd aws-cdk-examples/python/cross-account-eventbridge-in-organization`
		Desarrollador de aplicaciones

Implemente ProducerStack en la cuenta Source

Tarea	Descripción	Habilidades requeridas
Modifique `cdk.json` con sus detalles AWS Organizations y los de su cuenta.	En la carpeta raíz del proyecto, realiza los siguientes cambios en `cdk.json`:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	• `organization_id` : el ID de Organizations de las cuentas implicadas en su implementación • `event_bus_name` : `CrossAccount` , o puede cambiar el nombre. • `rules[].targets[].arn` – El Cuenta de AWS ID de la cuenta consumidora (cuenta de destino)	
Despliegue los ProducerStack recursos.	Desde el directorio raíz del proyecto, ejecute el siguiente comando: `cdk deploy ProducerStack --profile sourceAccount` Cuando se le solicite, acepte las nuevas funciones de IAM y otros permisos relacionados con la seguridad que se hayan creado mediante ellas. AWS CloudFormation	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Compruebe que los ProducerStack recursos estén desplegados.	Para verificar los recursos, haga lo siguiente: 1. En Consola de administración de AWS Para la cuenta de origen, elija CloudFormation. 2. En la lista de pilas, selecciona ProducerStack. 3. En la pestaña Información de pila, compruebe que el estado de la pila es `CREATE_COMPLETE` . Si lo desea, en la pestaña Recursos, revise los recursos configurados.	Desarrollador de aplicaciones

Implemente ConsumerStack en la cuenta de destino

Tarea	Descripción	Habilidades requeridas
Despliegue los ConsumerStack recursos.	Desde el directorio raíz del proyecto, ejecute el siguiente comando: `cdk deploy ConsumerStack --profile destinationAccount` Cuando se le solicite, acepte las nuevas funciones de IAM y otros permisos relacionados con la seguridad que se	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	hayan creado mediante ellas. CloudFormation	
Compruebe que los recursos estén desplegados ConsumerStack	1. En la consola de la cuenta de destino, elija CloudFormation. 2. En la lista de pilas, selecciona ConsumerStack. 3. En la pestaña Información de pila, compruebe que el estado de la pila es `CREATE_COMPLETE` . Si lo desea, en la pestaña Recursos, revise los recursos configurados.	Desarrollador de aplicaciones

Producción y consumo de eventos

Tarea	Descripción	Habilidades requeridas
Invoque la función de Lambda de producción.	1. En la consola de la cuenta de origen, elija Lambda. 2. En la lista de funciones , elija ProducerStack-ProducerLambda XXXX (XXXX representa una secuencia de caracteres generada automáticamente por AWS CDK). 3. Elija la pestaña Prueba. 4. En el panel Evento de prueba, seleccione Prueba.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	El contenido del área de texto JSON del evento puede ser cualquier JSON válido que se proporcione a la función de Lambda como carga útil. En este caso, basta con el JSON proporcionado de manera predeterminada. 5. Compruebe que el mensaje Función de ejecución: correcta aparece en un banner verde sobre la sección Evento de prueba.	

Tarea	Descripción	Habilidades requeridas
Verifique que se haya recibido el evento.	1. En la consola de la cuenta de destino, elija Lambda. 2. En la lista de funciones, elija ConsumerStack-ConsumerLambda XXXX (XXXX representa una secuencia de caracteres generada automáticamente por AWS CDK). 3. Elija la pestaña Supervisar. 4. En la sección Supervisar, elija Ver registros. CloudWatch 5. En la pestaña recién abierta, elija el nombre de flujo de registro del flujo de registro más reciente. 6. Compruebe que aparezca una sentencia de registro como la siguiente: `[DEBUG] 2024-04-08T19:08:10.091Z 9c16844a-f9de-444d-b621-86afe64d4cc8 Event: {'version':'0', 'id':'0b9faa96-973f-8be2-ecf8-75e4f328b980', 'detail-type':'TestType', 'source':'Producer', 'account' :'XXXXXXXXXXXX',`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`'time':'2024-04-08T19:08:09Z', 'region':'us-east-1', 'resources': [], 'detail': {'key1':'value1', 'key2':'value2', 'key3':'value3'}}`	

Limpieza

Tarea	Descripción	Habilidades requeridas
Destruye los ConsumerStack recursos.	Si utiliza este patrón como prueba, limpie los recursos implementados para evitar incurrir en costos adicionales. Desde el directorio raíz del proyecto, ejecute el siguiente comando: `cdk destroy ConsumerStack --profile destinationAccount` Se le pedirá que confirme la eliminación de la pila.	Desarrollador de aplicaciones
Destruye los ProducerStack recursos.	Desde el directorio raíz del proyecto, ejecute el siguiente comando:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`cdk destroy ProducerStack --profile sourceAccount` Se le pedirá que confirme la eliminación de la pila.	

Resolución de problemas

Problema	Solución
No se recibió ningún evento en la cuenta de destino.	1. Verifique que el ID de Organizations proporcionado sea correcto. 2. Compruebe que la cuenta de origen forme parte de la organización proporcionada. 3. Compruebe que las reglas del bus de eventos de la cuenta de origen se correspondan con la información correcta de la cuenta de destino.
Al invocar una función de Lambda desde la consola, se obtiene el siguiente error: `User: arn:aws:iam::123456789012:user/XXXXX is not authorized to perform: lambda:Invoke`	Póngase en contacto con su Cuenta de AWS administrador para recibir los permisos de `lambda:Invoke` acción adecuados en la `ProducerStack-ProducerLambdaXXXX` función Lambda.

Recursos relacionados

Referencias

- AWS Organizations Guía del usuario
- Patrones de EventBridge eventos de Amazon
- Reglas en Amazon EventBridge

Tutoriales y videos

- Tutorial: Creación y configuración de una organización
- AWS re:Invent 2023: patrones avanzados basados en eventos con Amazon (01-R) EventBridge COM3

Información adicional

Regla del productor

En la cuenta Source, se crea un bus de EventBridge eventos para aceptar los mensajes de los productores (como se muestra en la sección Arquitectura). En este bus de eventos se crea una regla con los correspondientes permisos de IAM. Las reglas se dirigen al bus de EventBridge eventos de la cuenta de destino y se basan en la siguiente `cdk.json` estructura:

```
"rules": [
  {
    "id": "CrossAccount",
    "sources": ["Producer"],
    "detail_types": ["TestType"],
    "targets": [
      {
        "id": "ConsumerEventBus",
        "arn": "arn:aws:events:us-east-2:012345678901:event-bus/CrossAccount"
      }
    ]
  }
]
```

Para cada bus de eventos que consume, se deben incluir el patrón de eventos y el bus de eventos de destino.

Patrón de eventos

Los patrones de eventos filtran a qué eventos se aplicará esta regla. Para los fines de este ejemplo, los orígenes de eventos y el registro `detail_types` identifican qué eventos se van a transmitir desde el bus de eventos de la cuenta de origen al bus de eventos de la cuenta de destino.

Bus de eventos de destino

Esta regla se dirige a un bus de eventos que existe en otra cuenta. El `arn` (nombre del recurso de Amazon) completo es necesario para identificar de forma única el bus de eventos de destino y `id` es el ID lógico utilizado por AWS CloudFormation. No es necesario que el bus de eventos de destino exista realmente en el momento de la creación de la regla de destino.

Consideraciones específicas de la cuenta de destino

En la cuenta de destino, se crea un bus de EventBridge eventos para recibir mensajes del bus de eventos de la cuenta de origen. Para permitir que los eventos se publiquen desde la cuenta de origen, debe crear una política basada en recursos:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowOrgToPutEvents",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "events:PutEvents",
    "Resource": "arn:aws:events:us-east-2:012345678901:event-bus/CrossAccount",
    "Condition": {
      "StringEquals": {
        "aws:PrincipalOrgID": "o-XXXXXXXXX"
      }
    }
  }]
}
```

Es especialmente importante conceder el permiso `events:PutEvents`, que permite a cualquier otra cuenta de la misma organización publicar eventos en este bus de eventos. Si `aws:PrincipalOrgId` se establece como ID de la organización, se conceden los permisos necesarios.

Patrón del evento

Puede modificar el patrón de eventos incluido para adaptarlo a su caso de uso:

```
rule = events.Rule(
    self,
    self.id + 'Rule' + rule_definition['id'],
    event_bus=event_bus,
    event_pattern=events.EventPattern(
        source=rule_definition['sources'],
```

```
        detail_type=rule_definition['detail_types'],
    )
)
```

Para reducir el procesamiento innecesario, el patrón de eventos debe especificar que solo los eventos que procese la cuenta de destino se transmitan al bus de eventos de la cuenta de destino.

Política basada en recursos

En este ejemplo, se utiliza el ID de la organización para controlar qué cuentas pueden incluir eventos en el bus de eventos de la cuenta de destino. Considere la posibilidad de utilizar una política más restrictiva, como especificar la cuenta de origen.

EventBridge cuotas

Tenga en cuenta las siguientes cuotas:

- La cuota predeterminada es de 300 reglas por bus de eventos. Se puede ampliar si es necesario, pero debería adaptarse a la mayoría de los casos de uso.
- El máximo permitido es de cinco destinos por regla. Recomendamos que los arquitectos de aplicaciones utilicen una regla distinta para cada cuenta de destino a fin de poder controlar de forma pormenorizada el patrón de eventos.

Entregue registros de DynamoDB a Amazon S3 mediante Kinesis Data Streams y Firehose con AWS CDK

Shashank Shrivastava y Daniel Matuki da Cunha, Amazon Web Services

Resumen

Este patrón proporciona un código de muestra y una aplicación para entregar registros de Amazon DynamoDB a Amazon Simple Storage Service (Amazon S3) mediante Amazon Kinesis Data Streams y Amazon Data Firehose. El enfoque del patrón utiliza construcciones de AWS Cloud Development Kit (AWS CDK) nivel 3 e incluye un ejemplo de cómo realizar la transformación de datos AWS Lambda antes de que los datos se entreguen al depósito S3 de destino en la nube de Amazon Web Services (AWS).

Kinesis Data Streams captura modificaciones a nivel de elemento en cualquier tabla de DynamoDB y las replica en una secuencia de datos de Kinesis. Sus aplicaciones pueden acceder al flujo de datos de Kinesis y ver los cambios a nivel de elemento casi en tiempo real. Kinesis Data Streams también le brinda acceso a otros servicios d Amazon Kinesis, como Firehose y Amazon Managed Service para Apache Flink. Puede crear aplicaciones que proporcionen paneles en tiempo real, generen alertas, apliquen precios y publicidad dinámicos y realicen análisis de datos sofisticados.

Puede usar este patrón para sus casos de uso de integración de datos. Por ejemplo, los vehículos de transporte o equipos industriales pueden enviar grandes volúmenes de datos a una tabla de DynamoDB. Estos datos se pueden transformar y almacenar en un lago de datos alojado en Amazon S3. A continuación, puede consultar y procesar los datos, así como predecir cualquier posible defecto, mediante servicios sin servidor como Amazon Athena, Amazon Redshift Spectrum, Amazon Rekognition y AWS Glue.

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- AWS Command Line Interface (AWS CLI), instalado y configurado. Para obtener más información, consulte Primeros pasos con AWS CLIél en la AWS CLI documentación.
- Node.js (18.x+) y npm, instalados y configurados. Para obtener más información, consulte Descargar e instalar Node.js y npm en la documentación de `npm`.

- aws-cdk (2.x+), instalado y configurado. Para obtener más información, consulte Introducción a él AWS CDK en la documentación. AWS CDK
- El repositorio GitHub aws-dynamodb-kinesisfirehose-sde 3 ingestas, clonado y configurado en su máquina local.
- Datos de ejemplo existentes para la tabla de DynamoDB. Los datos deben utilizar el siguiente formato: `{"SourceDataId": {"S": "123"},"MessageData":{"S": "Hello World"}}`

Arquitectura

En el siguiente diagrama se muestra un ejemplo de flujo de trabajo que entrega registros de DynamoDB en Amazon S3 mediante Kinesis Data Streams y Firehose.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Los datos se incorporan mediante Amazon API Gateway como proxy de DynamoDB. También puede usar cualquier otro origen para incorporar datos en DynamoDB.
2. Los cambios a nivel de elemento se generan prácticamente en tiempo real en Kinesis Data Streams para su entrega a Amazon S3.
3. Kinesis Data Streams envía los registros a Firehose para su transformación y entrega.
4. Una función de Lambda convierte los registros de un formato de registro de DynamoDB a un formato JSON, que contiene solo los nombres y valores de los atributos de los elementos del registro.

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que lo ayuda a definir y aprovisionar la infraestructura en la nube de AWS en código.
- AWS CDK El kit de herramientas es un kit de desarrollo en la nube de línea de comandos que le ayuda a interactuar con su aplicación. AWS CDK
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que te ayuda a interactuar Servicios de AWS mediante los comandos de tu shell de línea de comandos.

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todo el territorio y. Cuentas de AWS Regiones de AWS

Repositorio de código

El código de este patrón está disponible en el repositorio de GitHub aws-dynamodb-kinesisfirehose-s3 ingestas.

Epics

Instale y configure el código de muestra

Tarea	Descripción	Habilidades requeridas

Instale las dependencias.	En su máquina local, instale las dependencias de los archivos `package.json` en los directorios `pattern/aws-dynamodb-kinesisstreams-s3` y `sample-application` ejecutando los siguientes comandos:
	`cd <project_root>/pattern/aws-dynamodb-kinesisstreams-s3`
	`npm install && npm run build`
	`cd <project_root>/sample-application/`
	`npm install && npm run build`
		Desarrollador de aplicaciones, AWS general

Tarea	Descripción	Habilidades requeridas
Genere la plantilla CloudFormation .	1. Ejecute el comando `cd <project_root>/sample-application/ .` 2. Ejecute el `cdk synth` comando para generar la CloudFormation plantilla. 3. Los resultados `AwsDynamodbKinesisfirehoseS3IngestionStack.template.json` quedan almacenados en el directorio `cdk.out`. 4. Utilice AWS CDK o Consola de administración de AWS para procesar la plantilla CloudFormation.	Desarrollador de aplicaciones, AWS general, AWS DevOps

Implementación de recursos

Tarea	Descripción	Habilidades requeridas
Compruebe e implemente los recursos.	1. Ejecute el `cdk diff` comando para identificar los tipos de recursos que crea la AWS CDK construcción. 2. Ejecute el comando `cdk deploy` para implementar los recursos.	Desarrollador de aplicaciones, AWS general, AWS DevOps

Incorpore datos a la tabla de DynamoDB para probar la solución

Tarea	Descripción	Habilidades requeridas

Incorpore sus datos de muestra en la tabla de DynamoDB.	Envíe una solicitud a la tabla de DynamoDB ejecutando el siguiente comando en: AWS CLI
	
	`aws dynamodb put-item --table-name <your_table_name> --item '{"<table_partition_key>": {"S": "<partition_key_ID>"},"MessageData":{"S": "<data>"}}'`
	
	ejemplo:
	
	`aws dynamodb put-item --table-name SourceData_table --item '{"SourceDataId": {"S": "123"},"MessageData":{"S": "Hello World"}}'`
	
	De forma predeterminada, `put-item` no devuelve ningún valor como resultado si la operación se realiza correctamente. Si la operación falla, devuelve un error. Los datos se almacenan en DynamoDB y, a continuac
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	ión, se envían a Kinesis Data Streams y Firehose. **Note** Puede adoptar diferentes enfoques para añadir datos a una tabla de DynamoDB. Para obtener más informaci ón, consulte la sección Cargar datos en tablas en la documentación de DynamoDB.	
Verifique que se crea un objeto nuevo en el bucket de S3.	Inicie sesión en el bucket de S3 Consola de administración de AWS y supervise el mismo para comprobar que se ha creado un objeto nuevo con los datos que ha enviado. Para obtener más informaci ón, consulte GetObjectla documentación de Amazon S3.	Desarrollador de aplicaciones, AWS general

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Limpiar recursos.	Ejecute el comando `cdk destroy` para eliminar todos	Desarrollador de aplicaciones, AWS general

Tarea	Descripción	Habilidades requeridas
	los recursos usados por este patrón.	

Recursos relacionados

- s3- static-site-stack .ts (GitHub repositorio)
- aws-apigateway-dynamodb módulo (GitHub repositorio)
- aws-kinesisstreams-kinesisfirehose-sMódulo 3 (GitHub repositorio)
- Captura de datos de cambios para DynamoDB Streams (documentación de DynamoDB)
- Uso de Kinesis Data Streams para capturar cambios en DynamoDB (documentación de DynamoDB)

Implementación del control de versiones de API basado en rutas mediante dominios personalizados en Amazon API Gateway

Corey Schnedl, Marcelo Barbosa, Mario Lopez Martinez, Anbazhagan Ponnuswamy, Gaurav Samudra y Abhilash Vinod, Amazon Web Services

Resumen

Este patrón demuestra cómo puede utilizar la característica de asignación de API de dominios personalizados para implementar una solución de control de versiones de API basado en rutas para Amazon API Gateway.

Amazon API Gateway es un servicio totalmente gestionado que puede utilizar para crear, publicar, mantener, supervisar y proteger APIs a cualquier escala. Al utilizar la función de dominio personalizado del servicio, puede crear nombres de dominio personalizados que sean más sencillos e intuitivos y URLs que pueda proporcionarlos a los usuarios de su API. Puede utilizar las asignaciones de API para conectar etapas de la API a un nombre de dominio personalizado. Después de crear un nombre de dominio y configurar los registros de DNS, utiliza las asignaciones de API para enviarle tráfico a APIs través de su nombre de dominio personalizado.

Cuando una API pasa a estar disponible públicamente, los consumidores la utilizan. A medida que evoluciona una API pública, su contrato de servicio también evoluciona para reflejar las nuevas características y funcionalidades. Sin embargo, no es aconsejable cambiar ni eliminar las características existentes. Cualquier cambio importante podría afectar a las aplicaciones del consumidor y provocar fallos durante el tiempo de ejecución. El control de versiones de las API es importante para evitar interrumpir la compatibilidad con versiones anteriores e infringir un contrato.

Se necesita una estrategia clara de control de versiones de las API para ayudar a los consumidores a adoptarlas. El control de versiones APIs mediante rutas URLs es el enfoque más sencillo y utilizado con más frecuencia. En este tipo de control de versiones, las versiones se definen explícitamente como parte de la API. URIs El siguiente ejemplo URLs muestra cómo un consumidor puede usar el URI para especificar una versión de API para su solicitud:

```
https://api.example.com/api/v1/orders

https://api.example.com/api/v2/orders

https://api.example.com/api/vX/orders
```

Este patrón lo utiliza AWS Cloud Development Kit (AWS CDK) para crear, implementar y probar un ejemplo de implementación de una solución de control de versiones escalable basada en rutas para su API. AWS CDK es un marco de desarrollo de software de código abierto para modelar y aprovisionar los recursos de sus aplicaciones en la nube mediante lenguajes de programación conocidos.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.
- Se requiere la propiedad de un dominio para usar el repositorio de muestras de este patrón y para usar la funcionalidad de dominios personalizados de Amazon API Gateway. Puede usar Amazon Route 53 para crear y administrar los dominios de su organización. Para obtener información sobre cómo registrar o transferir un dominio con Route 53, consulte Registering new domains en la documentación de Route 53.
- Antes de configurar un nombre de dominio personalizado para una API, debe disponer de un certificado SSL/TLS listo en AWS Certificate Manager.
- Debe crear o actualizar el registro de recursos del proveedor de DNS para asignarlo al punto de conexión de la API. Si no se lleva a cabo esta asignación, las solicitudes de API vinculadas al nombre de dominio personalizado no pueden llegar a API Gateway.

Limitaciones

- Un nombre de dominio personalizado debe ser único dentro de un Región de AWS todo Cuentas de AWS.
- Para configurar asignaciones de la API con varios niveles, debe usar un nombre de dominio personalizado regional y usar la política de seguridad de TLS 1.2.
- En una asignación de API, el nombre de dominio personalizado y el mapeado APIs deben coincidir Cuenta de AWS.
- Las asignaciones de API deben contener solo letras, números y los siguientes caracteres: `$-_.+!*'()/`
- La longitud máxima de la ruta en una asignación de API es de 300 caracteres.
- Puede tener 200 asignaciones de API con varios niveles para cada nombre de dominio.
- Solo puede asignar HTTP APIs a un nombre de dominio personalizado regional con la política de seguridad TLS 1.2.

- No puedes asignarlo WebSocket APIs al mismo nombre de dominio personalizado que una API HTTP o una API REST.
- Algunas Servicios de AWS no están disponibles en todas Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- Este ejemplo de implementación se usa AWS CDK en la TypeScript versión 2.149.0.

Arquitectura

En el siguiente diagrama se muestra el flujo de trabajo de la arquitectura.

En el siguiente diagrama se ilustra lo siguiente:

1. El usuario de la API envía una solicitud a Amazon API Gateway con un nombre de dominio personalizado.
2. API Gateway dirige dinámicamente la solicitud del usuario a una instancia y etapa adecuadas de API Gateway, según la ruta indicada en la URL de la solicitud. En la siguiente tabla se muestra un ejemplo de cómo se pueden enrutar las distintas rutas basadas en URL a etapas específicas para distintas instancias de API Gateway.

API	Etapa	Ruta	Punto de conexión predeterminado
Cálculo APIv1	api	apiv1	Habilitado
Cálculo APIv2	api	apiv2	Habilitado
Cálculo APIv X	api	apivX	Habilitado

3. La instancia de API Gateway de destino procesa la solicitud y devuelve el resultado al usuario.

Automatización y escala

Te recomendamos que utilices AWS CloudFormation pilas independientes para cada versión de la API. Con este enfoque, puedes tener un aislamiento total entre el backend al APIs que se puede enrutar mediante la función de mapeo de API de dominio personalizado. Una ventaja de este enfoque es que se pueden implementar o eliminar diferentes versiones de la API de forma independiente sin que ello suponga el riesgo de modificar otra API. Este enfoque aumenta la resiliencia mediante el aislamiento de las CloudFormation pilas. Además, le proporciona diferentes opciones de back-end para su API AWS Lambda AWS Fargate, como los puntos finales HTTP y las acciones de. Servicios de AWS

Puedes usar estrategias de ramificación de Git, como Gitflow, en combinación con CloudFormation pilas aisladas para administrar el código fuente que se implementa en las diferentes versiones de la API. Al usar esta opción, puede mantener diferentes versiones de su API sin necesidad de duplicar el código fuente para las nuevas versiones. Con Gitflow, puede agregar etiquetas a las confirmaciones dentro de su repositorio de Git a medida que se vayan llevando a cabo los lanzamientos. Como resultado, tiene una instantánea completa del código fuente en relación con un lanzamiento específico. Como es necesario realizar actualizaciones, puedes consultar el código de una versión específica, realizar actualizaciones y, después, implementar el código fuente actualizado en la CloudFormation pila que se ajuste a la versión principal correspondiente. Este enfoque reduce el riesgo de interrumpir otra versión de la API, ya que cada versión de la API tiene un código fuente aislado y se implementa en CloudFormation pilas independientes.

Tools (Herramientas)

Servicios de AWS

- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket APIs a cualquier escala.
- AWS Certificate Manager (ACM) le ayuda a crear, almacenar y renovar claves y certificados SSL/TLS X.509 públicos y privados que protegen sus AWS sitios web y aplicaciones.
- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software de código abierto para definir su infraestructura de nube en código y aprovisionarla mediante ella. CloudFormationEl ejemplo de implementación de este patrón utiliza el AWS CDK in. TypeScript Para trabajar con AWS CDK in se TypeScript utilizan herramientas conocidas, como el TypeScript compilador de Microsoft (`tsc`), Node.js y el administrador de paquetes de nodos (`npm`). Si lo prefiere, puede usar Yarn, aunque en los ejemplos de este patrón se utiliza `npm`. Los módulos que componen la Biblioteca de constructos de AWS se distribuyen a través del repositorio `npm` , npmjs.org.

- CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y administrarlos a lo largo de su ciclo de vida en todo el mundo Cuentas de AWS . Regiones de AWS
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.
- AWS WAF es un firewall de aplicación web que lo ayuda a supervisar las solicitudes HTTP y HTTPS que se reenvían a los recursos de su aplicación web protegida.

Otras herramientas

- Bruno es un cliente de pruebas de API de código abierto y compatible con Git.
- cdk-nag es una utilidad de código abierto que comprueba AWS CDK las mejores prácticas en las aplicaciones mediante paquetes de reglas.

Repositorio de código

El código de este patrón está disponible en el repositorio -api-gateway. GitHub path-based-versioning-with

Prácticas recomendadas

- Utilice una sólida canalización de integración y entrega continuas (CI/CD) para automatizar las pruebas y el despliegue de las CloudFormation pilas creadas con. AWS CDK Para obtener más información relacionada con esta recomendación, consulte la Guía de AWS DevOps Well-Architected.
- AWS WAF es un firewall gestionado que se integra fácilmente con servicios como Amazon API Gateway. Si bien AWS WAF no es un componente necesario para que este patrón de control de versiones funcione, recomendamos incluirlo en API Gateway como práctica recomendada AWS WAF de seguridad.
- Anime a los consumidores de la API a que actualicen periódicamente a la versión más reciente de su API para que las versiones anteriores queden obsoletas y se eliminen de forma eficiente.

- Antes de utilizar este enfoque en un entorno de producción, implemente una estrategia de firewall y autorización para su API.
- Implemente el acceso a la administración de sus AWS recursos Cuenta de AWS mediante el modelo de acceso con privilegios mínimos.
- Para aplicar las mejores prácticas y las recomendaciones de seguridad para las aplicaciones creadas con él AWS CDK, le recomendamos que utilice la utilidad cdk-nag.

Epics

Preparación del entorno local

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Para clonar el repositorio de la aplicación de ejemplo, ejecute el siguiente ejemplo: `git clone https://github.com/aws-samples/path-based-versioning-with-api-gateway`	Desarrollador de aplicaciones
Navegue hasta el repositorio clonado.	Para ir a la ubicación de la carpeta del repositorio clonado, ejecute el siguiente comando: `cd api-gateway-custom-domain-versioning`	Desarrollador de aplicaciones
Instale las dependencias requeridas.	Para instalar las dependencias necesarias, ejecute el siguiente comando: `npm install`	Desarrollador de aplicaciones

Implemente la pila de enrutamiento CloudFormation

Tarea	Descripción	Habilidades requeridas
Iniciar la implementación de la pila de enrutamiento.	Para iniciar la implementación de la pila de CloudFormation enrutamiento`CustomDomainRouterStack`, ejecute el siguiente comando y `example.com` sustitúyalo por el nombre del dominio del que es propietario: `npx cdk deploy CustomDomainRouterStack --parameters PrerequisiteDomainName=example.com` **Note** La implementación de la pila no se llevará a cabo correctamente hasta que la siguiente tarea de validación del DNS del dominio se efectúe correctamente.	Desarrollador de aplicaciones

Verificar la propiedad del dominio

Tarea	Descripción	Habilidades requeridas
Verificar la propiedad de su dominio.	El certificado permanecerá en estado Pendiente de validación hasta que demuestre la propiedad del dominio asociado. Para demostrar la propiedad, agregue registros CNAME a la zona alojada asociada al dominio. Para obtener más información, consulte la validación de DNS en la AWS Certificate Manager documentación. Agregar los registros adecuados permite que la implementación de `CustomDomainRouterStack` se lleve a cabo correctamente.	Desarrollador de aplicaciones, administrador de sistemas de AWS, administrador de redes
Crear un registro de alias que apunte a su dominio personalizado de API Gateway.	Una vez que el certificado se haya emitido y validado correctamente, cree un registro de DNS que apunte a la URL del dominio personalizado de Amazon API Gateway. La URL del dominio personalizado se genera exclusivamente mediante el aprovisionamiento del dominio	Desarrollador de aplicaciones, administrador de sistemas de AWS, administrador de redes

Tarea	Descripción	Habilidades requeridas
	personalizado y se especific a como parámetro de CloudFormation salida. A continuación, se muestra un ejemplo del registro: Política de enrutamiento: enrutamiento sencillo Nombre del registro: `demo.api-gateway-custom-domain-versioning.example.com` Alias: sí Tipo de registro: registro DNS de tipo «A» que apunta a un AWS recurso Valor: `d-xxxxxxxxxx.execute-api.xx-xxxx-x.amazonaws.com` TTL (segundos): 300	

Implemente CloudFormation pilas e invoque la API

Tarea	Descripción	Habilidades requeridas
Implemente la pila de `ApiStackV1` .	Para implementar la pila de `ApiStackV1` , use el siguiente comando: `npm run deploy-v1`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	El siguiente código de CDK agrega la asignación de API: `var apiMapping = new CfnApiMapping(this, "ApiMapping", { apiId: this.lambdaRestApi.restApiId, domainName: props.customDomainName.domainName, stage: "api", apiMappingKey: "api/v1", });`	
Implemente la pila de `ApiStackV2` .	Para implementar la pila de `ApiStackV2` , use el siguiente comando: `npm run deploy-v2`	Desarrollador de aplicaciones
Invoque la API .	Para invocar la API y probar los puntos de conexión de la API mediante Bruno, consulte las instrucciones de Información adicional.	Desarrollador de aplicaciones

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Eliminación de recursos.	Para destruir los recursos asociados a esta aplicación de ejemplo, utilice el comando siguiente:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`npx cdk destroy --all` **Note** Asegúrese de limpiar todos los registros de DNS de Route 53 que se hayan agregado manualmente para el proceso de verificac ión de la propiedad del dominio.	

Resolución de problemas

Problema	Solución
La implementación de `CustomDom ainRouterStack` agota el tiempo de espera porque el certificado no se puede validar.	Asegúrese de haber agregado los registros CNAME de validación de DNS adecuados, tal como se describió en la tarea anterior. El nuevo certificado podría continuar mostrando el estado Pendiente de validación durante un máximo de 30 minutos después de agregar los registros de validación de DNS. Para obtener más información, consulta la validación de DNS en la AWS Certificate Manager documentación.

Recursos relacionados

- Implementación del control de versiones de API Gateway basado en encabezados con Amazon CloudFront: esta entrada del blog de AWS Compute ofrece una estrategia de control de versiones

basada en encabezados como alternativa a la estrategia de control de versiones basada en rutas que se describe en este patrón.

- AWS CDK Taller: este taller introductorio se centra en la creación e implementación de aplicaciones mediante el uso de. AWS AWS Cloud Development Kit (AWS CDK) Este taller es compatible con Go, Python y TypeScript.

Información adicional

Prueba de la API con Bruno

Le recomendamos que utilice Bruno, una herramienta de prueba de API de código abierto, para comprobar que el enrutamiento basado en rutas funciona correctamente en la aplicación de ejemplo. Este patrón proporciona una colección de ejemplo para facilitar las pruebas de la API de ejemplo.

Para invocar y probar la API, use los siguientes pasos:

1. Instale Bruno.
2. Abra Bruno.
3. En el repositorio de código de este patrón, selecciona Bruno/Sample-API- Gateway-Custom-Domain-Versioning y abre la colección.
4. Para ver el menú desplegable Entornos en la parte superior derecha de la interfaz de usuario (UI), seleccione cualquier solicitud de la colección.
5. En el menú desplegable Entornos, seleccione Configurar.
6. Sustituya el valor de `REPLACE_ME_WITH_YOUR_DOMAIN` por su dominio personalizado.
7. Elija Guardar y, a continuación, cierre la sección Configuración.
8. En Entorno de pruebas, compruebe que esté seleccionada la opción Activo.
9. Invoque su API mediante el botón -> de la solicitud seleccionada.
10. Observe cómo se gestiona la validación (pasando valores no numéricos) en V1 en comparación con V2.

Para ver capturas de pantalla de ejemplos de invocación de la API y una comparación de las validaciones de V1 y V2, consulte Testing your sample API en el archivo `README.md` del repositorio de código de este patrón.

Importe la biblioteca psycopg2 para interactuar con su base de AWS Lambda datos PostgreSQL

Louis Hourcade, Amazon Web Services

Resumen

Psycopg es un adaptador de bases de datos de PostgresSQL para Python. Los desarrolladores utilizan la biblioteca `psycopg2` para escribir aplicaciones de Python que interactúan con las bases de datos de PostgreSQL.

En Amazon Web Services (AWS), los desarrolladores también utilizan AWS Lambda para ejecutar código de aplicaciones o servicios de backend. Lambda es un servicio de computación sin servidor y basado en eventos que ejecuta código sin necesidad de aprovisionar ni administrar servidores.

De forma predeterminada, cuando se crea una función nueva que utiliza un tiempo de ejecución de Python compatible con Lambda, el entorno de tiempo de ejecución de Lambda se crea a partir de una imagen base de Lambda proporcionada por AWS. Bibliotecas como `pandas` o `psycopg2` no se incluyen en la imagen base. Para usar una biblioteca, debe agruparla en un paquete personalizado y adjuntarla a Lambda.

Hay varias formas de agrupar y adjuntar una biblioteca, incluidas las siguientes:

- Implemente la función de Lambda desde un archivo .zip.
- Implemente la función de Lambda a partir de una imagen de contenedor personalizada.
- Cree una capa de Lambda y adjúntela a su función de Lambda.

Este patrón muestra las dos primeras opciones.

Con un paquete de implementación .zip, agregar la biblioteca `pandas` a la función de Lambda es relativamente sencillo. Cree una carpeta en su máquina Linux, agregue el script de Lambda junto con la biblioteca `pandas` y las dependencias de la biblioteca a la carpeta, comprima la carpeta y proporciónela como origen para su función de Lambda.

Aunque el uso de un paquete de implementación .zip es una práctica habitual, ese enfoque no funciona para la biblioteca `psycopg2`. Este patrón muestra primero el error que se produce si se utiliza un paquete de implementación .zip para agregar la biblioteca `psycopg2` a la función de Lambda. A continuación, el patrón muestra cómo implementar Lambda desde un Dockerfile y editar la imagen de Lambda para que la biblioteca `psycopg2` funcione.

Para obtener información sobre los tres recursos que implementa el patrón, consulte la sección Información adicional.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS con permisos suficientes para implementar los recursos utilizados por este patrón AWS
- AWS Cloud Development Kit (AWS CDK) instalado globalmente mediante la ejecución `npm install -g aws-cdk`
- Un cliente Git
- Python
- Docker

Limitaciones

- Algunas Servicios de AWS no están disponibles en todos Regiones de AWS. Para conocer la disponibilidad de las regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- Versión de tiempo de ejecución de Python compatible con Lambda
- Versión 2.9.3 de Psycopg2
- Versión 1.5.2 de pandas

Arquitectura

Información general de la solución

Para ilustrar los desafíos a los que puede enfrentarse al utilizar la biblioteca `psycopg2` en Lambda, el patrón implementa dos funciones de Lambda:

- Una función de Lambda con el tiempo de ejecución de Python creada a partir de un archivo .zip. Las bibliotecas `psycopg2` y `pandas` se instalan en este paquete de implementación .zip mediante pip.

- Una función de Lambda con el tiempo de ejecución de Python creada a partir de un Dockerfile. El Dockerfile instala las bibliotecas `psycopg2` y `pandas` en la imagen de contenedor de Lambda.

La primera función de Lambda instala la biblioteca `pandas` y sus dependencias en un archivo .zip; y Lambda puede usar esa biblioteca.

La segunda función de Lambda demuestra que, al crear una imagen de contenedor para la función de Lambda, puede ejecutar las bibliotecas `pandas` y `psycopg2` en Lambda.

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que lo ayuda a definir y aprovisionar la infraestructura en la nube de AWS en código.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

Otras herramientas

- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización a nivel del sistema operativo para entregar software en contenedores.
- pandas es una herramienta de código abierto basada en Python para el análisis y la manipulación de datos.
- Psycopg es un adaptador de bases de datos de PostgreSQL para el lenguaje Python diseñado para aplicaciones de varios subprocesos. Este patrón emplea Psycopg2.
- Python es un lenguaje de programación informático de uso general.

Repositorio de código

El código de este patrón está disponible en el repositorio import-psycopg2 - -. in-lambda-to-interact with-postgres-database GitHub

Prácticas recomendadas

Este patrón le proporciona un ejemplo práctico de cómo crear una función Lambda AWS CDK a partir de un Dockerfile. Si reutiliza este código en su aplicación, asegúrese de que los recursos implementados cumplan con todos los requisitos de seguridad. Utilice herramientas como Checkov, que analiza las configuraciones de la infraestructura en la nube para detectar errores de configuración antes de implementar la infraestructura.

Epics

Clonación del repositorio y configuración de la implementación

Tarea	Descripción	Habilidades requeridas

Clonar el repositorio.	Para clonar el GitHub repositorio en su máquina local, ejecute los siguientes comandos:
	`git clone https://github.com/aws-samples/import-psycopg2-in-lambda-to-interact-with-postgres-database.git`
	`cd AWS-lambda-psycopg2`
		AWS general

Configurar su implementación.	Edite el `app.py` archivo con información sobre su Cuenta de AWS:
	`aws_acccount = "AWS_ACCOUNT_ID"`
	`region = "AWS_REGION"`
	`# Select the CPU architecture you are using to build the image (ARM or X86)`
	`architecture = "ARM"`
		AWS general

Inicio de su cuenta de AWS e implementación de la aplicación

Tarea	Descripción	Habilidades requeridas
Bootstrap tu. Cuenta de AWS	Si aún no ha iniciado su entorno de AWS, ejecute los siguientes comandos con las AWS credenciales de su AWS cuenta: `cdk bootstrap aws://<tooling-account-id>/<aws-region>`	AWS general
Implementar el código.	Para implementar la AWS CDK aplicación, ejecute el siguiente comando: `cdk deploy AWSLambdaPyscopg2`	AWS general

Prueba de las funciones de Lambda desde la Consola de administración de AWS

Tarea	Descripción	Habilidades requeridas
Probar la función de Lambda creada a partir del archivo .zip.	Para probar la función de Lambda que se creó a partir del archivo .zip, haga lo siguiente: 1. Inicie sesión en la consola y abra la consola Lambda en. https://console.aws.amazon.com/lambda/	AWS general

Tarea	Descripción	Habilidades requeridas
	2. Seleccione la función de Lambda `lambda-from-zip`. 3. Cree un evento de prueba para invocar la función. 4. Cuando se invoca, la función debería generar un error con el siguiente mensaje: `"errorMessage": Unable to import module 'lambda_code': libpq.so.5: cannot open shared object, "stackTrace": [] "errorType": Runtime.ImportModuleError",` 5. Abre la CloudWatch consola de Amazon en https://console.aws.amazon.com/cloudwatch/. Los CloudWatch registros muestran que la `pandas` biblioteca se ha importado correctamente, pero que la importación de la `psycopg2` biblioteca ha fallado. Como Lambda no encuentra las bibliotecas de PostgreSQL necesarias en la imagen	

Tarea	Descripción	Habilidades requeridas
	predeterminada, no puede utilizar la biblioteca `psycopg2`.	

Tarea	Descripción	Habilidades requeridas

Probar la función de Lambda creada a partir del Dockerfile.	Para utilizar la biblioteca `psycopg2` en la función de Lambda, debe editar la imagen de máquina de Amazon (AMI) de Lambda.
	
	Para probar la función de Lambda que se creó a partir del Dockerfile, haga lo siguiente:
	
	1. Inicie sesión en la consola y abra la consola de Lambda.
	2. Seleccione la función de Lambda `lambda-from-docker` .
	3. Cree un evento de prueba para invocar la función.
	4. Cuando se invoca, la función debe ejecutarse correctamente.
	
	El código siguiente muestra el Dockerfile que crea la AWS CDK plantilla:
	
	`# Start from lambda Python3.13 image`
	`FROM public.ecr.aws/lambda/python:3.13`
	
	`# Copy the lambda code, together with its requirements`
		AWS general

Tarea	Descripción	Habilidades requeridas

	``
	COPY lambda/requirement
	s.txt ${LAMBDA_
	TASK_ROOT}
	COPY lambda/lambda_code
	.py ${LAMBDA_TASK_ROOT
	}
	
	# Install postgresql-
	devel in your image
	RUN yum install -y gcc
	 postgresql-devel
	
	# install the requireme
	nts for the Lambda code
	RUN pip3 install -r
	 requirements.txt
	 --target "${LAMBDA
	_TASK_ROOT}"
	
	# Command can be
	 overwritten by
	 providing a different
	 command in the template
	 directly.
	CMD ["lambda_code.hand
	ler"]
	``
	
	El Dockerfile toma la imagen AWS Lambda proporcionada para el entorno de ejecución de Python e instala postgresql-devel, que contiene las bibliotecas necesarias para compilar aplicaciones que interactúan directamente con el servidor de administración de PostgreSQL. El Dockerfile también instala las bibliotecas `pandas` y `psycopg2`,	

Tarea	Descripción	Habilidades requeridas
	que se indican en el archivo `requirements.txt` .	

Recursos relacionados

- AWS CDK documentación
- AWS Lambda documentación

Información adicional

En este patrón, la AWS CDK plantilla proporciona una AWS pila con tres recursos:

- Un rol de AWS Identity and Access Management (IAM) para las funciones de Lambda.
- Una función de Lambda con el tiempo de ejecución de Python. La función se implementa desde el paquete de implementación `Constructs/lambda/lambda_deploy.zip`.
- Una función de Lambda con el tiempo de ejecución de Python. La función se implementa desde el Dockerfile de la carpeta `Constructs`.

El script de ambas funciones de Lambda comprueba si las bibliotecas `pandas` y `psycopg2` se han importado correctamente:

```
import pandas
print("pandas successfully imported")

import psycopg2
print("psycopg2 successfully imported")

def handler(event, context):
    """Function that checks whether psycopg2  and pandas are successfully imported or
 not"""
    return {"Status": "psycopg2 and pandas successfully imported"}
```

El paquete de implementación `lambda_deploy.zip` se crea con el script de bash `Constructs/lambda/build.sh`. Este script crea una carpeta, copia el script de Lambda, instala las bibliotecas

`pandas` y `psycopg2` y genera el archivo .zip. Para generar el archivo.zip usted mismo, ejecute este script bash y vuelva a implementar la pila. AWS CDK

El Dockerfile comienza con la imagen base AWS proporcionada para Lambda con un motor de ejecución de Python. El Dockerfile instala las bibliotecas `pandas` y `psycopg2` sobre la imagen predeterminada.

Integre Amazon API Gateway con Amazon SQS para gestionar el REST asíncrono APIs

Natalia Colantonio Favero y Gustavo Martim, Amazon Web Services

Resumen

Al implementar REST APIs, a veces es necesario exponer una cola de mensajes que las aplicaciones cliente puedan publicar. Por ejemplo, es posible que tenga problemas con la latencia de terceros APIs y que se produzcan retrasos en las respuestas, o puede que desee evitar el tiempo de respuesta de las consultas a la base de datos o escalar el servidor cuando hay un gran número de consultas APIs simultáneas. En estos escenarios, las aplicaciones cliente que publican en la cola solo necesitan saber que la API ha recibido los datos, no lo que ocurre después de recibirlos.

Este patrón crea un punto de conexión de la API de REST mediante Amazon API Gateway para enviar un mensaje a Amazon Simple Queue Service (Amazon SQS). Crea una easy-to-implement integración entre los dos servicios que evita el acceso directo a la cola de SQS.

Requisitos previos y limitaciones

- Una cuenta activa AWS

Arquitectura

En el siguiente diagrama se muestran estos pasos:

1. Solicite un punto de conexión de la API de REST POST mediante una herramienta como Postman, otra API u otras tecnologías.
2. API Gateway publica un mensaje, que se recibe en el cuerpo de la solicitud, en la cola.
3. Amazon SQS recibe el mensaje y envía una respuesta a API Gateway con un código de éxito o error.

Tools (Herramientas)

- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket APIs a cualquier escala.

- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.

Epics

Creación de una cola de SQS

Tarea	Descripción	Habilidades requeridas
Creación de una cola.	Para crear una cola de SQS que reciba los mensajes de la API de REST: 1. Inicie sesión en su Cuenta de AWS. 2. Abra la consola Amazon SQS en. https://console.aws.amazon.com/sqs/ 3. Elige Crear cola. 4. En la página Crear cola, elija la correcta en la lista desplegable Región de AWS de regiones. 5. En Tipo, mantenga los ajustes predeterminados (Estándar). 6. Escriba un Nombre para la cola. 7. Mantenga los valores predeterminados para el resto de ajustes. 8. Elige Crear cola.	Desarrollador de aplicaciones

Cómo proporcionar acceso a Amazon SQS

Tarea	Descripción	Habilidades requeridas
Crear un rol de IAM.	Este rol de IAM proporciona a los recursos de API Gateway acceso completo a Amazon SQS. 1. Abra la consola de IAM en https://console.aws.amazon.com/iam/. 2. En el panel de navegación, seleccione Roles, Crear rol. 3. En Tipo de entidad de confianza, elija Servicio de AWS. 4. En Caso de uso, elija API Gateway en la lista desplegable y, a continuación, elija Siguiente, Siguiente. 5. En el nombre del rol, introduzca AWSGatewayRoleForSQS y una descripción opcional y, a continuación, elija Crear rol. 6. En el panel Funciones, busque AWSGatewayRoleForSQS y seleccione su casilla de verificación. 7. En la sección Políticas de permisos, elija Agregar permisos, Adjuntar políticas.	Desarrollador de aplicaciones, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	8. Busca Amazon SQSFull Access y selecciónalo. 9. Elija Añadir permisos. 10. En la sección Resumen de AWSGatewayRoleForSQS, copie el número de recurso de Amazon (ARN). Usará este ID en un paso posterior.	

Crear una API de REST

Tarea	Descripción	Habilidades requeridas
Crear una API de REST.	Esta es la API de REST a la que se envían las solicitudes HTTP. 1. Abra la consola de API Gateway en https://console.aws.amazon.com/apigateway/. 2. En el cuadro API de REST, elija Crear. 3. En Nombre de API, ingrese un nombre y una descripción opcional para la API, conserve todas las demás configuraciones predeterminadas y, a continuación, seleccione Crear API.	Desarrollador de aplicaciones
Conectar API Gateway a Amazon SQS.	Este paso permite que el mensaje fluya desde el cuerpo	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	de la solicitud HTTP hasta Amazon SQS. 1. En la consola de API Gateway, elija la API que ha creado. 2. En la página Recursos, en la sección Métodos, elija Crear método. 3. En Tipo de método, elija POST. 4. En Tipo de integración, elija Servicio de AWS. 5. En Región de AWS, elija la región en la que creó la cola de SQS. 6. En Servicio de AWS, elija Simple Queue Service (SQS). 7. En Método HTTP, elija POST. 8. En Tipo de acción, elija Usar sustitución de ruta. 9. En Sustitución de ruta, ingrese <ID de la cuenta de AWS>/<nombre de la cola de SQS>. 10. En Rol de ejecución, pegue el ARN del rol que creó anteriormente. 11. Elija Crear método.	

Prueba de la API de REST

Tarea	Descripción	Habilidades requeridas

Probar la API de REST.	Ejecute una prueba para comprobar si falta alguna configuración:
	1. En la consola de API Gateway, elija la API de REST que ha creado.
	2. En el panel Recursos, elija el método POST.
	3. Elija la pestaña Prueba. (Use la flecha derecha si no se muestra la pestaña).
	4. En Cuerpo de la solicitud, pegue el siguiente código JSON:
	`{ "message": "lorem ipsum" }`
	5. Seleccione Probar
	Recibirá un error similar al siguiente:
	`<UnknownOperationException/>`
		Desarrollador de aplicaciones

Cambiar la integración de la API para reenviar la solicitud correctamente a Amazon SQS.	Complete la configuración para corregir el error de integración:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	1. En la consola de API Gateway, elija la API que creó y, a continuación, elija POST. 2. En la sección Ejecución de método se muestra la asignación visual entre API Gateway y Amazon SQS. En esta sección, elija Solicitud de integración y, a continuación, Editar. 3. Expanda la sección Encabezados HTTP y, a continuación, elija el parámetro Agregar encabezado de solicitud. • En Nombre, especifique Content-Type. • En Mapped from, introduzca «application/» x-www-form-urlencoded. Asegúrese de incluir las comillas simples. • Seleccione la casilla de verificación Almacenam iento en caché. 4. Expanda la sección Plantilla s de mapeo. • Elija Add mapping template (Añadir plantilla de asignación). • En Tipo de contenido, escriba application/json.	

Tarea	Descripción	Habilidades requeridas
	• En Cuerpo de la plantilla, pegue este código: `Action=SendMessage&MessageBody=$input.body` • Seleccione Save.	

Tarea	Descripción	Habilidades requeridas
Probar y validar el mensaje en Amazon SQS.	Ejecute una prueba para confirmar que la prueba se haya completado correctam ente: 1. En la consola de API Gateway, elija la API de REST que ha creado. 2. En el panel Recursos, elija el método POST. 3. Elija la pestaña Prueba. (Use la flecha derecha si no se muestra la pestaña). 4. En Cuerpo de la solicitud, pegue el siguiente código JSON: `{ "message": "lorem ipsum" }` 5. Seleccione Probar 6. Abra la consola de Amazon SQS. 7. En el panel de navegación, elija Colas y luego elija su cola. 8. Seleccione Enviar y recibir mensajes. 9. Seleccione Sondeo de mensajes. 10. Elija Mensaje. Debería aparecer lo siguiente:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`Body { "message": "lorem ipsum" }`	

Tarea	Descripción	Habilidades requeridas

Probar API Gateway con un carácter especial.	Ejecute una prueba que incluya caracteres especiales (como &) que no sean aceptables en un mensaje:
	1. En la consola de API Gateway, elija su API.
	2. Repita la prueba del paso anterior con el siguiente código JSON:
	`{ "message": "lorem ipsum &" }`
	3. Seleccione Probar
	Recibirá un error como el siguiente:
	`{ "Error": { "Code": "AccessDenied", "Message": "Access to the resource https://sqs.us-east-2.amazonaws.com/976166761794/Apg2 is denied.", "Type": "Sender" }, "RequestId": "e83c9c67-bcf6-5e9a-91e9-c737094b17ab"`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	<pre>}</pre> Esto se debe a que los caracteres especiales no se admiten de forma predeterminada en el cuerpo del mensaje. En el siguiente paso, configurará API Gateway para que admita caracteres especiales. Para obtener más información sobre las conversiones de tipos de contenido, consulte la documentación de API Gateway.	

Tarea	Descripción	Habilidades requeridas

Cambiar la configuración de la API para que admita caracteres especiales.	Ajuste la configuración para que acepte caracteres especiales en el mensaje:
	1. En la consola de API Gateway, elija la API que creó y, a continuación, elija POST.
	2. Elija Solicitud de integración y, a continuación, Editar.
	3. Cambie Tratamiento de contenido a Convertir en texto.
	4. En la sección Plantillas de mapeo:
	• En Tipo de contenido, escriba application/json.
	• En Cuerpo de la plantilla, especifique:
	`Action=SendMessage&MessageBody=$util.urlEncode($input.body)`
	• Seleccione Save.
	5. Elija la pestaña Prueba.
	6. En Cuerpo de la solicitud, ingrese el código JSON anterior:
	`{ " message": "lorem ipsum &" }`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	7. Seleccione Probar 8. Abra la consola de Amazon SQS. 9. Seleccione su cola y, a continuación, elija Enviar y recibir mensajes, Sondear si hay mensajes y Mensaje como antes. El nuevo mensaje debe incluir el carácter especial.	

Implementación de la API de REST

Tarea	Descripción	Habilidades requeridas
Implementar la API.	Para implementar la API de REST: 1. Abra la consola de API Gateway. 2. Elija la API. 3. Elija Implementar API. Para obtener más información sobre este paso, consulte la documentación de API Gateway.	Desarrollador de aplicaciones
Probar con una herramienta externa.	Ejecute una prueba con una herramienta externa para confirmar que el mensaje se ha recibido correctamente:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	1. Abra una herramienta como Postman, Insomnia o cURL. 2. Ejecute su API. 3. Abra la consola de Amazon SQS. 4. Seleccione su cola. 5. Cargue los mensajes para ver el mensaje nuevo.	

Eliminación

Tarea	Descripción	Habilidades requeridas
Eliminar la API.	En la consola de API Gateway, elija la API que creó y, a continuación, elija Eliminar.	Desarrollador de aplicaciones
Eliminación del rol de IAM.	En la consola de IAM, en el panel Funciones, seleccione AWSGatewayRoleForSQS y, a continuación, elija Eliminar.	Desarrollador de aplicaciones
Eliminar la cola de SQS.	En la consola de Amazon SQS, en el panel Colas, elija la cola de SQS que ha creado y, a continuación, elija Eliminar.	Desarrollador de aplicaciones

Recursos relacionados

- SQS- SendMessage (documentación de API Gateway)
- Conversiones de tipo de contenido en API Gateway (documentación de API Gateway)

- Variables $util (documentación de API Gateway)
- ¿Cómo puedo integrar una API REST de API Gateway con Amazon SQS y resolver los errores más comunes? (Artículo de AWS Re:POST)

Procesamiento de eventos de forma asíncrona con Amazon API Gateway y AWS Lambda

Andrea Meroni, Mariem Kthiri, Nadim Majed y Michael Wallner, Amazon Web Services

Resumen

Amazon API Gateway es un servicio totalmente gestionado que los desarrolladores pueden utilizar para crear, publicar, mantener, supervisar y proteger APIs a cualquier escala. Gestiona las tareas relacionadas con la aceptación y el procesamiento de centenares de miles de llamadas simultáneas a la API.

Una cuota de servicio importante de API Gateway es el tiempo de espera de la integración. El tiempo de espera es el tiempo máximo durante el que un servicio de backend debe devolver una respuesta antes de que la API de REST devuelva un error. El límite estricto de 29 segundos suele ser aceptable para las cargas de trabajo sincrónicas. Sin embargo, ese límite representa un desafío para los desarrolladores que desean usar API Gateway con cargas de trabajo asíncronas.

Este patrón muestra un ejemplo de arquitectura para procesar eventos de forma asíncrona mediante API Gateway y. AWS Lambda La arquitectura admite la puesta en marcha de trabajos de procesamiento con una duración de hasta 15 minutos y utiliza una API de REST básica como interfaz.

Projen se utiliza para configurar el entorno de desarrollo local y para implementar la arquitectura de ejemplo en un objetivo Cuenta de AWS, en combinación con el AWS Cloud Development Kit (AWS CDK) kit de herramientas, Docker y Node.js. Projen configura automáticamente un entorno virtual de Python con pre-commit y las herramientas que se utilizan para garantizar la calidad del código, analizar la seguridad y realizar pruebas unitarias. Para obtener más información, consulte la sección Herramientas.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Las siguientes herramientas están instaladas en su estación de trabajo:
  - AWS Cloud Development Kit (AWS CDK) Kit de herramientas versión 2.85.0
  - La versión 20.10.21 de Docker
  - Versión 18.13.0 de Node.js

- La versión 0.71.111 de Projen
- La versión 3.9.16 de Python

Limitaciones

- El tiempo de ejecución máximo de un trabajo está limitado por el tiempo de ejecución máximo de las funciones de Lambda (15 minutos).
- El número máximo de solicitudes de trabajo simultáneas está limitado por la simultaneidad reservada de la función de Lambda.

Arquitectura

El siguiente diagrama muestra la interacción de la API de trabajos con las funciones Lambda de procesamiento y gestión de errores de eventos, con los eventos almacenados en un archivo de eventos de Amazon. EventBridge

Un flujo de trabajo habitual incluye los siguientes pasos:

1. Usted se autentica con AWS Identity and Access Management (IAM) y obtiene las credenciales de seguridad.
2. Envía una solicitud `POST` HTTP al punto de conexión de la API de trabajos `/jobs`, especificando los parámetros del trabajo en el cuerpo de la solicitud.
3. La API de trabajos, que es una API de REST de API Gateway, le devuelve una respuesta HTTP que contiene el identificador del trabajo.
4. La API de trabajos invoca de forma asíncrona la función de Lambda de procesamiento de eventos.
5. La función de procesamiento de eventos procesa el evento y, a continuación, agrega los resultados del trabajo a la tabla de Amazon DynamoDB de trabajos.
6. Envía una solicitud `GET` HTTP al punto de conexión de la API de trabajos `/jobs/{jobId}`, con el identificador de trabajo del paso 3 como `{jobId}`.
7. La API de trabajos consulta la tabla `jobs` de DynamoDB para recuperar los resultados del trabajo.
8. La API de trabajos devuelve una respuesta HTTP que contiene los resultados del trabajo.
9. Si se produce un error al procesar un evento, la función de procesamiento de eventos envía el evento a la función de gestión de errores.
10. La función de gestión de errores agrega los parámetros del trabajo a la tabla `jobs` de DynamoDB.

11. Puede recuperar los parámetros del trabajo enviando una solicitud `GET` HTTP al punto de conexión de la API de trabajos `/jobs/{jobId}`.
12. Si se produce un error en la gestión de errores, la función de gestión de errores envía el evento a un archivo de eventos. EventBridge

    Puede reproducir los eventos archivados utilizando. EventBridge

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir y aprovisionar la Nube de AWS infraestructura en código.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, funciones de Lambda, puntos de conexión de invocación HTTP que utilizan destinos de API o buses de eventos en otras Cuentas de AWS.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

Otras herramientas

- autopep8 formatea automáticamente el código de Python según la guía de estilo Python Enhancement Proposal (PEP) 8.
- Bandit analiza el código de Python para detectar problemas de seguridad comunes.
- Commitizen un verificador de confirmaciones y generador de `CHANGELOG` de Git.
- cfn-lint es un linter AWS CloudFormation
- Checkov es una herramienta de análisis de código estático que revisa si la infraestructura como código (IaC) se ha configurado mal en términos de seguridad y cumplimiento.

- jq es una herramienta de línea de comandos para analizar JSON.
- Postman es una plataforma de API.
- pre-commit es un administrador de enlaces de Git.
- Projen es un generador de proyectos.
- pytest es un marco de Python para escribir pruebas pequeñas y legibles.

Repositorio de código

Este ejemplo de código de arquitectura se encuentra en el repositorio Lambda y procesamiento de eventos GitHub asíncrono con API Gateway.

Prácticas recomendadas

- Esta arquitectura de ejemplo no incluye la supervisión de la infraestructura implementada. Si su caso de uso requiere supervisión, evalúe la posibilidad de agregar CDK Monitoring Constructs u otra solución de supervisión.
- Esta arquitectura de ejemplo usa permisos de IAM para controlar el acceso a la API de trabajos. Cualquier persona autorizada a asumir `JobsAPIInvokeRole` podrá invocar la API de trabajos. Como tal, el mecanismo de control de acceso es binario. Si su caso de uso requiere un modelo de autorización más complejo, evalúe la posibilidad de usar un mecanismo de control de acceso diferente.
- Cuando un usuario envía una solicitud `POST` HTTP al punto de conexión de la API de trabajos `/jobs`, los datos de entrada se validan en dos niveles diferentes:
  - Amazon API Gateway se encarga de la validación de la primera solicitud.
  - La función de procesamiento de eventos realiza la segunda solicitud.

    No se hace ninguna validación cuando el usuario realiza una solicitud `GET` HTTP al punto de conexión de la API de trabajos `/jobs/{jobId}`. Si su caso de uso requiere una validación de entrada adicional y un mayor nivel de seguridad, evalúe la posibilidad de usar AWS WAF para proteger su API.

Epics

Configuración del entorno

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Para clonar el repositorio localmente, use el siguiente comando: `git clone https://github.com/aws-samples/asynchronous-event-processing-api-gateway-lambda-cdk.git`	DevOps ingeniero

Configure el proyecto.	Cambie el directorio a la raíz del repositorio y configure el entorno virtual de Python y todas las herramientas mediante Projen
	`cd asynchronous-event-processing-api-gateway-api-gateway-lambda-cdk`
	`npx projen`
		DevOps ingeniero

Instale enlaces de pre-commit.	Para instalar enlaces de pre-commit, haga lo siguiente: 1. Active el entorno virtual Python: `source .env/bin/activate` 2. Instale los enlaces de pre-commit:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`pre-commit install` `pre-commit install --hook-type commit-msg`	

Implementación de la arquitectura de ejemplo

Tarea	Descripción	Habilidades requeridas
Bootstrap. AWS CDK	Para arrancar AWS CDK Cuenta de AWS, ejecuta el siguiente comando: `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen bootstrap`	AWS DevOps
Implemente la arquitectura de ejemplo.	Para implementar la arquitectura de ejemplo en su Cuenta de AWS hogar, ejecute el siguiente comando: `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen deploy`	AWS DevOps

Prueba de la arquitectura

Tarea	Descripción	Habilidades requeridas
Instale los requisitos previos de prueba.	Instale en su estación de trabajo AWS Command Line Interface (AWS CLI), Postman y jq.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Se sugiere usar Postman para probar esta arquitectura de ejemplo, pero no es obligatorio. Si elige una herramienta para probar API alternativa, asegúrese de que sea compatible con la autenticación de AWS Signature Version 4 y consulte los puntos de conexión de la API expuestos, que se pueden inspeccionar exportando la API de REST.	

Tarea	Descripción	Habilidades requeridas
Asuma el `JobsAPIInvokeRole` .	Asuma el `JobsAPIInvokeRole` que apareció en la salida del comando de implementación: `CREDENTIALS=$(AWS_PROFILE=$<YOUR_AWS_PROFILE> aws sts assume-role \ --no-cli-pager \ --role-arn $<JOBS_API_INVOKE_ROLE_ARN> \ --role-session-name JobsAPIInvoke) export AWS_ACCESS_KEY_ID=$(cat $CREDENTIALS \| jq '.Credentials''.AccessKeyId') export AWS_SECRET_ACCESS_KEY=$(cat $CREDENTIALS \| jq '.Credentials''.SecretAccessKey') export AWS_SESSION_TOKEN==$(cat $CREDENTIALS | jq '.Credentials''.SessionToken')`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Configure Postman.	1. Para importar la colección de Postman que se incluye en el repositorio, siga las instrucciones de la documentación de Postman. 2. Defina las variables de `JobsAPI` con los siguientes valores: • `accessKey` : el valor del atributo `Credentials.AccessKeyId` del comando `assume-role` . • `baseUrl`: el valor de la salida de `JobsApiJobsAPIEndpoint` del comando de implementación sin la barra diagonal final. • `region`– El valor del Región de AWS lugar en el que implementó la arquitectura de ejemplo • `seconds`: el valor de un parámetro de entrada para el trabajo de ejemplo. Debe ser un entero positivo. • `secretKey` : el valor del atributo `Credentials.SecretAccessKey` del	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	comando `assume-role` . • `sessionToken` : el valor del atributo `Credentials.SessionToken` del comando `assume-role` .	
Pruebe la arquitectura de ejemplo.	Para probar la arquitectura de ejemplo, envíe solicitudes a la API de trabajos. Para obtener más información, consulte la documentación de Postman.	DevOps ingeniero

Resolución de problemas

Problema	Solución
La destrucción y posterior redespliegue de la arquitectura de ejemplo fallan porque el grupo de CloudWatch registros de Amazon Logs `/aws/apigateway/JobsAPIAccessLogs` ya existe.	1. Si es necesario, exporte los datos de registro a Amazon S3. 2. Elimine el grupo CloudWatch de registros `/aws/apigateway/JobsAPIAccessLogs` . 3. Vuelva a implementar la arquitectura de ejemplo.

Recursos relacionados

- Plantilla de mapeo de API Gateway y referencia de variables de registro de acceso
- Configurar la invocación asíncrona de la función Lambda de backend

Procesamiento de eventos de forma asíncrona con Amazon API Gateway y Amazon DynamoDB Streams

Andrea Meroni, Mariem Kthiri, Nadim Majed, Alessandro Trisolini y Michael Wallner,
Amazon Web Services

Resumen

Amazon API Gateway es un servicio totalmente gestionado que los desarrolladores pueden utilizar para crear, publicar, mantener, supervisar y proteger APIs a cualquier escala. Gestiona las tareas relacionadas con la aceptación y el procesamiento de centenares de miles de llamadas simultáneas a la API.

Una cuota de servicio importante de API Gateway es el tiempo de espera de la integración. El tiempo de espera es el tiempo máximo durante el que un servicio de backend debe devolver una respuesta antes de que la API de REST devuelva un error. El límite estricto de 29 segundos suele ser aceptable para las cargas de trabajo sincrónicas. Sin embargo, ese límite representa un desafío para los desarrolladores que desean usar API Gateway con cargas de trabajo asíncronas.

Este patrón muestra un ejemplo de arquitectura para procesar eventos de forma asíncrona mediante API Gateway, Amazon DynamoDB Streams y. AWS Lambda La arquitectura admite la puesta en marcha de trabajos de procesamiento en paralelo con los mismos parámetros de entrada y utiliza una API de REST básica como interfaz. En este ejemplo, el uso de Lambda como backend limita la duración de los trabajos a 15 minutos. Puede evitar este límite utilizando un servicio alternativo para procesar los eventos entrantes (por ejemplo,). AWS Fargate

Projen se utiliza para configurar el entorno de desarrollo local y para implementar la arquitectura de ejemplo en un objetivo Cuenta de AWS, en combinación con el AWS Cloud Development Kit (AWS CDK) kit de herramientas, Docker y Node.js. Projen configura automáticamente un entorno virtual de Python con pre-commit y las herramientas que se utilizan para garantizar la calidad del código, analizar la seguridad y realizar pruebas unitarias. Para obtener más información, consulte la sección Herramientas.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Las siguientes herramientas están instaladas en su estación de trabajo:

- AWS Cloud Development Kit (AWS CDK) Kit de herramientas versión 2.85.0 o posterior
- La versión 20.10.21 o posterior de Docker
- La versión 18 o posterior de Node.js
- La versión 0.71.111 o posterior de Projen
- La versión 3.9.16 o posterior de Python

Limitaciones

- El número máximo recomendado de lectores para DynamoDB Streams es de dos para evitar la limitación.
- El tiempo de ejecución máximo de un trabajo está limitado por el tiempo de ejecución máximo de las funciones de Lambda (15 minutos).
- El número máximo de solicitudes de trabajo simultáneas está limitado por la simultaneidad reservada de las funciones de Lambda.

Arquitectura

Arquitectura

El siguiente diagrama muestra la interacción de la API de trabajos con DynamoDB Streams y las funciones Lambda de procesamiento y gestión de errores de eventos, con los eventos almacenados en un archivo de eventos de Amazon. EventBridge

Un flujo de trabajo habitual incluye los siguientes pasos:

1. Se autentica con (IAM) y se obtienen las credenciales de seguridad AWS Identity and Access Management .
2. Envía una solicitud `POST` HTTP al punto de conexión de la API de trabajos `/jobs`, especificando los parámetros del trabajo en el cuerpo de la solicitud.
3. La API de trabajos devuelve una respuesta HTTP que contiene el identificador del trabajo.
4. La API de trabajos agrega los parámetros del trabajo a la tabla `jobs_table` de Amazon DynamoDB.
5. El flujo de DynamoDB de la tabla de DynamoDB `jobs_table` invoca las funciones de Lambda de procesamiento de eventos.

6. Las funciones de Lambda de procesamiento de eventos procesan el evento y, a continuación, agregan los resultados del trabajo a la tabla `jobs_table` de DynamoDB. Para garantizar la coherencia de los resultados, las funciones de procesamiento de eventos implementan un mecanismo de bloqueo positivo.
7. Envía una solicitud `GET` HTTP al punto de conexión de la API de trabajos `/jobs/{jobId}`, con el identificador de trabajo del paso 3 como `{jobId}`.
8. La API de trabajos consulta la tabla `jobs_table` de DynamoDB para recuperar los resultados del trabajo.
9. La API de trabajos devuelve una respuesta HTTP que contiene los resultados del trabajo.
10. Si el procesamiento de eventos falla, la asignación de orígenes de la función de procesamiento de eventos envía el evento al tema de Amazon Simple Notification Service (Amazon SNS) de gestión de errores.
11. El tema de gestión de errores de SNS envía el evento de forma asíncrona a la función de gestión de errores.
12. La función de gestión de errores agrega los parámetros del trabajo a la tabla `jobs_table` de DynamoDB.

    Puede recuperar los parámetros del trabajo enviando una solicitud `GET` HTTP al punto de conexión de la API de trabajos `/jobs/{jobId}`.
13. Si la gestión de errores falla, la función de gestión de errores envía el evento a un archivo de Amazon EventBridge .

    Puede reproducir los eventos archivados utilizando. EventBridge

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que lo ayuda a definir y aprovisionar la infraestructura en la nube de AWS en código.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, las funciones de AWS Lambda, los puntos de conexión de invocación HTTP que utilizan destinos de API o los buses de eventos de otras cuentas de AWS.

- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.

Otras herramientas

- autopep8 formatea automáticamente el código de Python según la guía de estilo Python Enhancement Proposal (PEP) 8.
- Bandit analiza el código de Python para detectar problemas de seguridad comunes.
- Commitizen un verificador de confirmaciones y generador de `CHANGELOG` de Git.
- cfn-lint es un linter AWS CloudFormation
- Checkov es una herramienta de análisis de código estático que revisa si la infraestructura como código (IaC) se ha configurado mal en términos de seguridad y cumplimiento.
- jq es una herramienta de línea de comandos para analizar JSON.
- Postman es una plataforma de API.
- pre-commit es un administrador de enlaces de Git.
- Projen es un generador de proyectos.
- pytest es un marco de Python para escribir pruebas pequeñas y legibles.

Repositorio de código

Este ejemplo de código de arquitectura se encuentra en el repositorio GitHub Asynchronous Processing with API Gateway y DynamoDB Streams.

Prácticas recomendadas

- Esta arquitectura de ejemplo no incluye la supervisión de la infraestructura implementada. Si su caso de uso requiere supervisión, evalúe la posibilidad de agregar CDK Monitoring Constructs u otra solución de supervisión.
- Esta arquitectura de ejemplo usa permisos de IAM para controlar el acceso a la API de trabajos. Cualquier persona autorizada a asumir `JobsAPIInvokeRole` podrá invocar la API de trabajos.

Como tal, el mecanismo de control de acceso es binario. Si su caso de uso requiere un modelo de autorización más complejo, evalúe la posibilidad de usar un mecanismo de control de acceso diferente.

- Cuando un usuario envía una solicitud `POST` HTTP al punto de conexión de la API de trabajos `/jobs`, los datos de entrada se validan en dos niveles diferentes:
  - API Gateway se encarga de la validación de la primera solicitud.
  - La función de procesamiento de eventos realiza la segunda solicitud.

    No se hace ninguna validación cuando el usuario realiza una solicitud `GET` HTTP al punto de conexión de la API de trabajos `/jobs/{jobId}`. Si su caso de uso requiere una validación de entrada adicional y un mayor nivel de seguridad, evalúe su uso AWS WAF para proteger su API.

- Para evitar limitaciones, la documentación de DynamoDB Streams desaconseja a los usuarios hacer operaciones de lectura con más de dos consumidores de la misma partición del flujo. Para escalar horizontalmente el número de consumidores, le recomendamos que utilice Amazon Kinesis Data Streams.
- En este ejemplo, se ha utilizado el bloqueo positivo para garantizar actualizaciones coherentes de los elementos de la tabla `jobs_table` de DynamoDB. Según los requisitos del caso de uso, es posible que tenga que implementar mecanismos de bloqueo más fiables, como el bloqueo negativo.

Epics

Configuración del entorno

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Para clonar el repositorio localmente, use el siguiente comando: `git clone https://github.com/aws-samples/asynchronous-event-processing-ap`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`i-gateway-dynamodb-streams-cdk.git`	

Configure el proyecto.	Cambie el directorio a la raíz del repositorio y configure el entorno virtual de Python y todas las herramientas mediante Projen:
	`cd asynchronous-event-processing-api-gateway-api-gateway-dynamodb-streams-cdk`
	`npx projen`
		DevOps ingeniero

Instale enlaces de pre-commit.	Para instalar enlaces de pre-commit, haga lo siguiente:
	1. Active el entorno virtual Python:
	`source .env/bin/activate`
	2. Instale los enlaces de pre-commit:
	`pre-commit install`
	`pre-commit install --hook-type commit-msg`
		DevOps ingeniero

Implementación de la arquitectura de ejemplo

Tarea	Descripción	Habilidades requeridas
Bootstrap. AWS CDK	Para arrancar AWS CDK Cuenta de AWS, ejecuta el siguiente comando: `AWS_PROFILE=$YOUR_ AWS_PROFILE npx projen bootstrap`	AWS DevOps
Implemente la arquitectura de ejemplo.	Para implementar la arquitectura de ejemplo en su Cuenta de AWS hogar, ejecute el siguiente comando: `AWS_PROFILE=$YOUR_ AWS_PROFILE npx projen deploy`	AWS DevOps

Prueba de la arquitectura

Tarea	Descripción	Habilidades requeridas
Instale los requisitos previos de prueba.	Instale en su estación de trabajo AWS Command Line Interface (AWS CLI), Postman y jq. Se sugiere usar Postman para probar esta arquitectura de ejemplo, pero no es obligatorio. Si elige una herramienta para probar API alternativa, asegúrese de que sea compatible con	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	la autenticación de AWA Signature Version 4 y consulte los puntos de conexión de la API expuestos, que se pueden inspeccionar exportando la API de REST.	
Asuma el `JobsAPIInvokeRole` .	Asuma el `JobsAPIInvokeRole` que apareció en la salida del comando `deploy`: `CREDENTIALS=$(AWS_PROFILE=$<YOUR_AWS_PROFILE> aws sts assume-role \ --no-cli-pager \ --role-arn $<JOBS_API_INVOKE_ROLE_ARN> \ --role-session-name JobsAPIInvoke) export AWS_ACCESS_KEY_ID=$(cat $CREDENTIALS \| jq '.Credentials''.AccessKeyId') export AWS_SECRET_ACCESS_KEY=$(cat $CREDENTIALS \| jq '.Credentials''.SecretAccessKey') export AWS_SESSION_TOKEN==$(cat $CREDENTIALS | jq '.Credentials''.SessionToken')`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

Configure Postman.	• Para importar la colección de Postman que se incluye en el repositorio, siga las instrucciones de la documentación de Postman.
	• Defina las variables de `JobsAPI` con los siguientes valores:
	  • `accessKey` : el valor del atributo `Credentials.AccessKeyId` del comando `assume-role` .
	  • `baseUrl`: el valor de la salida de `JobsApiJobsAPIEndpoint` del comando `deploy` sin la barra diagonal final.
	  • `region`– El valor del Región de AWS lugar en el que implementó la arquitectura de ejemplo.
	  • `seconds`: el valor de un parámetro de entrada para el trabajo de ejemplo. Debe ser un entero positivo.
	  • `secretKey` : el valor del atributo `Credentials.SecretAccessKey` del comando `assume-role` .
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• `sessionToken` : el valor del atributo `Credentials.SessionToken` del comando `assume-role` .	
Pruebe la arquitectura de ejemplo.	Para probar la arquitectura de ejemplo, envíe solicitudes a la API de trabajos. Para obtener más información, consulte la documentación de Postman.	DevOps ingeniero

Resolución de problemas

Problema	Solución
La destrucción y posterior redespliegue de la arquitectura de ejemplo fallan porque el grupo de CloudWatch registros de Amazon Logs `/aws/apigateway/JobsAPIAccessLogs` ya existe.	1. Si es necesario, exporte los datos de registro a Amazon Simple Storage Service (Amazon S3). 2. Elimine el grupo CloudWatch de registros `/aws/apigateway/JobsAPIAccessLogs`. 3. Vuelva a implementar la arquitectura de ejemplo.

Recursos relacionados

- Plantilla de mapeo de API Gateway y referencia de variables de registro de acceso
- Cambiar la captura de datos para DynamoDB Streams
- Bloqueo optimista con número de versión
- Uso de Kinesis Data Streams para capturar los cambios en DynamoDB

Procesamiento de eventos de forma asíncrona con Amazon API Gateway, Amazon SQS y AWS Fargate

Andrea Meroni, Mariem Kthiri, Nadim Majed, Alessandro Trisolini y Michael Wallner,
Amazon Web Services

Resumen

Amazon API Gateway es un servicio totalmente gestionado que los desarrolladores pueden utilizar para crear, publicar, mantener, supervisar y proteger APIs a cualquier escala. Gestiona las tareas relacionadas con la aceptación y el procesamiento de centenares de miles de llamadas simultáneas a la API.

Una cuota de servicio importante de API Gateway es el tiempo de espera de la integración. El tiempo de espera es el tiempo máximo durante el que un servicio de backend debe devolver una respuesta antes de que la API de REST devuelva un error. El límite estricto de 29 segundos suele ser aceptable para las cargas de trabajo sincrónicas. Sin embargo, ese límite representa un desafío para los desarrolladores que desean usar API Gateway con cargas de trabajo asíncronas.

Este patrón muestra un ejemplo de arquitectura para procesar eventos de forma asíncrona mediante API Gateway, Amazon Simple Queue Service (Amazon SQS) y. AWS Fargate La arquitectura admite la puesta en marcha de trabajos de procesamiento sin restricciones de duración y utiliza una API de REST básica como interfaz.

Projen se utiliza para configurar el entorno de desarrollo local y para implementar la arquitectura de ejemplo en un objetivo Cuenta de AWS, en combinación con Docker y Node.js. AWS Cloud Development Kit (AWS CDK) Projen configura automáticamente un entorno virtual de Python con pre-commit y las herramientas que se utilizan para garantizar la calidad del código, analizar la seguridad y realizar pruebas unitarias. Para obtener más información, consulte la sección Herramientas.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Las siguientes herramientas están instaladas en su estación de trabajo:
  - AWS Cloud Development Kit (AWS CDK) Kit de herramientas versión 2.85.0 o posterior

- La versión 20.10.21 o posterior de Docker
- La versión 18 o posterior de Node.js
- La versión 0.71.111 o posterior de Projen
- La versión 3.9.16 o posterior de Python

Limitaciones

- Los trabajos simultáneos están limitados a 500 tareas por minuto, que es el número máximo de tareas que Fargate puede aprovisionar.

Arquitectura

El siguiente diagrama muestra la interacción de la API de trabajos con la tabla `jobs` Amazon DynamoDB, el servicio Fargate de procesamiento de eventos y la función de gestión de errores. AWS Lambda Los eventos se almacenan en un archivo de EventBridge eventos de Amazon.

Un flujo de trabajo habitual incluye los siguientes pasos:

1. Usted se autentica con AWS Identity and Access Management (IAM) y obtiene las credenciales de seguridad.
2. Envía una solicitud `POST` HTTP al punto de conexión de la API de trabajos `/jobs`, especificando los parámetros del trabajo en el cuerpo de la solicitud.
3. La API de trabajos, que es una API de REST de API Gateway, le devuelve una respuesta HTTP que contiene el identificador del trabajo.
4. La API de trabajos envía un mensaje a la cola de SQS.
5. Fargate extrae el mensaje de la cola de SQS, procesa el evento y, a continuación, agrega los resultados del trabajo a la tabla `jobs` de DynamoDB.
6. Envía una solicitud `GET` HTTP al punto de conexión de la API de trabajos `/jobs/{jobId}`, con el identificador de trabajo del paso 3 como `{jobId}`.
7. La API de trabajos consulta la tabla `jobs` de DynamoDB para recuperar los resultados del trabajo.
8. La API de trabajos devuelve una respuesta HTTP que contiene los resultados del trabajo.
9. Si el procesamiento de eventos falla, la cola de SQS envía el evento a la cola de mensajes fallidos (DLQ).

10. Un EventBridge evento inicia la función de gestión de errores.
11. La función de gestión de errores agrega los parámetros del trabajo a la tabla `jobs` de DynamoDB.
12. Puede recuperar los parámetros del trabajo enviando una solicitud `GET` HTTP al punto de conexión de la API de trabajos `/jobs/{jobId}`.
13. Si la gestión de errores falla, la función de gestión de errores envía el evento a un archivo. EventBridge

    Puede reproducir los eventos archivados utilizando. EventBridge

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir y aprovisionar la Nube de AWS infraestructura en código.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- AWS Fargatele ayuda a ejecutar contenedores sin necesidad de gestionar servidores o instancias de Amazon Elastic Compute Cloud (Amazon EC2). Se utiliza en conjunto con Amazon Elastic Container Service (Amazon ECS).
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, funciones de Lambda, puntos de conexión de invocación HTTP que utilizan destinos de API o buses de eventos en otras Cuentas de AWS.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.

Otras herramientas

- autopep8 formatea automáticamente el código de Python según la guía de estilo Python Enhancement Proposal (PEP) 8.

- Bandit analiza el código de Python para detectar problemas de seguridad comunes.
- Commitizen un verificador de confirmaciones y generador de `CHANGELOG` de Git.
- cfn-lint es un linter AWS CloudFormation
- Checkov es una herramienta de análisis de código estático que revisa si la infraestructura como código (IaC) se ha configurado mal en términos de seguridad y cumplimiento.
- jq es una herramienta de línea de comandos para analizar JSON.
- Postman es una plataforma de API.
- pre-commit es un administrador de enlaces de Git.
- Projen es un generador de proyectos.
- pytest es un marco de Python para escribir pruebas pequeñas y legibles.

Repositorio de código

Este ejemplo de código de arquitectura se encuentra en el repositorio de SQS y procesamiento GitHub asíncrono con API Gateway.

Prácticas recomendadas

- Esta arquitectura de ejemplo no incluye la supervisión de la infraestructura implementada. Si su caso de uso requiere supervisión, evalúe la posibilidad de agregar CDK Monitoring Constructs u otra solución de supervisión.
- Esta arquitectura de ejemplo usa permisos de IAM para controlar el acceso a la API de trabajos. Cualquier persona autorizada a asumir `JobsAPIInvokeRole` podrá invocar la API de trabajos. Como tal, el mecanismo de control de acceso es binario. Si su caso de uso requiere un modelo de autorización más complejo, evalúe la posibilidad de usar un mecanismo de control de acceso diferente.
- Cuando un usuario envía una solicitud `POST` HTTP al punto de conexión de la API de trabajos `/jobs`, los datos de entrada se validan en dos niveles diferentes:
  - API Gateway se encarga de la validación de la primera solicitud.
  - La función de procesamiento de eventos realiza la segunda solicitud.

    No se hace ninguna validación cuando el usuario realiza una solicitud `GET` HTTP al punto de conexión de la API de trabajos `/jobs/{jobId}`. Si su caso de uso requiere una validación de entrada adicional y un mayor nivel de seguridad, evalúe su uso AWS WAF para proteger su API.

Epics

Configuración del entorno

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Para clonar el repositorio localmente, use el siguiente comando: `git clone https://github.com/aws-samples/asynchronous-event-processing-api-gateway-sqs-cdk.git`	DevOps ingeniero

Configure el proyecto.	Cambie el directorio a la raíz del repositorio y configure el entorno virtual de Python y todas las herramientas mediante Projen:
	`cd asynchronous-event-processing-api-gateway-api-gateway-sqs-cdk`
	`npx projen`
		DevOps ingeniero

Instale enlaces de pre-commit.	Para instalar enlaces de pre-commit, haga lo siguiente: 1. Active el entorno virtual Python: `source .env/bin/activate` 2. Instale los enlaces de pre-commit:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`pre-commit install` `pre-commit install --hook-type commit-msg`	

Implementación de la arquitectura de ejemplo

Tarea	Descripción	Habilidades requeridas
Bootstrap. AWS CDK	Para arrancar AWS CDK Cuenta de AWS, ejecuta el siguiente comando: `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen bootstrap`	AWS DevOps
Implemente la arquitectura de ejemplo.	Para implementar la arquitectura de ejemplo en su Cuenta de AWS servidor, ejecute el siguiente comando: `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen deploy`	AWS DevOps

Prueba de la arquitectura

Tarea	Descripción	Habilidades requeridas
Instale los requisitos previos de prueba.	Instale en su estación de trabajo AWS Command Line Interface (AWS CLI), Postman y jq.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Se sugiere usar Postman para probar esta arquitectura de ejemplo, pero no es obligatorio. Si elige una herramienta para probar API alternativa, asegúrese de que sea compatible con la autenticación de AWS Signature Version 4 y consulte los puntos de conexión de la API expuestos, que se pueden inspeccionar exportando la API de REST.	

Tarea	Descripción	Habilidades requeridas
Asuma el `JobsAPIInvokeRole` .	Asuma el `JobsAPIInvokeRole` que apareció en la salida del comando `deploy`: `CREDENTIALS=$(AWS_PROFILE=$<YOUR_AWS_PROFILE> aws sts assume-role \ --no-cli-pager \ --role-arn $<JOBS_API_INVOKE_ROLE_ARN> \ --role-session-name JobsAPIInvoke) export AWS_ACCESS_KEY_ID=$(cat $CREDENTIALS \| jq '.Credentials''.AccessKeyId') export AWS_SECRET_ACCESS_KEY=$(cat $CREDENTIALS \| jq '.Credentials''.SecretAccessKey') export AWS_SESSION_TOKEN==$(cat $CREDENTIALS | jq '.Credentials''.SessionToken')`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

Configure Postman.	• Para importar la colección de Postman que se incluye en el repositorio, siga las instrucciones de la documentación de Postman.
	• Defina las variables de `JobsAPI` con los siguientes valores:
	  • `accessKey` : el valor del atributo `Credentials.AccessKeyId` del comando `assume-role` .
	  • `baseUrl`: el valor de la salida de `JobsApiJobsAPIEndpoint` del comando `deploy` sin la barra diagonal final.
	  • `region`– El valor del Región de AWS lugar en el que implementó la arquitectura de ejemplo.
	  • `seconds`: el valor de un parámetro de entrada para el trabajo de ejemplo. Debe ser un entero positivo.
	  • `secretKey` : el valor del atributo `Credentials.SecretAccessKey` del comando `assume-role` .
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• `sessionToken` : el valor del atributo `Credentials.SessionToken` del comando `assume-role` .	
Pruebe la arquitectura de ejemplo.	Para probar la arquitectura de ejemplo, envíe solicitudes a la API de trabajos. Para obtener más información, consulte la documentación de Postman.	DevOps ingeniero

Resolución de problemas

Problema	Solución
La destrucción y posterior redespliegue de la arquitectura de ejemplo fallan porque el grupo de CloudWatch registros de Amazon Logs `/aws/apigateway/JobsAPIAccessLogs` ya existe.	1. Si es necesario, exporte los datos de registro a Amazon Simple Storage Service (Amazon S3). 2. Elimine el grupo CloudWatch de registros `/aws/apigateway/JobsAPIAccessLogs`. 3. Vuelva a implementar la arquitectura de ejemplo.
La destrucción y posterior redespliegue de la arquitectura del ejemplo fallan porque el grupo de CloudWatch registros `/aws/ecs/EventProcessingServiceLogs` ya existe.	1. Si es necesario, exporte los datos de registro a Amazon S3. 2. Elimine el grupo de CloudWatch registros `/aws/ecs/EventProcessingServiceLogs`. 3. Vuelva a implementar la arquitectura de ejemplo.

Recursos relacionados

- Plantilla de mapeo de API Gateway y referencia de variables de registro de acceso
- ¿Cómo integro una API de REST de API Gateway con Amazon SQS y soluciono los errores comunes?

Puesta en marcha de las tareas de Automatización de AWS Systems Manager de forma sincrónica desde AWS Step Functions

Elie El khoury, Amazon Web Services

Resumen

Este patrón explica cómo integrarse AWS Step Functions con AWS Systems Manager. Utiliza las integraciones de servicios del AWS SDK para llamar a la startAutomationExecutionAPI de Systems Manager con un token de tarea de un flujo de trabajo de una máquina de estado y se detiene hasta que el token regresa con una llamada correcta o errónea. Para demostrar la integración, este patrón implementa un encapsulador de documentos (manuales de procedimientos) de Automatización en torno a los documentos `AWS-RunShellScript` o `AWS-RunPowerShellScript`; además, usa `.waitForTaskToken` para llamar de forma sincrónica a `AWS-RunShellScript` o `AWS-RunPowerShellScript`. Para obtener más información sobre las integraciones de servicios del AWS SDK en Step Functions, consulta la Guía para AWS Step Functions desarrolladores.

Step Functions es un servicio de flujo de trabajo visual de bajo código que puede utilizar para crear aplicaciones distribuidas, automatizar los procesos empresariales y de TI y crear canalizaciones de datos y aprendizaje automático mediante AWS el uso de servicios. Los flujos de trabajo gestionan los errores, los reintentos, la paralelización, las integraciones de servicios y la observabilidad para que pueda centrarse en una lógica empresarial de mayor valor.

La automatización, una capacidad de AWS Systems Manager, simplifica las tareas comunes de mantenimiento, implementación y corrección para empresas Servicios de AWS como Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS), Amazon Redshift y Amazon Simple Storage Service (Amazon S3). Automation le ofrece un control granular sobre la concurrencia de sus automatizaciones. Por ejemplo, puede especificar a cuántos recursos desea dirigirse simultáneamente y cuántos errores pueden producirse antes de que se detenga una automatización.

Para obtener detalles sobre la implementación, incluidos los pasos, parámetros y ejemplos del manual de procedimientos, consulte la sección Información adicional.

Requisitos previos y limitaciones

Requisitos previos

- AWS Una cuenta activa
- AWS Identity and Access Management (IAM) para acceder a Step Functions y Systems Manager
- Una EC2 instancia con el Agente Systems Manager (SSM Agent) instalado en la instancia
- Un perfil de instancia de IAM para Systems Manager adjunto a la instancia en la que planea ejecutar el manual de procedimientos
- Un rol de Step Functions que tenga los siguientes permisos de IAM (que sigan el principio de privilegio mínimo):

```
{
            "Effect": "Allow",
            "Action": "ssm:StartAutomationExecution",
            "Resource": "*"
 }
```

Versiones de producto

- Versión de esquema de documento de SSM 0.3 o posterior
- SSM Agent versión 2.3.672.0 o posterior

Arquitectura

Pila de tecnología de destino

- AWS Step Functions
- AWS Systems Manager Automation

Arquitectura de destino

Automatización y escala

- Este patrón proporciona una AWS CloudFormation plantilla que puede usar para implementar los manuales de ejecución en varias instancias. (Consulte el repositorio de implementación de GitHub Step Functions y Systems Manager).

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y administrarlos a lo largo de su ciclo de vida en todas Cuentas de AWS las regiones.
- AWS Identity and Access Management (IAM) lo ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Step Functionses un servicio de organización sin servidor que le ayuda a combinar AWS Lambda funciones y otras Servicios de AWS para crear aplicaciones esenciales para la empresa.
- AWS Systems Manager lo ayuda a administrar las aplicaciones y la infraestructura que se ejecutan en la Nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo necesario para detectar y resolver problemas operativos y le ayuda a administrar sus recursos de forma segura y a escala. AWS

Código

El código de este patrón está disponible en el repositorio de implementación de GitHub Step Functions y Systems Manager.

Epics

Creación de manuales de procedimientos

Tarea	Descripción	Habilidades requeridas
Descargue la CloudFormation plantilla.	Descarga la `ssm-automation-documents.cfn.json` plantilla de la `cloudformation` carpeta del GitHub repositorio.	AWS DevOps
Cree manuales de procedimientos.	Inicie sesión en Consola de administración de AWS, abra la CloudFormation consola e implemente la plantilla. Para obtener más información sobre la implementación	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	de CloudFormation plantillas, consulte Crear una pila en la CloudFormation consola en la CloudFormation documentación. La CloudFormation plantilla implementa tres recursos: • `SfnRunCommandByInstanceIds` — Runbook que te permite ejecutar `AWS-RunShellScript` o usar una `AWS-RunPowerShellScript` instancia. IDs • `SfnRunCommandByTargets` : manual de procedimientos que le permite poner en marcha `AWS-RunShellScript` o `AWS-RunPowerShellScript` usando destinos. • `SSMSyncRole` : el rol de IAM que asumen los manuales de procedimientos.	

Crear una máquina de estado de muestra

Tarea	Descripción	Habilidades requeridas
Crear una máquina de estado de prueba.	Siga las instrucciones de la Guía para desarrolladores	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	de AWS Step Functions para crear y poner en marcha una máquina de estados. Para la definición, utilice el siguiente código. Asegúrese de actualizar el valor `InstanceIds` con el ID de una instancia válida habilitada para Systems Manager en su cuenta. `{ "Comment": "A description of my state machine", "StartAt": "StartAutomationWaitForCallBack", "States": { "StartAutomationWaitForCallBack": { "Type": "Task", "Resource": "arn:aws:states:::aws-sdk:ssm:startAutomationExecution.waitForTaskToken", "Parameters": { "DocumentName": "SfnRunCommandByInstanceIds", "Parameters": { "InstanceIds": ["i-1234567890abcdef0"], "taskToken.$": "States.Array($$.Task.Token)",`	

Tarea	Descripción	Habilidades requeridas

```
          "workingD
irectory": [
            "/home/ssm-
user/"
          ],
          "Commands": [
            "echo \"This
 is a test running
 automation waitForTa
skToken\" >> automatio
n.log",
            "sleep 100"
          ],
          "executio
nTimeout": [
              "10800"
          ],
          "delivery
Timeout": [
              "30"
          ],
          "shell": [
              "Shell"
          ]
            }
      },
      "End": true
    }
  }
}
```

Este código llama al manual de procedimientos para ejecutar dos comandos que demuestran la llamada `waitForTaskToken` a Systems Manager Automation.

El valor del parámetro `shell` (`Shell` o `PowerShell`)

Tarea	Descripción	Habilidades requeridas
	determina si el documento de Automatización se pone en marcha en `AWS-RunShellScript` o `AWS-RunPowerShellScript`. La tarea escribe en el `/home/ssm-user/automation.log` archivo «Se trata de un waitForTask token de automatización en ejecución de pruebas» y, a continuación, se suspende durante 100 segundos antes de responder con el token de la tarea y lanzar la siguiente tarea del flujo de trabajo. Si, en vez de eso, quiere llamar al manual de procedimientos `SfnRunCommandByTargets`, sustituya la sección `Parameters` del código anterior por la siguiente: `"Parameters": { "Targets": [ { "Key": "InstanceIds", "Values": [ "i-02573cafcfEXAMPLE",`	

Tarea	Descripción	Habilidades requeridas

	<pre>"i-0471e04240EXAMPLE"
	]
	}
	],</pre>	

Actualice el rol de IAM de la máquina de estado.	El paso anterior crea automáticamente un rol de IAM dedicado para la máquina de estados. Sin embargo, no concede permisos para llamar al manual de procedimientos. Actualice el rol añadiendo los permisos siguientes:
	<pre>{
	"Effect": "Allow",
	"Action":
	"ssm:StartAutomati
	onExecution",
	"Resource": "*"
	}</pre>
		AWS DevOps

Valide las llamadas sincrónic as.	Ejecute la máquina de estados para validar la llamada sincrónica entre Step Functions y Systems Manager Automation. Para ver un ejemplo de salida, consulte la sección Informaci ón adicional.	AWS DevOps

Recursos relacionados

- Cómo empezar con AWS Step Functions (Guía para AWS Step Functions desarrolladores)

- Espere a que le devuelvan la llamada con el token de la tarea (guía para AWS Step Functions desarrolladores, patrones de integración de servicios)
- Llamadas a las API send_task_success y send_task_failure (documentación de Boto3)
- AWS Systems Manager Automatización (guía AWS Systems Manager del usuario)

Información adicional

Detalles de la implementación

Este patrón proporciona una CloudFormation plantilla que despliega dos manuales de ejecución de Systems Manager:

- `SfnRunCommandByInstanceIds`ejecuta el `AWS-RunPowerShellScript` comando `AWS-RunShellScript` o mediante la instancia. IDs
- `SfnRunCommandByTargets` pone en marcha el comando `AWS-RunShellScript` o `AWS-RunPowerShellScript` usando destinos.

Cada manual de procedimientos implementa cuatro pasos para lograr una llamada sincrónica cuando se usa la opción `.waitForTaskToken` de Step Functions.

Paso	Action	Description (Descripción)
1	`Branch`	Comprueba el valor del parámetro `shell` (`Shell` o `PowerShell`) para decidir si poner en marcha `AWS-RunShellScript` en Linux o `AWS-RunPowerShellScript` en Windows.
2	`RunCommand_Shell` o `RunCommand_PowerShell`	Recibe varias entradas y pone en marcha el comando `RunShellScript` o `RunPowerShellScript` . Para obtener más información, consulte la pestaña Detalles de `RunCommand_Shell`

		o `RunCommand_PowerShell` del documento de Automatización en la consola de Systems Manager.
3	`SendTaskFailure`	Se ejecuta cuando se anula o cancela el paso 2. Llama a la API send_task_failure de Step Functions, que acepta tres parámetros como entrada: el token pasado por la máquina de estados, el error de error y una descripción de la causa del error.
4	`SendTaskSuccess`	Se ejecuta cuando el paso 2 se realiza correctamente. Llama a la API send_task_success de Step Functions, que acepta el token pasado por la máquina de estados como entrada.

Parámetros del manual de procedimientos

Manual de procedimientos `SfnRunCommandByInstanceIds`:

Nombre del parámetro	Tipo	Opcional u obligatorio	Description (Descripción)
`shell`	Cadena	Obligatorio	El intérprete de comandos de las instancias para decidir si poner en marcha `AWS-RunShellScript` para Linux o `AWS-RunPo`

			werShellScript para Windows.
deliveryTimeout	Entero	Opcional	La cantidad, en segundos, de espera para que un comando se envíe a SSM Agent de una instancia. Este parámetro tiene un valor mínimo de 30 (0,5 minutos) y un valor máximo de 2 592 000 (720 horas).
executionTimeout	Cadena	Opcional	El tiempo, en segundos, para que un comando se complete antes de considerar que se ha producido un error. El valor predeterminado es de 3600 (1 hora). El valor máximo es 172800 (48 horas).
workingDirectory	Cadena	Opcional	La ruta al directorio de trabajo en la instancia .
Commands	StringList	Obligatorio	El script o comando del intérprete de comandos que se va a ejecutar.

`InstanceIds`	StringList	Obligatorio	La IDs de las instancias en las que desea ejecutar el comando.
`taskToken`	Cadena	Obligatorio	El token de tarea que se utilizará para las respuesta s de devolución de llamada.

Manual de procedimientos `SfnRunCommandByTargets`:

Name	Tipo	Opcional u obligatorio	Description (Descripc ión)
`shell`	Cadena	Obligatorio	El intérprete de comandos de las instancias para decidir si poner en marcha `AWS-RunSh ellScript` para Linux o `AWS-RunPo werShellScript` para Windows.
`deliveryTimeout`	Entero	Opcional	La cantidad, en segundos, de espera para que un comando se envíe a SSM Agent de una instancia. Este parámetro tiene un valor mínimo de 30 (0,5 minutos) y un valor máximo

			de 2 592 000 (720 horas).
`executionTimeout`	Entero	Opcional	El tiempo, en segundos, para que un comando se complete antes de considerar que se ha producido un error. El valor predeterminado es de 3600 (1 hora). El valor máximo es 172800 (48 horas).
`workingDirectory`	Cadena	Opcional	La ruta al directorio de trabajo en la instancia.
`Commands`	StringList	Obligatorio	El script o comando del intérprete de comandos que se va a ejecutar.

`Targets`	MapList	Obligatorio	Una matriz de criterios de búsqueda que identifica las instancias utilizando los pares clave-valor que usted especifique. Por ejemplo: `[{"Key":"InstanceIds","Values":["i-02573cafcfEXAMPLE","i-0471e04240EXAMPLE"]}]`
`taskToken`	Cadena	Obligatorio	El token de tarea que se utilizará para las respuestas de devolución de llamada.

Resultados de ejemplo

La siguiente tabla proporciona un ejemplo de salida de la función step. Muestra que el tiempo total de ejecución es superior a 100 segundos entre el paso 5 (`TaskSubmitted`) y el paso 6 (`TaskSucceeded`). Esto demuestra que la función de Step Functions esperó a que finalizara el comando `sleep 100` antes de pasar a la siguiente tarea del flujo de trabajo.

ID	Tipo	Paso	Recurso	Tiempo transcurrido (ms)	Timestamp
1	`ExecutionStarted`		-	0	11 de marzo de 2022

					02:50:34.303 p.m.
2	TaskStateEntered	StartAutomationWaitForCallBack	-	40	11 de marzo de 2022 02:50:34.343 p.m.
3	TaskScheduled	StartAutomationWaitForCallBack	-	40	11 de marzo de 2022 02:50:34.343 p.m.
4	TaskStarted	StartAutomationWaitForCallBack	-	154	11 de marzo de 2022 02:50:34.457 p.m.
5	TaskSubmitted	StartAutomationWaitForCallBack	-	657	11 de marzo de 2022 02:50:34.960 p.m.
6	TaskSucceeded	StartAutomationWaitForCallBack	-	103835	11 de marzo de 2022 02:52:18.138 p.m.
7	TaskStateExited	StartAutomationWaitForCallBack	-	103860	11 de marzo de 2022 02:52:18.163 p.m.
8	ExecutionSucceeded		-	103897	11 de marzo de 2022 02:52:18.200 p.m.

Ejecute lecturas paralelas de objetos S3 mediante Python en una AWS Lambda función

Eduardo Bortoluzzi, Amazon Web Services

Resumen

Puede utilizar este patrón para recuperar y resumir una lista de documentos de buckets de Amazon Simple Storage Service (Amazon S3) en tiempo real. El patrón proporciona código de ejemplo para leer en paralelo objetos de buckets de S3 en Amazon Web Services (AWS). El patrón muestra cómo ejecutar eficientemente tareas I/O enlazadas con AWS Lambda funciones usando Python.

Una empresa financiera utilizó este patrón en una solución interactiva para aprobar o rechazar manualmente las transacciones financieras correlacionadas en tiempo real. Los documentos de las transacciones financieras se almacenaron en un bucket de S3 relacionado con el mercado. Un operador seleccionó una lista de documentos del bucket de S3, analizó el valor total de las transacciones calculadas por la solución y decidió aprobar o rechazar el lote seleccionado.

Las tareas vinculadas a operacioness de E/S admiten varios subprocesos. En este código de ejemplo, el concurrent.futures. ThreadPoolExecutorse utiliza con un máximo de 30 subprocesos simultáneos, aunque las funciones Lambda admiten hasta 1024 subprocesos (uno de los cuales es el proceso principal). Este límite se debe a que demasiados subprocesos crean problemas de latencia debido al cambio de contexto y al uso de los recursos de computación. También es necesario aumentar el número máximo de conexiones del grupo en `botocore` para que todos los subprocesos puedan descargar el objeto de S3 de forma simultánea.

El código de ejemplo usa un objeto de 8,3 KB, con datos JSON en un bucket de S3. El objeto se lee varias veces. Cuando la función de Lambda lee el objeto, los datos JSON se decodifican en un objeto de Python. En diciembre de 2024, el resultado tras ejecutar este ejemplo fue de 1000 lecturas procesadas en 2,3 segundos y 10 000 lecturas procesadas en 27 segundos mediante una función Lambda configurada con 2304 MB de memoria. AWS Lambda admite configuraciones de memoria de 128 MB a 10 240 MB (10 GB), aunque aumentar la memoria Lambda a más de 2304 MB no ayudó a reducir el tiempo de ejecución de esta tarea específica vinculada a la E/S.

La herramienta AWS Lambda Power Tuning se utilizó para probar diferentes configuraciones de memoria Lambda y verificar la mejor performance-to-cost relación para la tarea. Para obtener más información, consulte la sección Información adicional.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Competencia en desarrollo con Python.

Limitaciones

- Una función de Lambda puede tener como máximo 1024 procesos o subprocesos de puesta en marcha.
- Cuentas de AWS Los nuevos tienen un límite de memoria Lambda de 3.008 MB. Ajuste la herramienta de ajuste AWS Lambda de potencia en consecuencia. Para obtener más información, consulte la sección Solución de problemas.
- Amazon S3 tiene un límite de 5500 GET/HEAD solicitudes por segundo por prefijo particionado.

Versiones de producto

- Python 3.9 o posterior
- AWS Cloud Development Kit (AWS CDK) v2
- AWS Command Line Interface (AWS CLI) versión 2
- AWS Lambda Power Tuning 4.3.6 (opcional)

Arquitectura

Pila de tecnología de destino

- AWS Lambda
- Amazon S3
- AWS Step Functions (si se ha implementado AWS Lambda Power Tuning)

Arquitectura de destino

En el siguiente diagrama, se muestra una función de Lambda que lee objetos de un bucket de S3 en paralelo. El diagrama también incluye un flujo de trabajo de Step Functions para que la

herramienta AWS Lambda Power Tuning ajuste con precisión la memoria de funciones Lambda. Este refinamiento permite lograr un buen equilibrio entre el costo y el rendimiento.

Automatización y escala

Las funciones de Lambda se escalan rápidamente cuando es necesario. Para evitar los errores 503 de ralentización de Amazon S3 cuando hay mucha demanda, le recomendamos que ponga algunos límites al escalado.

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK) v2 es un marco de desarrollo de software que le ayuda a definir y aprovisionar la Nube de AWS infraestructura en código. La infraestructura de ejemplo se creó para implementarla con AWS CDK.
- AWS Command Line InterfaceAWS CLIes una herramienta de código abierto que le ayuda a interactuar Servicios de AWS mediante comandos en su shell de línea de comandos. En este patrón, la AWS CLI versión 2 se utiliza para cargar un archivo JSON de ejemplo.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le permite almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Step Functionses un servicio de organización sin servidor que le ayuda a combinar AWS Lambda funciones y otros servicios de AWS para crear aplicaciones críticas para la empresa.

Otras herramientas

- Python es un lenguaje de programación informático de uso general. La reutilización de subprocesos de trabajo inactivos se introdujo en la versión 3.8 de Python, y el código de la función de Lambda de este patrón se creó para la versión 3.9 y posteriores de Python.

Repositorio de código

El código de este patrón está disponible en el repositorio. aws-lambda-parallel-download GitHub

Prácticas recomendadas

- Esta AWS CDK construcción se basa en sus permisos Cuenta de AWS de usuario para implementar la infraestructura. Si tienes pensado usar AWS CDK Pipelines o despliegues multicuenta, consulta los sintetizadores Stack.
- Esta aplicación de ejemplo no tiene habilitados los registros de acceso en el bucket de S3. Se recomienda habilitar los registros de acceso en el código de producción.

Epics

Preparación del entorno de desarrollo

Tarea	Descripción	Habilidades requeridas
Compruebe la versión instalada de Python.	Este código se probó específicamente en Python 3.9 y Python 3.13, y debería funcionar en todas las versiones entre estas versiones. Para comprobar su versión de Python, use el comando `python3 -V` en su terminal e instale una versión más reciente si es necesario. Para verificar que los módulos necesarios estén instalados, use `python3 -c "import pip, venv"`. Si no aparece ningún mensaje de error, significa que los módulos están instalados correctamente y que todo está listo para poner en marcha este ejemplo.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Instala. AWS CDK	Para instalarlo AWS CDK si aún no está instalado, siga las instrucciones que aparecen en Introducción al AWS CDK. Para confirmar que la AWS CDK versión instalada es 2.0 o posterior, ejecute`cdk --version`.	Arquitecto de la nube
Arranque su entorno de .	Para arrancar su entorno, si aún no lo ha hecho, siga las instrucciones de Bootstrap your environment for use with the AWS CDK.	Arquitecto de la nube

Clonación del repositorio de ejemplo

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Para instalar la versión más reciente del repositorio, use el siguiente comando: `git clone --depth 1 --branch v1.2.0 \ git@github.com:aws-samples/aws-lambda-parallel-download.git`	Arquitecto de la nube
Cambie el directorio de trabajo al repositorio clonado.	Use el siguiente comando: `cd aws-lambda-parallel-download`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Cree un entorno virtual de Python.	Para crear un entorno virtual de Python, use el siguiente comando: `python3 -m venv .venv`	Arquitecto de la nube
Active el entorno virtual.	Para activar el entorno virtual, puede usar el siguiente comando: `source .venv/bin/activate`	Arquitecto de la nube
Instalar las dependencias.	Para instalar las dependencias de Python, use el comando `pip`: `pip install -r requirements.txt`	Arquitecto de la nube
Examine el código.	(Opcional) El código de ejemplo que descarga un objeto del bucket de S3 está en `resources/parallel.py`. El código de la infraestructura está en la carpeta `parallel_download`.	Arquitecto de la nube

Implementación y pruebas de la aplicación

Tarea	Descripción	Habilidades requeridas
Implemente la aplicación.	Ejecute `cdk deploy`.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Anote los AWS CDK resultados: • `ParallelDownloadStack.LambdaFunctionARN` • `ParallelDownloadStack.SampleS3BucketName` • `ParallelDownloadStack.StateMachineARN`	
Cargue un archivo JSON de ejemplo.	El repositorio contiene un archivo JSON de ejemplo de unos 9 KB. Para cargar el archivo en el bucket de S3 de la pila creada, use el siguiente comando: `aws s3 cp sample.json s3://<ParallelDownloadStack.SampleS3BucketName>` Reemplace `<ParallelDownloadStack.SampleS3BucketName>` con el valor correspondiente de la AWS CDK salida.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Ejecute la aplicación.	Para poner en marcha la aplicación, haga lo siguiente: 1. Inicie sesión en Consola de administración de AWS, vaya a la consola de Lambda y localice la función Lambda que tiene el ARN en la salida. AWS CDK `ParallelDownloadStack.LambdaFunctionARN` 2. En la pestaña Probar, cambie el Evento JSON por el siguiente: `{"objectKey": "sample.json"}` 3. Seleccione Probar 4. En el cuadro de resultados, elija Detalles. Los detalles mostrarán las estadísticas de la descarga paralela, la información de la puesta en marcha y los registros.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Agregue el número de descargas.	(Opcional) Para poner en marcha 1500 llamadas a get object, use el siguiente JSON en Evento JSON del parámetro `Test`: `{"repeat": 1500, "objectKey": "sample.json"}`	Arquitecto de la nube

Opcional: ejecute Power Tuning AWS Lambda

Tarea	Descripción	Habilidades requeridas
Ejecute la herramienta AWS Lambda de ajuste de potencia.	1. Inicie sesión en la consola y vaya a Step Functions. 2. Localice la máquina de estados con el ARN de la AWS CDK salida. `ParallelDownloadStack.StateMachineARN` 3. Seleccione Iniciar la ejecución y pegue el siguiente JSON: `{ "lambdaARN": "<ParallelDownloadStack.LambdaFunctionARN>", "num": 10, "strategy": "balanced",`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas

	<pre>"payload":
	{"repeat": 2000,
	"objectKey":
	"sample.json"}
	}</pre>
	Recuerde `<ParallelDownloadStack.LambdaFunctionARN>` reemplazarla por el valor de la AWS CDK salida.
	
	Al final de la ejecución, el resultado aparecerá en la pestaña Entrada y salida de ejecución.	

Vea los resultados del ajuste de AWS Lambda potencia en un gráfico.	En la pestaña Entrada y salida de ejecución, copie el enlace de la propiedad `visualization` y péguelo en una nueva pestaña del navegador.	Arquitecto de la nube

Limpieza

Tarea	Descripción	Habilidades requeridas

Elimine los objetos del bucket de S3.	Antes de destruir los recursos implementados, debe eliminar todos los objetos del bucket de S3:
	
	<pre>aws s3 rm s3://<ParallelDownloadStack.SampleS3BucketName>
	\</pre>
		Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	`--recursive` Recuerde `<ParallelDownloadStack.SampleS3BucketName>` sustituir por el valor de las AWS CDK salidas.	
Destruya los recursos.	Para destruir todos los recursos que se hayan creado para este piloto, use el siguiente comando: `cdk destroy`	Arquitecto de la nube

Resolución de problemas

Problema	Solución
`'MemorySize' value failed to satisfy constraint: Member must have value less than or equal to 3008`	En el caso de las cuentas nuevas, es posible que no pueda configurar más de 3008 MB en las funciones de Lambda. Para probar con AWS Lambda Power Tuning, añada la siguiente propiedad en el JSON de entrada al iniciar la ejecución de Step Functions: `"powerValues": [ 512, 1024, 1536, 2048, 2560, 3008 ]`

Recursos relacionados

- Python: futuros simultáneos. ThreadPoolExecutor
- Cuotas de Lambda: Configuración, implementación y ejecución de funciones
- Trabajando con el AWS CDK en Python
- Funciones de creación de perfiles con AWS Lambda Power Tuning

Información adicional

Código

El siguiente fragmento de código realiza el procesamiento paralelo I/O :

```
with ThreadPoolExecutor(max_workers=MAX_WORKERS) as executor:
  for result in executor.map(a_function, (the_arguments)):
    ...
```

`ThreadPoolExecutor` reutiliza los subprocesos cuando están disponibles.

Pruebas y resultados

Estas pruebas se realizaron en diciembre de 2024.

La primera prueba procesó 2500 lecturas de objetos, con el siguiente resultado:

A partir de 3009 MB, el nivel de tiempo de procesamiento se mantuvo prácticamente igual para cualquier incremento de memoria, pero el costo se hacía mayor a medida que aumentaba el tamaño de la memoria.

En otra prueba, se investigó el intervalo entre 1536 MB y 3072 MB de memoria. Se utilizaron valores que eran múltiplos de 256 MB y se procesaron 10 000 lecturas de objetos; los resultados son los siguientes:

La mejor performance-to-cost relación fue con la configuración Lambda de 2.304 MB de memoria.

A modo de comparación, un proceso secuencial de 2500 lecturas de objetos tardó 47 segundos. El proceso paralelo con la configuración de Lambda de 2304 MB tardó 7 segundos, lo que supone un 85 por ciento menos.

Envíe datos de telemetría desde y AWS Lambda OpenSearch para análisis y visualización en tiempo real

Tabby Ward, Guy Bachar y David Kilzer, Amazon Web Services

Resumen

Las aplicaciones modernas están cada vez más distribuidas y se basan cada vez más en eventos, lo que refuerza la necesidad de monitoreo y observabilidad en tiempo real. AWS Lambda es un servicio de computación sin servidor que desempeña un papel crucial en la creación de arquitecturas escalables y basadas en eventos. Sin embargo, la supervisión y la solución de problemas de las funciones de Lambda pueden resultar complicadas si se confía únicamente en Amazon CloudWatch Logs, que puede introducir latencia y períodos de retención limitados.

Para abordar este desafío, AWS presentó la API de telemetría Lambda, que permite a las funciones de Lambda enviar datos de telemetría directamente a herramientas de monitoreo y observabilidad de terceros. Esta API admite la transmisión en tiempo real de registros, métricas y seguimientos, y proporciona una visión completa y puntual del rendimiento y el estado de las funciones de Lambda.

Este patrón explica cómo integrar la API de telemetría Lambda con OpenSearchun motor de búsqueda y análisis distribuido de código abierto. OpenSearch ofrece una plataforma potente y escalable para la ingesta, el almacenamiento y el análisis de grandes volúmenes de datos, lo que la convierte en la opción ideal para los datos de telemetría Lambda. En concreto, este patrón muestra cómo enviar registros desde una función de Lambda escrita en Python directamente a un OpenSearch clúster mediante una extensión de Lambda proporcionada por. AWS Esta solución es flexible y personalizable, por lo que puede crear su propia extensión de Lambda o modificar el código fuente del ejemplo para cambiar el formato de salida según lo desee.

El patrón explica cómo configurar y configurar la integración de la API de telemetría Lambda con OpenSearch la API de telemetría de Lambda e incluye las prácticas recomendadas en materia de seguridad, optimización de costes y escalabilidad. El objetivo es que pueda obtener información más detallada sobre las funciones de Lambda y mejorar la observabilidad general de sus aplicaciones sin servidor.

Nota: Este patrón se centra en la integración de la API de telemetría Lambda con la gestionad a. OpenSearch Sin embargo, los principios y las técnicas analizados también son aplicables a la búsqueda automática y a la búsqueda automática OpenSearch .

Requisitos previos y limitaciones

Antes de comenzar el proceso de integración, asegúrese de que cumple los requisitos previos que se indican a continuación:

Cuenta de AWS: Un activo Cuenta de AWS con los permisos adecuados para crear y administrar los siguientes recursos: AWS

- AWS Lambda
- AWS Identity and Access Management (IAM)
- Amazon OpenSearch Service (si utilizas un OpenSearch clúster gestionado)

OpenSearch clúster:

- Puede utilizar un OpenSearch clúster autogestionado existente o un servicio gestionado como OpenSearch Service.
- Si utilizas el OpenSearch Servicio, configura el OpenSearch clúster siguiendo las instrucciones de Introducción a Amazon OpenSearch Service en la documentación del OpenSearch Servicio.
- Asegúrese de que se pueda acceder al OpenSearch clúster desde la función Lambda y de que esté configurado con los ajustes de seguridad necesarios, como las políticas de acceso, el cifrado y la autenticación.
- Configure el OpenSearch clúster con las asignaciones de índices y los ajustes necesarios para ingerir los datos de telemetría de Lambda. Para obtener más información, consulta Cómo cargar datos de streaming en Amazon OpenSearch Service en la documentación del OpenSearch servicio.

Conectividad de red:

- Asegúrese de que la función Lambda tenga la conectividad de red necesaria para acceder al OpenSearch clúster. Para obtener orientación sobre cómo configurar los ajustes de la nube privada virtual (VPC), consulte Lanzar sus dominios de Amazon OpenSearch Service dentro de una VPC en la documentación del servicio. OpenSearch

Roles y políticas de IAM:

- Cree un rol de IAM con los permisos necesarios para que su función Lambda pueda acceder al clúster y acceder a OpenSearch las credenciales almacenadas en él. AWS Secrets Manager

- Adjunte las políticas de IAM adecuadas al rol, como la `AWSLambdaBasicExecutionRole` política y cualquier permiso adicional necesario para interactuar con él. OpenSearch
- Compruebe que los permisos de IAM concedidos a la función Lambda le permiten escribir datos en el clúster. OpenSearch Para obtener información sobre la administración de los permisos de IAM, consulte Definición de permisos de funciones de Lambda con un rol de ejecución en la documentación de Lambda.

Conocimientos del lenguaje de programación:

- Necesitará conocimientos básicos de Python (o del lenguaje de programación que prefiera) para comprender y modificar el código de ejemplo de la función de Lambda y la extensión de Lambda.

Entorno de desarrollo:

- Configure un entorno de desarrollo local con las herramientas y dependencias necesarias para crear e implementar funciones y extensiones de Lambda.

AWS CLI o: Consola de administración de AWS

- Instale y configure el AWS Command Line Interface (AWS CLI) o utilícelo Consola de administración de AWS con las credenciales adecuadas para interactuar con lo requerido Servicios de AWS.

Supervisión y registro:

- Familiarícese con las mejores prácticas de monitoreo y registro AWS, incluidos servicios como Amazon, CloudWatch y AWS CloudTrail con fines de monitoreo y auditoría.
- Compruebe CloudWatch los registros de su función de Lambda para identificar cualquier error o excepción relacionados con la integración de la API de telemetría de Lambda. Para obtener orientación sobre la solución de problemas, consulte la documentación de la API de telemetría de Lambda.

Arquitectura

Este patrón utiliza OpenSearch Service para almacenar registros y datos de telemetría generados por las funciones de Lambda. Este enfoque le permite transmitir rápidamente los registros

directamente a su OpenSearch clúster, lo que reduce la latencia y los costes asociados al uso de CloudWatch Logs como intermediario.

> **Note**
>
> El código de extensión de Lambda puede enviar la telemetría al OpenSearch Servicio, ya sea directamente mediante la OpenSearch API o mediante una biblioteca cliente. OpenSearch La extensión Lambda puede usar las operaciones masivas compatibles con la OpenSearch API para agrupar eventos de telemetría y enviarlos a OpenSearch Service en una sola solicitud.

El siguiente diagrama de flujo de trabajo ilustra el flujo de trabajo de registro para las funciones de Lambda cuando se utiliza un OpenSearch clúster como punto final.

La arquitectura incluye los siguientes componentes:

- Función de Lambda: función sin servidor que genera registros y datos de telemetría durante la puesta en marcha.
- Extensión Lambda: extensión basada en Python que usa la API de telemetría de Lambda para integrarse directamente con el clúster. OpenSearch Las extensiones se ponen en marcha en el mismo entorno de ejecución que la función de Lambda.
- API de telemetría de Lambda: la API que permite a las extensiones de Lambda enviar datos de telemetría, como registros, métricas y trazas, directamente a herramientas de supervisión y observabilidad de terceros.
- Clúster de Amazon OpenSearch Service: OpenSearch clúster gestionado que se aloja en AWS. Este clúster es responsable de ingerir, almacenar e indexar los datos de registro transmitidos desde la función de Lambda a través de la extensión de Lambda.

El flujo de trabajo consta de los pasos siguientes:

1. Se llama a la función de Lambda y genera registros y datos de telemetría durante su puesta en marcha.
2. La extensión de Lambda se pone en marcha junto con la función para capturar los registros y los datos de telemetría mediante la API de telemetría de Lambda.

3. La extensión Lambda establece una conexión segura con el clúster de OpenSearch servicios y transmite los datos de registro en tiempo real.
4. El clúster de OpenSearch servicios ingiere, indexa y almacena los datos de registro para que estén disponibles para su búsqueda, análisis y visualización mediante el uso de herramientas como Kibana u otras aplicaciones compatibles.

Al evitar los CloudWatch registros y enviar los datos de registro directamente al OpenSearch clúster, esta solución ofrece varias ventajas:

- Transmisión y análisis de registros en tiempo real, lo que permite una resolución de problemas más rápida y una mejor observabilidad.
- Reducción de la latencia y posibles limitaciones de retención asociadas CloudWatch a los registros.
- Flexibilidad para personalizar la extensión de Lambda o crear su propia extensión para formatos de salida específicos o procesamiento adicional.
- Integración con las capacidades de búsqueda, análisis y visualización del OpenSearch Servicio para el análisis y la supervisión de los registros.

La sección Epics proporciona step-by-step instrucciones para configurar la extensión Lambda, configurar la función Lambda e integrarla con el clúster de servicios. OpenSearch Para ver las consideraciones de seguridad, las estrategias de optimización de costos y los consejos para supervisar y solucionar problemas de la solución, consulte la sección Prácticas recomendadas.

Tools (Herramientas)

Servicios de AWS

- AWS Lambda es un servicio automático que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- Amazon OpenSearch Service es un servicio totalmente gestionado que proporciona y AWS que facilita la implementación, el funcionamiento y el escalado de OpenSearch clústeres en la nube.
- Las extensiones de Lambda amplían la funcionalidad de las funciones de Lambda al poner en marcha código personalizado junto con ellas. Puede utilizar extensiones de Lambda para integrar Lambda con varias herramientas de supervisión, observabilidad, seguridad y gobernanza.

- AWS Lambda La API de telemetría le permite usar extensiones para capturar datos mejorados de monitoreo y observabilidad directamente desde Lambda y enviarlos al destino que elija.
- CloudFormationle ayuda a modelar y configurar sus AWS recursos para que pueda dedicar menos tiempo a gestionarlos y más tiempo a centrarse en sus aplicaciones.

Repositorios de código

- AWS Lambda Extensions incluye demostraciones y proyectos de AWS muestra de AWS socios que le ayudarán a empezar a crear sus propias extensiones.
- Ejemplo de integraciones de telemetría Lambda para proporciona OpenSearch un ejemplo de extensión de Lambda que muestra cómo enviar registros desde una función de Lambda a un clúster. OpenSearch

Otras herramientas

- OpenSearches un motor de búsqueda y análisis distribuido de código abierto que proporciona una plataforma potente para la ingesta, el almacenamiento y el análisis de grandes volúmenes de datos.
- Kibana es una herramienta de exploración y visualización de datos de código abierto con la que puedes usarla. OpenSearch Tenga en cuenta que la implementación de la visualización y el análisis están fuera del alcance de este patrón. Para obtener más información, consulte la documentación de Kibana y otros recursos.

Prácticas recomendadas

Al integrar la API de telemetría Lambda con OpenSearch, tenga en cuenta las siguientes prácticas recomendadas.

Seguridad y control de acceso

- Comunicación segura: cifre todas las comunicaciones entre las funciones de Lambda y OpenSearch el clúster mediante HTTPS. Configure los SSL/TLS ajustes necesarios en la extensión y OpenSearch configuración de Lambda.
- Permisos de IAM:

  - Las extensiones se ponen en marcha en el mismo entorno de ejecución que la función de Lambda, por lo que heredan el mismo nivel de acceso a los recursos, como el sistema de archivos, las redes y las variables de entorno.
  - Otorgue los permisos de IAM mínimos necesarios a sus funciones de Lambda para acceder a la API de telemetría de Lambda y escribir datos en el clúster. OpenSearch Aplique el principio de privilegio mínimo para limitar el alcance de los permisos.
- OpenSearch control de acceso: implemente un control de acceso detallado en su OpenSearch clúster para restringir el acceso a los datos confidenciales. Utilice las funciones de seguridad integradas, como la autenticación de usuarios, el control de acceso basado en roles y los permisos a nivel de índice, en. OpenSearch
- Extensiones fiables: instale siempre las extensiones que provengan únicamente de una fuente fiable. Utilice herramientas de infraestructura como código (IaC) CloudFormation para simplificar el proceso de adjuntar la misma configuración de extensión, incluidos los permisos de IAM, a varias funciones de Lambda. Las herramientas de IaC también proporcionan un registro de auditoría de las extensiones y versiones utilizadas anteriormente.
- Gestión de información confidencial: al crear extensiones, evite registrar información confidencial. Limpie las cargas útiles y los metadatos antes de registrarlos o conservarlos con fines de auditoría.

Optimización de costos

- Supervisión y alertas: configure mecanismos de supervisión y alerta para realizar un seguimiento del volumen de datos que se envían OpenSearch desde las funciones de Lambda. Esto le permitirá identificar y abordar cualquier posible sobrecosto.
- Retención de datos: considere detenidamente el período de retención de datos adecuado para sus datos de telemetría Lambda en. OpenSearch Los periodos de retención más prolongados pueden aumentar los costos de almacenamiento, así que equilibre sus necesidades de observabilidad con la optimización de costos.
- Compresión e indexación: habilite la compresión de datos y optimice su estrategia de OpenSearch indexación para reducir el espacio de almacenamiento de sus datos de telemetría Lambda.
- Menor dependencia de CloudWatch: al integrar directamente la API de telemetría Lambda con ella OpenSearch, puede reducir potencialmente su dependencia de los CloudWatch registros, lo que puede suponer un ahorro de costes. Esto se debe a que la API de telemetría Lambda le permite enviar registros directamente a OpenSearch, lo que evita la necesidad de almacenar y procesar los datos en ella. CloudWatch

Escalabilidad y fiabilidad

- Procesamiento asíncrono: utilice patrones de procesamiento asíncrono, como Amazon Simple Queue Service (Amazon SQS) o Amazon Kinesis, para desacoplar la ejecución de la función Lambda de la ingesta de datos. OpenSearch Esto ayuda a mantener la capacidad de respuesta de las funciones de Lambda y mejora la fiabilidad general del sistema.
- OpenSearch escalado de clústeres: supervise el rendimiento y la utilización de los recursos de su OpenSearch clúster y amplíelo o reduzca según sea necesario para gestionar el creciente volumen de datos de telemetría de Lambda.
- Conmutación por error y recuperación ante desastres: implemente una estrategia sólida de recuperación ante desastres para su OpenSearch clúster, que incluya copias de seguridad periódicas y la capacidad de restaurar los datos rápidamente en caso de que se produzca un error.

Observabilidad y supervisión

- Paneles y visualizaciones: utilice Kibana u otras herramientas de paneles para crear paneles y visualizaciones personalizados que proporcionen información sobre el rendimiento y el estado de sus funciones de Lambda en función de los datos de telemetría incluidos. OpenSearch
- Alertas y notificaciones: configure alertas y notificaciones para supervisar de forma proactiva cualquier anomalía, error o problema de rendimiento en las funciones de Lambda. Integre estas alertas y notificaciones con sus procesos de administración de incidentes existentes.
- Rastreo y correlación: asegúrese de que sus datos de telemetría Lambda incluyan información de seguimiento relevante, como la IDs solicitud o la IDs correlación, para end-to-end permitir la observabilidad y la solución de problemas en sus aplicaciones distribuidas sin servidor.

Si sigue estas prácticas recomendadas, puede asegurarse de que la integración de la API de telemetría Lambda con OpenSearch es segura, rentable y escalable, y proporciona una capacidad de observación completa para sus aplicaciones sin servidor.

Epics

Creación e implementación la capa de extensión de Lambda

Tarea	Descripción	Habilidades requeridas
Descargue el código fuente.	Descargue las extensiones de ejemplo del repositorio AWS Lambda Extensions.	Desarrollador de aplicaciones, arquitecto de la nube
Vaya a la carpeta `python-example-telemetry-opensearch-extension` .	El repositorio AWS Lambda Extensions que descargó contiene numerosos ejemplos de varios casos de uso y tiempos de ejecución de varios lenguajes. Navegue hasta la carpeta python-example-telemetry-opensearch-extension para usar la OpenSearch extensión Python, que envía los registros a OpenSearch.	Desarrollador de aplicaciones, arquitecto de la nube
Agregue permisos para poner en marcha el punto de conexión de la extensión.	Use el siguiente comando para poner en marcha el punto de conexión de la extensión. `chmod +x python-example-telemetry-opensearch-extension/extension.py`	Desarrollador de aplicaciones, arquitecto de la nube
Instale las dependencias de la extensión de forma local.	Use el siguiente comando para instalar manualmente las dependencias para el código en Python:	Desarrollador de aplicaciones, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	`pip3 install -r python-example-telemetry-opensearch-extension/requirements.txt -t ./python-example-telemetry-opensearch-extension/` Estas dependencias se montarán junto con el código de la extensión.	

Cree un paquete .zip para que la extensión se implemente como una capa.	El archivo .zip de la extensión debe contener un directorio raíz denominado `extensions/`, donde se encuentra el ejecutable de la extensión, y otro directorio raíz denominado `python-example-telemetry-opensearch-extension/`, donde se encuentran la lógica central de la extensión y sus dependencias.
	
	Cree el paquete .zip para la extensión:
	
	`chmod +x extensions/python-example-telemetry-opensearch-extension`
	`zip -r extension.zip extensions python-example-telemetry-opensearch-extension`
		Desarrollador de aplicaciones, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Implemente la extensión como una capa de Lambda.	Publique la capa mediante el archivo .zip de su extensión y el siguiente comando: `aws lambda publish-layer-version \ --layer-name "python-example-telemetry-opensearch-extension" \ --zip-file "fileb://extension.zip"`	Desarrollador de aplicaciones, arquitecto de la nube

Integración de la extensión en la función

Tarea	Descripción	Habilidades requeridas
Agregue la capa a la función.	1. Inicie sesión en la página de funciones de la AWS Lambda consola Consola de administración de AWS y ábrala. 2. Seleccione su función. 3. En Layers (Capas), elija Add a layer (Añadir una capa). 4. En Elija una capa, seleccione Capas personalizadas como origen de la capa y agregue su capa. Para obtener más información sobre la adición de una capa a su función de Lambda,	Desarrollador de aplicaciones, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	consulte la documentación de Lambda.	

Tarea	Descripción	Habilidades requeridas
Configure las variables de entorno para la función.	En la página de funciones , seleccione la pestaña Configuración y agregue las siguientes variables de entorno a la función: • `URL`— El URI del OpenSearch punto final al que se enviarán los registros. • `AUTH_SECRET` — El ARN de sus OpenSearch credenciales almacenadas en. AWS Secrets Manager Debe almacenarse como un par clave-valor y tener dos claves: `username` y `password`. • `PLATFORM_INDEX` , `FUNCTION_INDEX` y `EXTENSION_INDEX` : los nombres de los índices que almacenarán los datos de telemetría, los registros de funciones y los registros de extensiones. Asegúrese de que cumplan con los criterios de nomenclatura adecuados. De lo contrario, no se crearán los índices. • `DISPATCH_MIN_BATCH_SIZE` : el número de eventos de registro que desea agrupar. Sin	Desarrollador de aplicaciones, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	embargo, cuando la función se cierre, sus registros se enviarán independi entemente de esta configura ción.	

Adición de declaraciones de registro y pruebas de la función

Tarea	Descripción	Habilidades requeridas

Agregue declaraciones de registro a la función.	Agregue declaraciones de registro a su función mediante uno de los mecanismos de registro integrados o el módulo de registro que prefiera.
	
	A continuación, se muestran ejemplos de registro de mensajes en Python:
	
	`print("Your Log Message Here")`
	`logger = logging.getLogger(__name__)`
	
	`logger.info("Test Info Log.")`
	`logger.error("Test Error Log.")`
		Desarrollador de aplicaciones, arquitecto de la nube

Comprobación de la función de .	1. En la página de la función, seleccione la pestaña Prueba. 2. Cree un evento de prueba para su función y ponga	Desarrollador de aplicaciones, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	en marcha la prueba. Para obtener más informaci ón, consulte Probar la función de Lambda en la documentación de Lambda. Debería ver Ejecutando la función: listo si todo funciona correctamente.	

Vea sus inicios de sesión OpenSearch

Tarea	Descripción	Habilidades requeridas
Consulte sus índices.	En OpenSearch, ejecuta el siguiente comando para consultar tus índices: `SELECT * FROM index-nam e` Sus registros deberían mostrarse en los resultados de la consulta.	Arquitecto de la nube

Resolución de problemas

Problema	Solución
Problemas de conectividad	• Confirme que la función Lambda tenga la conectividad de red necesaria para acceder al OpenSearch clúster. Consulte la documentación del OpenSearch servicio

Problema	Solución
	para obtener instrucciones sobre cómo configurar los ajustes de la VPC. • Compruebe que los permisos de IAM concedidos a la función Lambda le permiten escribir datos en el clúster. OpenSearch Consulte la documentación de Lambda para obtener información sobre la administración de los permisos de IAM.
Errores de ingesta de datos	• Compruebe CloudWatch los registros de su función de Lambda para identificar cualquier error o excepción relacionados con la integración de la API de telemetría de Lambda. Consulte la documentación de la API de telemetría de Lambda para obtener orientación sobre la solución de problemas. • Compruebe que el OpenSearch clúster esté configurado correctamente y que tenga las asignaciones de índices y los ajustes necesarios para ingerir los datos de telemetrí a de Lambda. Consulte la documentación para obtener más información. OpenSearch

Recursos relacionados

- Ejemplo de integraciones de telemetría Lambda para (repositorio) OpenSearch GitHub
- Aumente las funciones de Lambda utilizando extensiones de Lambda (documentación de Lambda)
- API de telemetría de Lambda (documentación de Lambda)
- Presentamos la API de AWS Lambda telemetría (entrada de blog)AWS
- Integración de la API de AWS Lambda telemetría con Prometheus y (entrada del blog) OpenSearch AWS

Información adicional

Alteración de la estructura de los registros

De forma predeterminada, la extensión envía los registros como un documento anidado. OpenSearch Esto le permite realizar consultas anidadas para recuperar valores de columnas individuales.

Si la salida de registro predeterminada no satisface sus necesidades específicas, puede personalizarla modificando el código fuente de la extensión Lambda proporcionada por. AWS AWS anima a los clientes a adaptar la producción a los requisitos de su empresa. Para cambiar la salida del registro, busque la función `dispatch_to_opensearch` en el archivo `telemetry_dispatcher.py` dentro del código fuente de la extensión y realice las modificaciones necesarias.

Configuración de un router de celdas sin servidor para una arquitectura basada en celdas

Mian Tariq and Ioannis Lioupras, Amazon Web Services

Resumen

Como punto de entrada al sistema de una aplicación global basada en células, el enrutador de celdas es responsable de asignar de manera eficiente los usuarios a las celdas adecuadas y de proporcionar los puntos de conexión a los usuarios. El enrutador de celdas maneja funciones tales como almacenar user-to-cell mapeos, monitorear la capacidad de la celda y solicitar nuevas celdas cuando sea necesario. Es importante mantener la funcionalidad del router de celdas durante interrupciones posibles.

El marco de diseño de los enrutadores de celdas de este patrón se centra en la resiliencia, la escalabilidad y la optimización general del rendimiento. El patrón utiliza un enrutamiento estático, en el que los clientes almacenan en caché los puntos de conexión al iniciar sesión por primera vez y se comunican directamente con las celdas. Esta disociación mejora la resiliencia del sistema, ya que ayuda a garantizar la funcionalidad ininterrumpida de la aplicación basada en celdas durante una afectación del router de celdas.

Este patrón utiliza una AWS CloudFormation plantilla para implementar la arquitectura. Para obtener detalles sobre lo que implementa la plantilla o para implementar la misma configuración mediante el Consola de administración de AWS, consulte la sección de información adicional.

> **Important**
>
> La demostración, el código y la CloudFormation plantilla que se presentan en este patrón tienen únicamente fines explicativos. El material proporcionado tiene la finalidad única de ilustrar el patrón de diseño y ayudar a la comprensión. La demostración y el código no están listos para la producción y no deben utilizarse para ninguna actividad de producción en directo. Se recomienda no utilizar el código o la demostración en un entorno de producción. Hacerlo será bajo su propia responsabilidad. Recomendamos consultar con los profesionales adecuados y hacer pruebas exhaustivas antes de implementar este patrón o sus componentes en un entorno de producción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa
- La última versión de AWS Command Line Interface (AWS CLI)
- Credenciales de AWS con los permisos necesarios para crear la CloudFormation pila, AWS Lambda las funciones y los recursos relacionados

Versiones de producto

- Python 3.12

Arquitectura

En el diagrama siguiente se muestra un diseño general del router de celdas.

En el diagrama se muestra el flujo de trabajo siguiente:

1. El usuario se pone en contacto con Amazon API Gateway, que sirve de interfaz para los puntos de conexión de la API del router de celdas.
2. Amazon Cognito gestiona la autenticación y la autorización.
3. El AWS Step Functions flujo de trabajo consta de los siguientes componentes:
   - Orchestrator: se `Orchestrator` utiliza AWS Step Functions para crear un flujo de trabajo o una máquina de estados. La API del router de celdas desencadena el flujo de trabajo. `Orchestrator` ejecuta funciones de Lambda según la ruta del recurso.
   - Dispatcher: la función `Dispatcher` de Lambda identifica y asigna una celda estática por cada usuario registrado nuevo. La función busca la celda con el menor número de usuarios, la asigna al usuario y devuelve los puntos de conexión.
   - Mapper – La `Mapper` operación gestiona las user-to-cell asignaciones dentro de la base de datos `RoutingDB` Amazon DynamoDB creada por la plantilla. CloudFormation Cuando se desencadena, la función `Mapper` proporciona sus puntos de conexión a los usuarios ya asignados.
   - Scaler: la función `Scaler` hace un seguimiento de la ocupación de las celdas y de la capacidad disponible. Cuando sea necesario, la función `Scaler` puede enviar una solicitud

a través de Amazon Simple Queue Service (Amazon SQS) a la capa de aprovisionamiento e implementación para solicitar celdas nuevas.

- Validator: la función `Validator` valida los puntos de conexión de las celdas y detecta problemas posibles.

4. `RoutingDB`Almacena la información y los atributos de las celdas (puntos finales de la API, estado, Región de AWS métricas).
5. Cuando la capacidad disponible de las celdas supera un umbral, el router de celdas solicita servicios de aprovisionamiento e implementación a través de Amazon SQS para crear celdas nuevas.

Cuando se crean celdas nuevas, `RoutingDB` se actualiza desde la capa de aprovisionamiento e implementación. Sin embargo, ese proceso está fuera del ámbito de este patrón. Para obtener información general de las premisas de diseño de la arquitectura basada en celdas y detalles sobre el diseño del router de celdas que se utiliza en este patrón, consulte la sección Información adicional.

Tools (Herramientas)

Servicios de AWS

- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket APIs a cualquier escala.
- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todo el Cuentas de AWS mundo Regiones de AWS.
- Amazon Cognito ofrece autenticación, autorización y administración de usuarios para aplicaciones móviles y web.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.
- AWS Step Functionses un servicio de organización sin servidor que le ayuda a combinar funciones de Lambda y otras Servicios de AWS para crear aplicaciones críticas para la empresa.

Otras herramientas

- Python es un lenguaje de programación informático de uso general.

Repositorio de código

El código de este patrón está disponible en el repositorio Serverless-Cell-Router. GitHub

Prácticas recomendadas

Para conocer las mejores prácticas a la hora de crear arquitecturas basadas en celdas, consulte la siguiente guía de Well-Architected AWS :

- Reducing the Scope of Impact with Cell-Based Architecture
- AWS Pilar de confiabilidad de un marco bien diseñado REL1: 0-BP04 Utilice arquitecturas de mamparo para limitar el alcance del impacto

Epics

Preparación del archivo de origen

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código de muestra.	Para clonar el Serverless-Cell-Router GitHub repositorio en su ordenador, utilice el siguiente comando: `git clone https://github.com/aws-samples/Serverless-Cell-Router/`	Desarrollador

Tarea	Descripción	Habilidades requeridas
Configure las credenciales AWS CLI temporales.	Configure el AWS CLI con las credenciales para su Cuenta de AWS. Este tutorial utiliza las credenciales temporales proporcionadas por la línea de comandos de AWS IAM Identity Center o la opción de acceso programático. Esto establece las variables de `AWS_SESSION_TOKEN` AWS entorno y `AWS_ACCES S_KEY_ID AWS_SECRE T_ACCESS_KEY` , con las credenciales adecuadas para su uso con. AWS CLI	Desarrollador
Cree un bucket de S3.	Cree un bucket de S3 que se utilizará para almacenar y acceder a las funciones de Serverless-Cell-Router Lambda para su despliegue mediante la CloudFormation plantilla. Para crear el bucket de S3, utilice el comando siguiente: `aws s3api create-bucket --bucket <bucket name> --region eu-central-1 --create-bucket-configuration LocationConstraint=eu-central-1`	Desarrollador

Tarea	Descripción	Habilidades requeridas

Cree los archivos .zip.	Cree un archivo .zip para cada función de Lambda ubicada en el directorio Functions. Estos archivos .zip se utilizarán para implementar las funciones de Lambda. En un equipo Mac, utilice los comandos `zip` siguientes:
	`zip -j mapper-scr.zip Functions/Mapper.py`
	`zip -j dispatcher-scr.zip Functions/Dispatcher.py`
	`zip -j scaler-scr.zip Functions/Scaler.py`
	`zip -j cp validator-scr.zip Functions/Validator.py`
	`zip -j dynamodbDummyData-scr.zip Functions/DynamodbDummyData.py`
		Desarrollador

Tarea	Descripción	Habilidades requeridas

Copie los archivos .zip en el bucket de S3.	Para copiar todos los archivos .zip de la función de Lambda al bucket de S3, utilice los comandos siguientes:
	`aws s3 cp mapper-scr.zip s3://<bucket name>`
	`aws s3 cp dispatcher-scr.zip s3://<bucket name>`
	`aws s3 cp scaler-scr.zip s3://<bucket name>`
	`aws s3 cp validator-scr.zip s3://<bucket name>`
	`aws s3 cp dynamodbDummyData-scr.zip s3://<bucket name>`
		Desarrollador

Cree la pila CloudFormation

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla.	Para implementar la CloudFormation plantilla, ejecute el siguiente AWS CLI comando: `aws cloudformation create-stack --stack-name serverless.cell-router \`	Desarrollador

Tarea	Descripción	Habilidades requeridas
	`--template-body file://Serverless-Cell-Router-Stack-v10.yaml \ --capabilities CAPABILITY_IAM \ --parameters ParameterKey=LambdaFunctionMapperS3KeyParameterSCR,ParameterValue=mapper-scr.zip \ ParameterKey=LambdaFunctionDispatcherS3KeyParameterSCR,ParameterValue=dispatcher-scr.zip \ ParameterKey=LambdaFunctionScalerS3KeyParameterSCR,ParameterValue=scaler-scr.zip \ ParameterKey=LambdaFunctionAddDynamoDBDummyItemsS3KeyParameterSCR,ParameterValue=dynamodbDummyData-scr.zip \ ParameterKey=LambdaFunctionsS3BucketParameterSCR,ParameterValue=<S3 bucket storing lambda zip files> \ ParameterKey=CognitoDomain,ParameterValue=<Cognito Domain Name> \ --region <enter your aws region id, e.g. "eu-central-1">`	

Tarea	Descripción	Habilidades requeridas
Compruebe el progreso.	Inicia sesión en Consola de administración de AWS, abre la CloudFormation consola en https://console.aws.amazon.com/cloudformation/y comprueba el progreso del desarrollo de la pila. Cuando el estado sea `CREATE_COMPLETE` , la pila se habrá implementado correctamente.	Desarrollador

Evaluación y verificación

Tarea	Descripción	Habilidades requeridas
Asigne celdas al usuario.	Para iniciar `Orchestrator` , ejecute el comando curl siguiente: `curl -X POST \ -H "Authorization: Bearer {User id_token}" \ https://xxxxxx.execute-api.eu-central-1.amazonaws.com/Cell_Router_Development/cells` `Orchestrator` desencadena la ejecución de la función `Dispatcher` . `Dispatcher` , a su vez, verifica la existencia del usuario. Si se encuentra el usuario,	Desarrollador

Tarea	Descripción	Habilidades requeridas
	`Dispatcher` devuelve el ID de celda y el punto final asociados URLs. Si no se encuentra al usuario, `Dispatcher` asigna una celda y envía el ID de celda a la función `Scaler` para evaluar la capacidad residual de la celda asignada. La respuesta de la función `Scaler` es la siguiente: `"cellID : cell-0002 , endPoint_1 : https://xxxxx.execute-api.eu-north-1 .amazonaws.com/ , endPoint_2 : https://xxxxxxx.execute-api .eu-central-1.amaz onaws.com/"`	

Tarea	Descripción	Habilidades requeridas

Recupere las celdas de los usuarios.	Para utilizar `Orchestrator` para ejecutar la función `Mapper`, ejecute el comando siguiente:
	`curl -X POST \ -H "Authorization: Bearer {User id_token}" \ https://xxxxxxxxx.execute-api.eu-central-1.amazonaws.com/Cell_Router_Development/mapper`
	`Orchestrator` Busca la celda asignada al usuario y devuelve el ID de la celda y URLs obtiene la siguiente respuesta:
	`"cellID : cell-0002 , endPoint_1 : https://xxxxx.execute-api.eu-north-1.amazonaws.com/ , endPoint_2 : https://xxxxxxx.execute-api.eu-central-1.amazonaws.com/"`
		Desarrollador

Limpieza

Tarea	Descripción	Habilidades requeridas
Limpie los recursos.	Para evitar el cobro de otros cargos en su cuenta, haga lo siguiente: 1. Vacíe el bucket de S3 que creó para las funciones de Lambda. 2. Elimine el bucket . 3. Elimine la CloudFormation pila.	Desarrollador de aplicaciones

Recursos relacionados

Referencias

- Estabilidad estática con zonas de disponibilidad
- AWS Fault Isolation Boundaries: Static stability

Video

Physalia: Cell-based Architecture to Provide Higher Availability on Amazon EBS

https://www.youtube-nocookie.com/embed/6 ¿Iknq? RZMFic controles = 0

Información adicional

Premisas de diseño de arquitectura basada en celdas

Si bien este patrón se centra en el router de celdas, es importante comprender todo el entorno. El entorno está estructurado en tres capas discretas:

- La capa de enrutamiento, o capa delgada, que contiene el enrutador de celdas
- La capa de celdas, que comprende varias celdas

- La capa de aprovisionamiento e implementación, que aprovisiona las celdas e implementa la aplicación

Cada capa mantiene su funcionalidad incluso en el caso de que las deficiencias afecten a otras capas. Cuentas de AWS sirven como límite de aislamiento de fallas.

En el diagrama siguiente se muestran las capas en un nivel general. La capa de celdas y la capa de aprovisionamiento e implementación quedan fuera del alcance de este patrón.

Para más información sobre la arquitectura basada en celdas, consulte Reducing the Scope of Impact with Cell-Based Architecture: Cell routing.

Patrón de diseño de router de celdas

El enrutador de celdas es un componente compartido en las celdas. Para mitigar los impactos posibles, es importante que la capa de enrutamiento utilice un diseño simplista y escalable horizontalmente que sea lo más delgado posible. La capa de enrutamiento, que sirve como punto de entrada al sistema, consta solo de los componentes necesarios para asignar a los usuarios de manera eficiente a las celdas adecuadas. Los componentes de esta capa no participan en la administración ni en la creación de celdas.

Este patrón utiliza el enrutamiento estático, lo que significa que el cliente almacena los puntos de conexión en las memorias caché durante el inicio de sesión inicial y, posteriormente, establece una comunicación directa con la celda. Se inician interacciones periódicas entre el cliente y el router de celdas para confirmar el estado actual o recuperar las actualizaciones. Este desacoplamiento intencionado permite a los usuarios actuales operar sin interrupciones en caso de que haya tiempo de inactividad del router de celdas y proporciona una funcionalidad y resiliencia continuas al sistema.

En este patrón, el router de celdas admite las funcionalidades siguientes:

- Recuperación de datos de celdas a partir de la base de datos de celdas en la capa de aprovisionamiento e implementación. Almacenamiento o actualización de la base de datos local.
- Asignación de una celda a cada usuario registrado nuevo de la aplicación mediante el algoritmo de asignación de celdas.
- Almacenar el user-to-cells mapeo en la base de datos local.
- Comprobación de la capacidad de las celdas durante la asignación de usuarios. Generación de un evento para la máquina expendedora a la capa de aprovisionamiento e implementación para crear celdas.

- Uso del algoritmo de criterios de creación de celdas para proporcionar esta funcionalidad.
- Responder a las solicitudes de los usuarios recién registrados proporcionando URLs las celdas estáticas. Se URLs almacenarán en caché en el cliente con un tiempo de vida (TTL).
- Respuesta a las solicitudes de los usuarios existentes sobre una URL no válida al proporcionar una URL nueva o actualizada.

Para comprender mejor el router celular de demostración que se configura mediante la CloudFormation plantilla, revise los siguientes componentes y pasos:

1. Defina y configure el grupo de usuarios de Amazon Cognito.
2. Defina y configure la API de API Gateway para el router de celdas.
3. Crear una tabla de DynamoDB.
4. Cree y configure una cola de SQS.
5. Implemente la función `Orchestrator`.
6. Implemente las funciones de Lambda: `Dispatcher`, `Scaler`, `Mapper`, `Validator`.
7. Evalúe y verifique.

El supuesto es que la capa de aprovisionamiento e implementación ya está establecida. Los detalles de su implementación quedan fuera del alcance de este artefacto.

Como estos componentes se configuran y configuran mediante una CloudFormation plantilla, los siguientes pasos se presentan de forma descriptiva y de alto nivel. Se supone que tiene los AWS conocimientos necesarios para completar la instalación y la configuración.

1. Defina y configure el grupo de usuarios de Amazon Cognito

Inicie sesión en y abra la Consola de administración de AWS consola de Amazon Cognito en. https://console.aws.amazon.com/cognito/ Defina y configure un grupo de usuarios de Amazon Cognito denominado `CellRouterPool`, con integración de aplicaciones, interfaz de usuario alojada y permisos necesarios.

2. Defina y configure la API de API Gateway para el router de celdas

Abra la consola de API Gateway en https://console.aws.amazon.com/apigateway/. Defina y configure una API denominada `CellRouter`, mediante un autorizador de Amazon Cognito integrado con el grupo de usuarios `CellRouterPool` de Amazon Cognito. Implemente los elementos siguientes:

- Recursos de API `CellRouter`, tal como los métodos `POST`
- Integración con el flujo de trabajo de Step Functions implementada en el paso 5
- Autorización a través del autorizador de Amazon Cognito
- Asignaciones de solicitudes y respuestas de integración
- Asignación de los permisos necesarios

3. Crear una tabla de DynamoDB

Abra la consola de DynamoDB https://console.aws.amazon.com/dynamodb/en y cree una tabla de DynamoDB estándar llamada con la siguiente configuración: `tbl_router`

- Clave de partición – `marketId`
- Clave de clasificación – `cellId`
- Modo de capacidad: provisioned
- Point-in-time recuperación (PITR) – Desactivada

En la pestaña Índices, cree un índice secundario global llamado `marketId-currentCapacity-index`. La función de Lambda `Scaler` utilizará el índice para hacer búsquedas eficaces en la celda con el menor número de usuarios asignados.

Cree la estructura de tabla con los atributos siguientes:

- `marketId`: Europe
- `cellId`: cell-0002
- `currentCapacity`: 2
- `endPoint_1`: <su punto de conexión de la primera región>
- `endPoint_2`: <su punto de conexión de la segunda región>
- `IsHealthy`: true
- `maxCapacity`: 10
- `regionCode_1` – `eu-north-1`
- `regionCode_2` – `eu-central-1`
- `userIds`: <su dirección de correo electrónico>

4. Cree y configure una cola de SQS

Abra la consola de Amazon SQS en https://console.aws.amazon.com/sqs/y cree una cola SQS estándar denominada configurada con cifrado de claves **`CellProvisioning`** Amazon SQS.

5. Implemente la función Orchestrator

Desarrolle un flujo de trabajo de Step Functions que sirva de `Orchestrator` para el router. Se puede acceder al flujo de trabajo a través de la API del enrutador de celdas. El flujo de trabajo ejecuta las funciones de Lambda designadas según la ruta de recursos. Integre la función step con la API de API Gateway para el router de celdas `CellRouter` y configure los permisos necesarios para invocar las funciones de Lambda.

El siguiente diagrama muestra el flujo de trabajo. El estado de elección invoca una de las funciones de Lambda. Si la función de Lambda se ejecuta de manera correcta, el flujo de trabajo termina. Si se produce un error en la función de Lambda, se invoca el estado de error.

6. Implemente las funciones de Lambda

Implemente las funciones `Dispatcher`, `Mapper`, `Scaler` y `Validator`. Al definir y configurar cada función en la demostración, defina un rol para la función y asigne los permisos necesarios para realizar las operaciones necesarias en la tabla de DynamoDB `tbl_router`. Además, integre cada función en el flujo de trabajo `Orchestrator`.

Función dispatcher

La función `Dispatcher` se encarga de identificar y asignar una única celda estática para cada nuevo usuario registrado. Cuando un usuario nuevo se registra en la aplicación global, la solicitud se dirige a la función `Dispatcher`. La función procesa la solicitud mediante criterios de evaluación predefinidos, como los siguientes:

1. Región: seleccione la celda del mercado donde se encuentra el usuario. Por ejemplo, si el usuario accede a la aplicación global desde Europa, seleccione una celda que se utilice Regiones de AWS en Europa.
2. Proximidad o latencia: seleccione la celda más cercana al usuario. Por ejemplo, si el usuario accede a la aplicación desde Holanda, la función considerará una celda que utilice Fráncfort e Irlanda. La decisión sobre qué celda está más cerca se basa en métricas como la latencia entre la ubicación del usuario y las regiones de la celda. Para este patrón de ejemplo, la información se suministra de manera estática desde la capa de aprovisionamiento e implementación.
3. Estado: la función `Dispatcher` comprueba si es correcto el estado de la celda seleccionada según el estado de la celda proporcionado (Correcto = verdadero o falso).

4. Capacidad: la distribución de usuarios se basa en la lógica del número mínimo de usuarios de una celda, por lo que el usuario se asigna a la celda que tiene el menor número de usuarios.

> **Note**
>
> Estos criterios se presentan solo para explicar este patrón de ejemplo. Para una implementación real de un router de celdas, puede definir criterios más refinados y basados en casos de uso.

La función `Orchestrator` invoca la función Dispatcher para asignar usuarios a las celdas. En esta función de demostración, el valor de mercado es un parámetro estático definido como `europe`.

La función `Dispatcher` evalúa si una celda ya está asignada al usuario. Si la celda ya está asignada, la función `Dispatcher` devuelve los puntos de conexión de la celda. Si no se asigna ninguna celda al usuario, la función busca la celda con el menor número de usuarios, la asigna al usuario y devuelve los puntos de conexión. La eficacia de la consulta de búsqueda de celdas se optimiza mediante el uso del índice secundario global.

Función mapper

La `Mapper` función supervisa el almacenamiento y el mantenimiento de las user-to-cell asignaciones en la base de datos. Se asigna una celda única a cada usuario registrado. Cada celda tiene dos celdas distintas URLs, una para cada región de AWS. Funcionan como puntos finales de API alojados en API Gateway y URLs funcionan como puntos de entrada a la aplicación global.

Cuando la `Mapper` función recibe una solicitud de la aplicación cliente, ejecuta una consulta en la `tbl_router` tabla de DynamoDB para recuperar user-to-cell la asignación asociada al ID de correo electrónico proporcionado. Si encuentra una celda asignada, la `Mapper` función proporciona inmediatamente las dos de la celda. URLs La `Mapper` función también monitorea activamente las alteraciones de la celda URLs e inicia notificaciones o actualizaciones de la configuración del usuario.

Función scaler

La función `Scaler` administra la capacidad residual de la celda. Para cada nueva solicitud de registro de usuario, la función `Scaler` evalúa la capacidad disponible de la celda que la función `Dispatcher` asignó al usuario. Si la celda ha alcanzado su límite predeterminado de acuerdo

con los criterios de evaluación especificados, la función inicia una solicitud a través de una cola de Amazon SQS a la capa de aprovisionamiento e implementación, y solicita el aprovisionamiento y la implementación de celdas nuevas. El escalado de las celdas se puede ejecutar según un conjunto de criterios de evaluación, como los siguientes:

1. Usuarios máximos: cada celda puede tener un número máximo de 500 usuarios.
2. Capacidad del búfer: la capacidad del búfer de cada celda es del 20 %, lo que significa que cada celda se puede asignar a 400 usuarios en cualquier momento. El 20 % restante de la capacidad de búfer se reserva para futuros casos de uso y para la gestión de situaciones inesperadas (por ejemplo, cuando los servicios de creación y aprovisionamiento de celdas no están disponibles).
3. Creación de celdas: en cuanto una celda existente alcanza el 70 % de su capacidad, se activa una solicitud para crear una celda adicional.

> **Note**
>
> Estos criterios se presentan solo para explicar este patrón de ejemplo. Para una implementación real de un router de celdas, puede definir criterios más refinados y basados en casos de uso.

El código `Scaler` de demostración es ejecutado por la función `Orchestrator` después de que la función `Dispatcher` ha asignado correctamente una celda al usuario recién registrado. La función `Scaler`, tras recibir el ID de la celda por parte de la función `Dispatcher`, evalúa si la celda designada tiene la capacidad adecuada para alojar a más usuarios, según los criterios de evaluación predefinidos. Si la capacidad de la celda es insuficiente, la función `Scaler` envía un mensaje al servicio Amazon SQS. El servicio recupera este mensaje en la capa de aprovisionamiento e implementación e inicia el aprovisionamiento de una celda nueva.

Función validator

La función `Validator` identifica y resuelve los problemas relacionados con el acceso a la celda. Cuando un usuario inicia sesión en la aplicación global, la aplicación recupera las celdas de la configuración del perfil URLs del usuario y dirige las solicitudes de los usuarios a una de las dos regiones asignadas dentro de la celda. Si no URLs se puede acceder a ellas, la aplicación puede enviar una solicitud de validación de URL al router móvil. El router de celdas de la función `Orchestrator` invoca a la función `Validator`. La función `Validator` inicia el proceso de validación. La validación puede incluir, entre otras comprobaciones, las siguientes:

- Hacer una referencia cruzada de la celda URLs de la solicitud con la URLs almacenada en la base de datos para identificar y procesar posibles actualizaciones
- Hacer una comprobación de estado exhaustiva (por ejemplo, una solicitud `HTTP GET` al punto de conexión de la celda)

En conclusión, la función `Validator` responde a las solicitudes de los clientes y proporciona el estado de la validación y las medidas correctivas necesarias.

La función `Validator` está diseñada para mejorar la experiencia del usuario. Imagine un escenario en el que usuarios determinados tengan dificultades para acceder a la aplicación global porque un incidente provoca que las celdas no estén disponibles temporalmente. En lugar de presentar errores genéricos, la función `Validator` puede proporcionar pasos de corrección instructivos. Entre estos pasos se pueden incluir los siguientes:

- Informe a los usuarios acerca del incidente.
- Proporcione un tiempo de espera aproximado antes de la disponibilidad del servicio.
- Proporcione un número de contacto de asistencia para obtener información adicional.

El código de demostración de la `Validator` función verifica que la celda proporcionada por el usuario URLs en la solicitud coincida con los registros almacenados en la tabla. `tbl_router` La función `Validator` también comprueba si el estado de las celdas es correcto.

Configuración del acceso privado a un bucket de Amazon S3 a través de un punto de conexión de VPC

Martin Maritsch, Nicolas Jacob Baer, Gabriel Rodriguez Garcia, Shukhrat Khodjaev, Mohan Gowda Purushothama y Joaquin Rinaudo, Amazon Web Services

Resumen

En Amazon Simple Storage Service (Amazon S3), los URLs prefirmados permiten compartir archivos de tamaño arbitrario con los usuarios de destino. De forma predeterminada, URLs se puede acceder a Amazon S3 prefirmados desde Internet dentro de un período de tiempo de caducidad, lo que facilita su uso. Sin embargo, los entornos corporativos a menudo requieren que el acceso a Amazon S3 esté prefirmado URLs para estar limitado únicamente a una red privada.

Este patrón presenta una solución sin servidor para interactuar de forma segura con los objetos de S3 mediante el uso de objetos prefirmados URLs desde una red privada sin acceso a Internet. En la arquitectura, los usuarios acceden a un equilibrador de carga de aplicación a través de un nombre de dominio interno. El tráfico se enruta de manera interna a través de Amazon API Gateway y un punto de conexión de nube privada virtual (VPC) del bucket de S3. La AWS Lambda función genera descargas de archivos prefirmados URLs a través del punto final de la VPC privada, lo que ayuda a mejorar la seguridad y la privacidad de los datos confidenciales.

Requisitos previos y limitaciones

Requisitos previos

- Una VPC que incluye una subred implementada en una Cuenta de AWS que está conectada a la red corporativa (por ejemplo, a través de). AWS Direct Connect

Limitaciones

- El bucket S3 debe tener el mismo nombre que el dominio, por lo que le recomendamos que consulte Reglas de nomenclatura de buckets de Amazon S3.
- Este ejemplo de arquitectura no incluye características de supervisión para la infraestructura implementada. Si su caso de uso requiere supervisión, considere la posibilidad de añadir servicios de supervisión de AWS.

- Este ejemplo de arquitectura no incluye la validación de entradas. Si su caso de uso requiere la validación de las entradas y un mayor nivel de seguridad, considere utilizarla AWS WAF para proteger su API.
- Esta arquitectura de ejemplo no incluye el registro de acceso con el equilibrador de carga de aplicación Si el caso de uso requiere el registro de acceso, considere la posibilidad de habilitar los registros de acceso del equilibrador de carga.

Versiones

- Python versión 3.11 o posterior
- Terraform versión 1.6 o posterior

Arquitectura

Pila de tecnología de destino

Los servicios siguientes de AWS se utilizan en la pila de tecnologías de destino:

- Amazon S3 es el servicio de almacenamiento principal que se utiliza para cargar, descargar y almacenar archivos de manera segura.
- Amazon API Gateway expone los recursos y puntos de conexión para interactuar con el bucket de S3. Este servicio desempeña un papel en la generación de datos prefirmados URLs para descargar o cargar.
- AWS Lambdagenera archivos prefirmados URLs para descargar desde Amazon S3. API Gateway llama a la función de Lambda.
- Amazon VPC implementa recursos en una VPC para proporcionar aislamiento de la red. La VPC incluye subredes y tablas de enrutamiento para controlar el flujo de tráfico.
- El equilibrador de carga de aplicación dirige el tráfico entrante a API Gateway o al punto de conexión de VPC del bucket de S3. Permite a los usuarios de la red corporativa acceder a los recursos de manera interna.
- El punto de conexión de VPC para Amazon S3 permite la comunicación directa y privada entre los recursos de la VPC y Amazon S3 sin tener que atravesar la Internet pública.
- AWS Identity and Access Management (IAM) controla el acceso a AWS los recursos. Los permisos se configuran para garantizar interacciones seguras con la API y otros servicios.

Arquitectura de destino

En el siguiente diagrama se ilustra lo siguiente:

1. Los usuarios de la red corporativa pueden acceder al equilibrador de carga de aplicación a través de un nombre de dominio interno. Suponemos que existe una conexión entre la red corporativa y la subred de la intranet Cuenta de AWS (por ejemplo, a través de una Direct Connect conexión).
2. El Application Load Balancer dirige el tráfico entrante a API Gateway para generar datos prefirmados URLs para descargar o cargar en Amazon S3, o al punto final de VPC del bucket de S3. En ambos casos, las solicitudes se enrutan internamente y no es necesario que atraviesen Internet.
3. API Gateway expone los recursos y puntos de conexión para interactuar con el bucket de S3. En este ejemplo, proporcionamos un punto de conexión para descargar archivos del bucket de S3, pero esto podría ampliarse para proporcionar también la funcionalidad de carga.
4. La función de Lambda genera la URL prefirmada para descargar un archivo de Amazon S3 mediante el nombre de dominio del equilibrador de carga de aplicación en lugar del dominio público de Amazon S3.
5. El usuario recibe la URL prefirmada y la utiliza para descargar el archivo de Amazon S3 mediante el equilibrador de carga de aplicación. El equilibrador de carga incluye una ruta predeterminada para enviar el tráfico que no está destinado a la API hacia el punto de conexión de VPC del bucket de S3.
6. El punto de conexión de VPC enruta la URL prefirmada con el nombre de dominio personalizado al bucket de S3. El bucket de S3 debe tener el mismo nombre que el dominio.

Automatización y escala

Este patrón utiliza Terraform para implementar la infraestructura del repositorio de código en una Cuenta de AWS.

Tools (Herramientas)

Herramientas

- Python es un lenguaje de programación informático de uso general.
- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.

- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que te ayuda a interactuar con los AWS servicios mediante comandos en tu consola de línea de comandos.

Repositorio de código

El código de este patrón está disponible en un GitHub repositorio en private-s3-vpce. https://github.com/aws-samples/

Prácticas recomendadas

La arquitectura de ejemplo para este patrón utiliza permisos de IAM para controlar el acceso a la API. Cualquier persona que tenga credenciales de IAM válidas puede llamar a la API. Si su caso de uso requiere un modelo de autorización más complejo, es posible que quiera utilizar un mecanismo de control de acceso distinto.

Epics

Implemente la solución en un Cuenta de AWS

Tarea	Descripción	Habilidades requeridas
Obtenga AWS las credencia les.	Revise sus AWS credencia les y el acceso a su cuenta. Para obtener instrucciones, consulte los ajustes de configuración y del archivo de credenciales en la AWS CLI documentación.	AWS DevOps, AWS general
Clonar el repositorio.	Clona el GitHub repositor io proporcionado con este patrón: `git clone https://github.com/aws-samples/private-s3-vpce`	AWS DevOps, AWS general

Tarea	Descripción	Habilidades requeridas
Configure las variables	1. En su ordenador, en el GitHub repositorio, abra la `terraform` carpeta: `cd terraform` 2. Abra el archivo `example.tfvars` y personalice los parámetros según sus necesidades.	AWS DevOps, AWS general
Implemente la solución.	1. En la carpeta `terraform`, ejecute Terraform y pase las variables que personalizó: `terraform apply -var-file="example.tfvars"` 2. Confirme que los recursos que se muestran en el diagrama de arquitectura se implementaron correctamente.	AWS DevOps, AWS general

Pruebe la solución

Tarea	Descripción	Habilidades requeridas
Crear un archivo de prueba.	Cargue un archivo en Amazon S3 para crear un escenario de prueba para la descarga del archivo. Puede utilizar la consola Amazon	AWS DevOps, AWS general

Tarea	Descripción	Habilidades requeridas
	S3 o el siguiente AWS CLI comando: `aws s3 cp /path/to/ testfile s3://your-bucket-name/testfile`	
Pruebe la funcionalidad de las URL prefirmadas.	1. Envíe una solicitud al equilibrador de carga de aplicación para crear una URL prefirmada para el archivo de prueba mediante awscurl: `awscurl https://your-domain-name/api/ get_url?key=testfile` Este paso crea una firma válida a partir de sus credenciales, que será validada por API Gateway. 2. Analice el enlace a partir de la respuesta que reciba en el paso anterior y abra la URL prefirmada para descargar el archivo.	AWS DevOps, AWS general
Elimine recursos.	Asegúrese de eliminar los recursos cuando ya no sean necesarios: `terraform destroy`	AWS DevOps, AWS general

Resolución de problemas

Problema	Solución
Los nombres de clave de objetos de S3 con caracteres especiales, como signos numéricos (#), infringen los parámetros de la URL y provocan errores.	Codifique los parámetros de URL correctam ente y asegúrese de que el nombre de la clave del objeto S3 siga las directrices de Amazon S3.

Recursos relacionados

Amazon S3:

- Compartir objetos con prefirmados URLs
- Controlar el acceso desde los puntos finales de la VPC con políticas de bucket

Amazon API Gateway:

- Usa políticas de puntos finales de VPC de forma privada APIs en API Gateway

Equilibrador de carga de aplicación:

- Alojamiento de sitios web estáticos HTTPS internos con ALB, S3 y PrivateLink (AWS entrada de blog)

Solucione problemas de estados AWS Step Functions mediante Amazon Bedrock

Aniket Kurzadkar y Sangam Kushwaha, Amazon Web Services

Resumen

AWS Step Functions Las capacidades de gestión de errores pueden ayudarlo a detectar un error que se produce durante un estado de un flujo de trabajo, pero aun así puede resultar difícil encontrar la causa raíz de un error y depurarlo. Este patrón aborda ese desafío y muestra cómo Amazon Bedrock puede serle útil para resolver los errores que se producen durante los estados de Step Functions.

Step Functions orquesta el flujo de trabajo, lo que facilita a los desarrolladores la automatización de los procesos. Step Functions también proporciona una funcionalidad de gestión de errores que ofrece las ventajas siguientes:

- Los desarrolladores pueden crear aplicaciones más resilientes que no fallen por completo cuando algo sale mal.
- Los flujos de trabajo pueden incluir lógica condicional para gestionar los distintos tipos de errores de otra manera.
- El sistema puede volver a intentar las operaciones erróneas de manera automática, tal vez con un retroceso exponencial.
- Se pueden definir rutas de ejecución alternativas para los escenarios de error, lo que permite que el flujo de trabajo se adapte y continúe procesándose.

Cuando se produce un error en un flujo de trabajo de Step Functions, este patrón muestra cómo se pueden enviar el mensaje de error y el contexto a un modelo fundacional (FM) como Claude 3, compatible con Step Functions. El FM puede analizar el error, clasificarlo y sugerir posibles medidas de corrección.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Comprensión básica de los flujos de trabajo de AWS Step Functions
- Conectividad con la API de Amazon Bedrock

Limitaciones

- Puede utilizar el enfoque de este patrón para varios Servicios de AWS. Sin embargo, los resultados pueden variar en función del mensaje creado por AWS Lambda Amazon Bedrock y evaluado posteriormente.
- Algunos Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

En el siguiente diagrama se muestran los componentes de la arquitectura y el flujo de trabajo de esta aplicación.

En el diagrama se muestra el flujo de trabajo automatizado para la gestión y notificación de errores en una máquina de estados de Step Functions:

1. El desarrollador inicia la ejecución de una máquina de estados.
2. La máquina de estados de Step Functions comienza a procesar sus estados. Hay dos resultados posibles:
   - (a) Si todos los estados se ejecutan correctamente, el flujo de trabajo pasa de manera directa a Amazon SNS para recibir una notificación de operación correcta por correo electrónico.
   - (b) Si se produce un error en algún estado, el flujo de trabajo pasa a la función de Lambda de gestión de errores.
3. En caso de error, sucede lo siguiente:
   - (a) Se desencadena la función de Lambda (controlador de errores). La función de Lambda extrae el mensaje de error de los datos del evento que le pasó la máquina de estados de Step Functions. A continuación, la función de Lambda prepara una petición según este mensaje de error y la envía a Amazon Bedrock. La petición solicita soluciones y sugerencias relacionadas con el error específico encontrado.
   - (b) Amazon Bedrock, que aloja el modelo de IA generativa, procesa la petición de entrada. (Este patrón utiliza el modelo de base Anthropic Claude 3 (FM), que es uno de los muchos FMs que admite Amazon Bedrock). El modelo de IA analiza el contexto del error. A continuación, el modelo genera una respuesta que puede incluir explicaciones de por qué se produjo el error,

soluciones posibles para resolverlo y sugerencias para evitar cometer los mismos errores en el futuro.

Amazon Bedrock devuelve su respuesta generada por IA a la función de Lambda. La función de Lambda procesa la respuesta y, posiblemente, la formatea o extrae información clave. A continuación, la función de Lambda envía la respuesta a la salida de la máquina de estados.

4. Tras la gestión del error o una ejecución correcta, el flujo de trabajo finaliza con la activación de Amazon SNS para que envíe una notificación por correo electrónico.

Tools (Herramientas)

Servicios de AWS

- Amazon Bedrock es un servicio totalmente gestionado que pone a su disposición modelos básicos de alto rendimiento (FMs) de las principales empresas emergentes de IA y Amazon a través de una API unificada.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- AWS Step Functionses un servicio de organización sin servidor que le ayuda a combinar AWS Lambda funciones y otras Servicios de AWS para crear aplicaciones esenciales para la empresa.

Prácticas recomendadas

- Dado que Amazon Bedrock es un modelo de IA generativo que aprende de los datos entrenados, también utiliza esos datos para entrenar y generar contexto. Como práctica recomendada, oculte la información privada que pueda provocar problemas de filtración de datos.
- Si bien la IA generativa puede proporcionar información valiosa, una persona debe supervisar las decisiones críticas relacionadas con la gestión de errores, sobre todo en los entornos de producción.

Epics

Creación de una máquina de estados para un flujo de trabajo

Tarea	Descripción	Habilidades requeridas
Crear una máquina de estado	Para crear una máquina de estados que sea adecuada para el flujo de trabajo, haga lo siguiente: 1. Inicie sesión en la consola y Consola de administración de AWSábrala. AWS Step Functions 2. En el panel de navegación izquierdo, elija Máquinas de estado. 3. Elija Crear máquina de estado. 4. Elija una plantilla según su caso de uso o elija En blanco para crear una plantilla según sus necesidades.	AWS DevOps

Crear una función de Lambda

Tarea	Descripción	Habilidades requeridas
Creación de una función de Lambda.	Para crear una función de Lambda, haga lo siguiente: 1. En el Consola de administración de AWS, navegue	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	hasta la AWS Lambda consola. 2. En el panel de navegación de la izquierda, seleccione Funciones y Crear una función. 3. En la página Crear función, elija entre las opciones para crear una función. A continuación, indique un nombre en Nombre de función y elija el idioma correspondiente en la lista desplegable de Tiempo de ejecución. 4. Seleccione Creación de función.	

Tarea	Descripción	Habilidades requeridas
Configure la lógica requerida en el código de Lambda.	• Para conectarse a la API de Amazon Bedrock mediante AWS SDK para Python (Boto3), utilice el código siguiente. Este código configura un cliente para Amazon Bedrock, prepara los parámetros necesarios y, a continuación, envía una solicitud al modelo Claude 3 con una petición específica. Este patrón invoca el modelo Claude 3. Para obtener más información sobre todos los modelos de cimentación compatibl es, incluido el modelo relacionado IDs, consulte los modelos de cimentaci ón compatibles en Amazon Bedrock en la documenta ción de Amazon Bedrock. `client = boto3.client( service_n ame="bedrock-runti me", region_na me="selected-region" ) # Invoke Claude 3 with the text prompt`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	<pre> model_id = "your-mod
	el-id" # Select your
	 Model ID, Based on the
	 Model Id, Change the
	 body format
	
	    try:
	        response =
	 client.invoke_model(
	            modelId=m
	odel_id,
	            body=json
	.dumps(
	                {
	
	 "anthropic_version":
	 "bedrock-2023-05-31",
	
	 "max_tokens": 1024,
	
	 "messages": [
	
	 {
	
	    "role": "user",
	
	          "content"
	: [{"type": "text",
	 "text": prompt}],
	
	 }
	                    ],
	                }
	            ),
	        )</pre>
	• (Opcional) Sustituya la cuenta por una cuenta de marcador Cuenta de AWS IDs de posición. IDs	

Tarea	Descripción	Habilidades requeridas

	Por motivos de seguridad, este enfoque puede resultar útil para depurar registros, mensajes de error u otros resultados que podrían contener información confidencial sobre las cuentas.
	
	El siguiente código localizará cualquier número de 12 dígitos que aparezca entre dos puntos (que es el formato utilizado en Cuenta de AWS IDs Amazon Resource Names (ARNs) y algunos otros AWS identificadores) y lo sustituirá por el identificador de cuenta del marcador de posición. `":123456789012:"`
	
	`def replace_account_id(input_string):`
	`  # Use a regular expression to find the AWS account ID pattern`
	`  account_id_pattern = r'(:\d{12}:)'`
	`  # Replace the matched pattern with ":123456789012:"`	

Tarea	Descripción	Habilidades requeridas
	<pre> modified_string = re.sub(account_id_pattern, ":123456789012:", input_string) return modified_string</pre>	

Integración de Step Functions con Lambda

Tarea	Descripción	Habilidades requeridas
Configure Lambda para gestionar los errores en Step Functions.	Para configurar Step Functions a fin de gestionar los errores sin interrumpir el flujo de trabajo, haga lo siguiente: 1. En la consola de Step Functions, vaya a la máquina de estados que creó anteriormente. 2. Elija Editar y, a continuación, elija el servicio para configurar la gestión de errores y elija Gestión de errores. 3. Elija Agregar nuevo detector y, en Estado de reserva, elija Lambda y, a continuación, elija la función de Lambda que creó anteriormente. Para más información, consulte	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	la Detectar errores en la documentación de Step Functions.	

Resolución de problemas

Problema	Solución
Lambda no puede acceder a la API de Amazon Bedrock (no tiene autorización para realizar la operación)	Este error se produce cuando el rol de Lambda no tiene permiso para acceder a la API de Amazon Bedrock. Para resolver este problema, agregue la política `AmazonBedrockFullAccess` para el rol de Lambda. Para obtener más información, consulte AmazonBedrockFullAccessla Guía de referencia de políticas AWS administradas.
Error del tiempo de espera de Lambda	A veces, es posible que tarde más de 30 segundos en generar una respuesta y enviarla, según la petición. Para resolver este problema, aumente el tiempo de configuración. Para más información, consulte Configure Lambda function timeout en la AWS Lambda Developer Guide.

Recursos relacionados

- Amazon Bedrock
- Amazon Bedrock API access
- Cree su primera función Lambda
- Desarrollo de flujos de trabajo con Step Functions
- AWS Step Functions

Más patrones

- Acceder, consultar y unirse a las tablas de Amazon DynamoDB con Athena
- Automatice las CodeGuru revisiones de Amazon para aplicaciones de AWS CDK Python mediante GitHub Actions
- Automatice la evaluación de recursos de AWS
- Automatice la implementación de aplicaciones anidadas mediante SAM de AWS
- Automatice la implementación de lagos de Supply Chain datos en una configuración de múltiples repositorios
- Automatice la replicación de las instancias de Amazon RDS en Cuentas de AWS
- Automatice la configuración del emparejamiento entre regiones con AWS Transit Gateway
- Archivar automáticamente los elementos en Amazon S3 con DynamoDB TTL
- Detecta automáticamente los cambios e inicia diferentes CodePipeline canalizaciones para un monorepo en CodeCommit
- Cree una arquitectura sin servidor multiusuario en Amazon Service OpenSearch
- Cree un visor de archivos de unidad central avanzada en la nube de AWS
- Calcule el valor en riesgo (VaR) mediante los servicios de AWS
- Copiar los productos de AWS Service Catalog en diferentes cuentas y regiones de AWS
- Crear automáticamente canalizaciones de CI dinámicas para proyectos de Java y Python
- Descomponga monolitos en microservicios mediante CQRS y abastecimiento de eventos
- Implemente una aplicación de una sola página basada en React en Amazon S3 y CloudFront
- Implemente una API de Amazon API Gateway en un sitio web interno mediante puntos de conexión privados y un Equilibrador de carga de aplicación
- Implementar y administrar un lago de datos sin servidor en la nube de AWS mediante el uso de la infraestructura como código
- Implemente un caso de uso de RAG AWS mediante Terraform y Amazon Bedrock
- Desarrollo de un asistente basado en el chat totalmente automatizado con los agentes y las bases de conocimiento de Amazon Bedrock
- Desarrolle asistentes avanzados de IA generativa basados en chat mediante RAG y solicitudes ReAct
- Genere dinámicamente una política de IAM con IAM Access Analyzer mediante Step Functions

- Incorpore componentes visuales de Amazon Quick Sight en aplicaciones web mediante Amazon Cognito y la automatización iAC
- Asegúrese de que el registro de Amazon EMR en Amazon S3 esté habilitado en el lanzamiento
- Estime el costo de una tabla de DynamoDB para la capacidad bajo demanda
- Genere recomendaciones personalizadas y reclasificadas con Amazon Personalize
- Genere datos de prueba con un trabajo de AWS Glue y Python
- Implemente SHA1 el hash para los datos de PII al migrar de SQL Server a PostgreSQL
- Implementar el patrón saga sin servidor mediante AWS Step Functions
- Mejore el rendimiento operativo habilitando Amazon DevOps Guru en varias regiones y cuentas de AWS y OUs con la CDK de AWS
- Lance un CodeBuild proyecto en todas las cuentas de AWS mediante Step Functions y una función de proxy Lambda
- Migración de cargas de trabajo de Apache Cassandra a Amazon Keyspaces mediante AWS Glue
- Supervise el uso de una imagen de máquina de Amazon compartida en múltiples Cuentas de AWS
- Optimice las implementaciones sin servidor con varias cuentas mediante los flujos de trabajo y Actions AWS CDK GitHub
- Organice una canalización de ETL con validación, transformación y particionamiento mediante AWS Step Functions
- Consulta de las tablas de Amazon DynamoDB con SQL mediante Amazon Athena
- Envío de atributos personalizados a Amazon Cognito e ingesta en los tokens
- Sirva contenido estático en un bucket de Amazon S3 a través de una VPC mediante Amazon CloudFront
- Simplificación del desarrollo y la implementación de los bots de Amazon Lex mediante un flujo de trabajo automatizado
- Estructure un proyecto de Python en una arquitectura hexagonal con AWS Lambda
- Traduce el lenguaje natural a consultas (DSL) para consultas de Elasticsearch OpenSearch y consultas de Elasticsearch
- Descarga de datos de un clúster de Amazon Redshift entre las cuentas a Amazon S3
- Coordine la dependencia de los recursos y la ejecución de tareas mediante la construcción AWS Fargate WaitCondition hook
- Uso de agentes de Amazon Bedrock para automatizar la creación de controles de entrada de acceso en Amazon EKS mediante peticiones basadas en texto

Red

Temas

- Automatice la configuración del emparejamiento entre regiones con AWS Transit Gateway
- Centralice la conectividad de red con AWS Transit Gateway
- Configure el cifrado HTTPS para Oracle JD Edwards EnterpriseOne en Oracle WebLogic mediante un Application Load Balancer
- Connect to MGN data and control planes over a private network
- Cree objetos de Infoblox con los recursos CloudFormation personalizados de AWS y Amazon SNS
- Cree una arquitectura IPAM jerárquica y multirregional mediante Terraform AWS
- Personaliza las CloudWatch alertas de Amazon para AWS Network Firewall
- Despliega recursos en una AWS Wavelength zona mediante Terraform
- Migración de registros DNS de forma masiva a una zona alojada privada de Amazon Route 53
- Cómo modificar los encabezados HTTP al migrar de F5 a un equilibrador de carga de aplicación en AWS
- Cree un informe con los hallazgos de Network Access Analyzer sobre el acceso entrante a Internet en múltiples Cuentas de AWS
- Configurar la resolución de DNS para redes híbridas en un entorno de cuentas múltiples AWS
- Verifique que los equilibradores de carga ELB requieran la terminación de TLS
- Visualización de los registros y las métricas de AWS Network Firewall mediante Splunk
- Más patrones

Automatice la configuración del emparejamiento entre regiones con AWS Transit Gateway

Ram Kandaswamy, Amazon Web Services

Resumen

AWS Transit Gatewayconecta nubes privadas virtuales (VPCs) y redes locales a través de un hub central. El tráfico de Transit Gateway no atraviesa la Internet pública, lo que reduce los vectores de amenazas, como las vulnerabilidades más comunes y los ataques de denegación de servicio (DDoS) distribuidos.

Si necesitas comunicarte entre dos o más Regiones de AWS, puedes usar la interconexión de Transit Gateway entre regiones para establecer conexiones de interconexión entre pasarelas de tránsito de diferentes regiones. Sin embargo, la configuración manual de la interconexión entre regiones con Transit Gateway puede resultar compleja y llevar mucho tiempo. Este patrón proporciona una guía para usar la infraestructura como código (IaC) para configurar la interconexión. Puede utilizar este enfoque si tiene que configurar varias regiones de forma repetida y Cuentas de AWS para configurar una organización multirregional.

Este patrón configura una AWS CloudFormationpila que incluye un AWS Step Functions flujo de trabajo, AWS Lambda funciones, roles AWS Identity and Access Management (IAM) y grupos de CloudWatch registros en Amazon Logs. A continuación, ejecute el flujo de trabajo de Step Functions para crear la conexión de peering interregional para sus pasarelas de tránsito.

Requisitos previos y limitaciones

Requisitos previos

- Una activa. Cuenta de AWS
- Un IDE con capacidad de generación de código, como Kiro.
- Un bucket de Amazon Simple Storage Service (Amazon S3) y permisos para cargar objetos en él.
- Pasarelas de tránsito creadas en las regiones solicitantes y aceptadoras.
- VPCs creadas en las regiones solicitantes y aceptadoras. Etiquete VPCs con una `addToTransitGateway` clave con un valor `detrue`.
- Grupos de seguridad configurados para usted de VPCs acuerdo con sus requisitos.
- Listas de control de acceso a la red (ACLs) configuradas para usted VPCs según sus necesidades.

Limitaciones

- Solo algunas Regiones de AWS admiten la interconexión entre regiones. Para ver una lista completa de las regiones que admiten la interconexión entre regiones, consulta la. AWS Transit Gateway FAQs

Arquitectura

El enfoque de desarrollo de la IA entre agencias descrito en este patrón implica los siguientes pasos:

1. Defina el mensaje de automatización: Kiro recibe un mensaje en lenguaje natural en el que se detallan los requisitos de interconexión.
2. Generar script de automatización: Kiro genera los scripts Lambda CloudFormation y los scripts Lambda en función de la solicitud proporcionada.
3. Implemente la pila: Kiro utiliza CloudFormation para implementar los recursos necesarios.
4. Configurar el peering: Kiro ejecuta el flujo de trabajo Step Functions, que llama a las funciones Lambda para crear conexiones de peering y modificar tablas de enrutamiento.

El siguiente diagrama muestra el flujo de trabajo de Step Functions:

El flujo de trabajo consta de los pasos siguientes:

1. El flujo de trabajo de Step Functions llama a la función Lambda para el peering de Transit Gateway.
2. El flujo de trabajo espera un minuto.
3. El flujo de trabajo recupera el estado de emparejamiento y lo envía al bloque de condiciones. El bloque es responsable del bucle.
4. Si no se cumple la condición de éxito, el flujo de trabajo se codifica para entrar en la fase de temporización.
5. Si se cumple la condición de éxito, una función Lambda modifica las tablas de enrutamiento.
6. Finaliza el flujo de trabajo de Step Functions.

Tools (Herramientas)

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todo el Cuentas de AWS mundo Regiones de AWS.
- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas y aplicaciones Servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- AWS Identity and Access Management(IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- Kiro es una herramienta de desarrollo de IA para agencias que le ayuda a crear aplicaciones listas para la producción mediante un desarrollo basado en especificaciones.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Step Functionses un servicio de organización sin servidor que le ayuda a combinar funciones y otras para crear aplicaciones críticas para la empresa. AWS Lambda Servicios de AWS

Epics

Genere código de Lambda y Step Functions

Tarea	Descripción	Habilidades requeridas

Rellenar los marcadores de posición de los mensajes con detalles específicos	1. Actualice el siguiente mensaje sustituyendo los nombres de los cubos Regiones de AWS y:
	`- Active region: ACTIVE_REGION`
	`- Passive region: PASSIVE_REGION`
	`- S3_BUCKET : my-lambda-packages-bucket`
		AWS general, administrador de red

Tarea	Descripción	Habilidades requeridas

```
- STACK_NAME :
 transit-gateway-pe
ering
- All Lambda functions
 use two boto3 EC2
 clients at module
 level (one per
 region), each with
 signature_version v4
 and retries max_attem
pts=1 mode=standard.
- Print all API
 responses for
 CloudWatch logging.
```

2. Guárdalo como un archivo de rebajas.
3. Añada este archivo markdown a su proyecto de Kiro para darle contexto.

> **Note**
>
> Como alternativa, puedes añadirlo como un mensaje en línea que haga referenci a a las variables anteriores sin adjuntar el archivo como contexto.

Tarea	Descripción	Habilidades requeridas
Cree una función Lambda que cree los adjuntos de emparejamiento.	1. En su proyecto de Kiro, introduzca el siguiente mensaje: `Write a Python Lambda that creates a transit gateway peering attachment from active region to passive region. Both of these regions will be read as environment variables of the Lambda function. Use two boto3 EC2 clients at the module level, one per Region. The handler should describe available transit gateways in both Regions. Then check if a peering attachment already exists on the active side by filtering describe_transit_gateway_attachments for resource-type "peering" and states: available, initiatingRequest, modifying, pendingAcceptance, pending, rejected, and rejecting. Only if zero results, create the peering attachment with tags for both Transit Gateway IDs, then wait 60 seconds (AWS`	AWS general, administrador de red, ingeniería rápida

Tarea	Descripción	Habilidades requeridas
	needs this before the passive side can accept), then call accept_transit_gateway_peering_attachment on the passive client. Print all API responses. 2. Guarde este archivo y llámelo `peer-transit-gateway.py` .	

Tarea	Descripción	Habilidades requeridas
Cree una función Lambda que sondee el estado del adjunto entre pares.	1. En su proyecto de Kiro, introduzca la siguiente solicitud: `Using the shared context above, write a Python Lambda that polls peering attachment status. Describe available transit gateways in both regions, then call describe_transit_gateway_attachments on the active client filtered by the active Transit Gateway ID only (no resource-type filter). Return exactly `{'status': status}` where status is the State field from the first attachment. Do not return statusCode or body — the Step Function Choice state reads `$.Payload.status` and compares to "available".` 2. Guarde este archivo y llámelo `get-transit-gateway-peering-status.py` .	AWS general, administrador de red, ingeniería rápida

Tarea	Descripción	Habilidades requeridas
Cree una función Lambda que añada rutas estáticas a ambas regiones.	1. En su proyecto de Kiro, introduzca la siguiente solicitud: `Using the shared context, write a Python Lambda that adds static routes to both regions' TGW route tables. Describe available transit gateways in both Regions, extract each transit gateway's AssociationDefaultRouteTableId. Discover routable VPCs by filtering describe_vpcs with tag `addtotransitgateway=true` in each region, collecting their CIDRs. Get the peering attachment ID from the active side by filtering on the active route table ID. For each passive CIDR, search the active route table using `route-search.exact-match` — only create the route if none found. For each active CIDR, search the passive route table using `route-search.supernet-of-match` (not exact-match —	AWS general, administrador de red

Tarea	Descripción	Habilidades requeridas
	passive side may have supernet routes) — only create if none found. Both sides use the same peering attachment ID. 2. Guarde este archivo y asígnele el nombre. `modify-transit-gateway-routes.py`	

Tarea	Descripción	Habilidades requeridas
Cree la CloudFormation plantilla.	1. Introduzca la siguiente solicitud de orquestación, que crea una CloudFormation plantilla: `Write a CloudFormation JSON template that deploys: three Lambda functions (peer-transit-gateway with 600s timeout, get-transit-gateway-peering-status with 30s timeout, modify-transit-gateway-routes with 600s timeout), Lambda code from an S3 bucket parameter (no default value — user must supply the bucket name at deploy time), a Step Functions state machine, and CloudWatch log groups with 90-day retention. The state machine flow is:`  `1. Invoke peer-transit-gateway` `2. Wait 20 seconds (attachment needs time after the Lambda's internal 20s sleep + acceptance)` `3. Invoke get-transit-gateway-peering-status`	AWS DevOps, AWS general, ingeniería rápida

Tarea	Descripción	Habilidades requeridas
	```4. Choice: if `$.Payload.status` equals "available" # go to step 5, otherwise loop back to step 2 5. Invoke modify-transit-gateway-routes # End Use `Fn::Sub` with Lambda ARN references like `${PeerTransitGateways.Arn}` in the DefinitionString. The polling loop has no max retry — it loops until "available" (typically 3-5 minutes total).``` 2. Guarde y asigne un nombre al archivo `transit-gateway-peering.json` .	

Implemente los AWS recursos

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation pila mediante las indicaciones.	Ingresa la siguiente solicitud: ```Using the outputs from Prompts 1-4, package and deploy the full stack. Steps:```	AWS DevOps, administrador de la nube, AWS general, pronta ingeniería

Tarea	Descripción	Habilidades requeridas
	1. For each of the three Python files from Prompts 1-3, create a zip named after the file (e.g. peer-transit-gateway.zip that contains peer-transit-gateway.py). 2. Upload all three zips to S3_BUCKET. 3. Deploy the CloudFormation template from Prompt 4 to ACTIVE_REGION with S3BucketName=S3_BUCKET and CAPABILITY_NAMED_IAM. 4. Initiate the Step Function from the deployed stack. Zip file names must match the S3Key values in the template exactly.	
Valide la implementación.	1. Supervise el flujo de trabajo de Step Functions para que se complete correctamente. Para obtener instrucciones, consulte la documentación de Step Functions. 2. Compruebe que el estado de interconexión de adjuntos de Transit Gateway esté disponible. Para obtener instrucciones, consulte la documentación de Transit Gateway.	AWS general

Recursos relacionados

- Inicio de ejecuciones de máquinas de estado en Step Functions
- Archivos adjuntos de peering de Transit Gateway
- Interconexión Regiones de AWS mediante VPCs el uso AWS Transit Gateway(vídeo)

Centralice la conectividad de red con AWS Transit Gateway

Mydhili Palagummi y Nikhil Marrapu, Amazon Web Services

Resumen

Este patrón describe la configuración más sencilla en la que se puede usar AWS Transit Gateway para conectar una red local a nubes privadas virtuales (VPCs) en varias cuentas de AWS dentro de una región de AWS. Con esta configuración, puede establecer una red híbrida que conecte varias redes de VPC en una región y una red en las instalaciones. Esto se logra mediante el uso de una puerta de enlace de tránsito y una conexión de red privada virtual (VPN) a la red en las instalaciones.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta para alojar servicios de red, administrada como una cuenta de miembro de una organización en AWS Organizations
- VPCs en varias cuentas de AWS, sin superponer bloques de enrutamiento entre dominios sin clase (CIDR)

Limitaciones

Este patrón no admite el aislamiento del tráfico entre determinadas redes VPCs o entre redes locales. Todas las redes conectadas a la puerta de enlace de tránsito podrán comunicarse entre sí. Para aislar el tráfico, debe usar tablas de enrutamiento personalizadas en la puerta de enlace de tránsito. Este patrón solo conecta la VPCs red local con una única tabla de rutas de Transit Gateway predeterminada, que es la configuración más sencilla.

Arquitectura

Pila de tecnología de destino

- AWS Transit Gateway
- Site-to-SiteVPN DE AWS
- VPC
- AWS Resource Access Manager (AWS RAM)

Arquitectura de destino

Tools (Herramientas)

Servicios de AWS

- AWS Resource Access Manager (AWS RAM) le ayuda a compartir sus recursos de forma segura entre las cuentas de AWS y dentro de su organización o unidades organizativas en AWS Organizations.
- AWS Transit Gateway es un centro central que conecta nubes privadas virtuales (VPCs) y redes locales.

Epics

Crear una puerta de enlace de tránsito en la cuenta de servicios de red

Tarea	Descripción	Habilidades requeridas
Crear una puerta de enlace de tránsito	En la cuenta de AWS en la que desee alojar los servicios de red, cree una puerta de enlace de tránsito en la región de AWS de destino. Para obtener instrucciones, consulte Creación de una puerta de enlace de tránsito. Tenga en cuenta lo siguiente: • Seleccione Default route table association (Asociación de tablas de enrutamiento predeterminada). • Seleccione Default route table propagation (Propagación de tablas de enrutamiento predeterminada).	Administrador de red

Conecte la puerta de enlace de tránsito a su red en las instalaciones

Tarea	Descripción	Habilidades requeridas
Cambio de la puerta de enlace de cliente para una conexión de VPN.	El dispositivo de puerta de enlace del cliente está conectado al lado local de la conexión Site-to-Site VPN entre la puerta de enlace de tránsito y la red local. Para obtener más información, consulte El dispositivo de puerta de enlace del cliente en la documentación de AWS Site-to-Site VPN. Identifique o inicie un dispositivo de cliente en las instalaciones compatible y anote su dirección IP pública. La configuración de la VPN se completará más adelante en esta epopeya.	Administrador de red
En la cuenta de servicios de red, cree una conexión VPC a la puerta de enlace de tránsito.	Para configurar una conexión, cree una conexión VPN para la puerta de enlace de tránsito. Para obtener instrucciones, consulte las conexiones VPN de puerta de enlace de tránsito.	Administrador de red
Configure la VPN en el dispositivo de la puerta de enlace de cliente en las instalaciones.	Descargue el archivo de configuración de la conexión Site-to-Site VPN asociada a la puerta de enlace de tránsito y configure los ajustes de la VPN en el dispositivo de la puerta de enlace del cliente.	Administrador de red

Tarea	Descripción	Habilidades requeridas
	Para obtener las instrucciones, consulte Descargar el archivo de configuración.	

Comparta la puerta de enlace de tránsito de la cuenta de servicios de red con otras cuentas de AWS o con su organización

Tarea	Descripción	Habilidades requeridas
En la cuenta de administración de AWS Organizations, active el uso compartido.	Para compartir la puerta de enlace de tránsito con su organización o con determinadas unidades organizativas, active el uso compartido en AWS Organizations. De lo contrario, tendrá que compartir la puerta de enlace de tránsito de cada cuenta de forma individual. Para obtener instrucciones, consulte Habilitar el uso compartido de recursos en AWS Organizations.	Administrador de sistemas de AWS
Cree el recurso compartido de la puerta de enlace de tránsito en la cuenta de servicios de red.	Para permitir que otras cuentas de AWS de su organización se VPCs conecten a la puerta de enlace de tránsito, en la cuenta de servicios de red, utilice la consola RAM de AWS para compartir el recurso de la puerta de enlace de tránsito. Para obtener instrucciones,	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	consulte Crear un recurso compartido.	

Conéctese VPCs a la pasarela de tránsito

Tarea	Descripción	Habilidades requeridas
Cree adjuntos de VPC en cuentas individuales.	En las cuentas con las que se ha compartido la puerta de enlace de tránsito, cree adjuntos de VPC de la puerta de enlace de tránsito. Para obtener instrucciones, consulte Creación de una conexión de puerta de enlace de tránsito a una VPC.	Administrador de red
Acepte las solicitudes de adjuntos de la VPC.	En la cuenta de servicios de red, acepte las solicitudes de adjuntos de VPC de la puerta de enlace de tránsito. Para obtener instrucciones, consulte Aceptar un archivo adjunto compartido.	Administrador de red

Configuración del enrutamiento

Tarea	Descripción	Habilidades requeridas
Configure las rutas en una cuenta individual VPCs.	En cada VPC de cuenta individual, agregue rutas a la red en las instalaciones y a otras redes de VPC, utilizando la puerta de enlace de tránsito	Administrador de red

Tarea	Descripción	Habilidades requeridas
	como destino. Para obtener instrucciones, consulte Agregar y eliminar rutas de una tabla de enrutamiento.	
Configure la ruta a la tabla de enrutamiento de la puerta de enlace de tránsito.	Las rutas desde VPCs y hacia la conexión VPN deben propagarse y deben aparecer en la tabla de rutas predeterminada de la pasarela de tránsito. Si es necesario, cree cualquier ruta estática (un ejemplo son las rutas estáticas para la conexión VPN estática) en la tabla de enrutamiento predeterminada de la puerta de enlace de tránsito. Para obtener instrucciones, consulte Crear una ruta estática.	Administrador de red
Agregar reglas de grupos de seguridad y listas de control de acceso a la red (ACL).	Para las EC2 instancias y otros recursos de la VPC, asegúrese de que las reglas del grupo de seguridad y las reglas de ACL de la red permitan el tráfico entre VPCs la red local y la red local. Para obtener instrucciones, consulte Controlar el tráfico hacia los recursos mediante grupos de seguridad y Agregar y eliminar reglas de una ACL.	Administrador de red

Prueba de conectividad

Tarea	Descripción	Habilidades requeridas
Pruebe la conectividad entre. VPCs	Asegúrese de que la ACL de la red y los grupos de seguridad permitan el tráfico del Protocolo de mensajes de control de Internet (ICMP) y, a continuación, haga ping desde las instancias de una VPC a otra VPC que también esté conectada a la puerta de enlace de tránsito.	Administrador de red
Pruebe la conectividad entre la red local VPCs y la red local.	Asegúrese de que las reglas de ACL de la red, las reglas de los grupos de seguridad y cualquier firewall permitan el tráfico ICMP y, a continuación, haga ping entre la red local y las instancias de la EC2 misma. VPCs La comunicac ión de red debe iniciarse primero desde la red en las instalaciones para que la conexión VPN recupere el estado UP.	Administrador de red

Recursos relacionados

- Creación de una infraestructura de red de AWS multiVPC escalable y segura (documento técnico de AWS)
- Trabajar con recursos compartidos (documentación de RAM de AWS)
- Cómo trabajar con puertas de enlace de tránsito (documentación de AWS Transit Gateway)

Configure el cifrado HTTPS para Oracle JD Edwards EnterpriseOne en Oracle WebLogic mediante un Application Load Balancer

Thanigaivel Thirumalai, Amazon Web Services

Resumen

Este patrón explica cómo configurar el cifrado HTTPS para la descarga de SSL en Oracle JD Edwards EnterpriseOne en cargas de trabajo de Oracle. WebLogic Este enfoque cifra el tráfico entre el navegador del usuario y un equilibrador de carga para eliminar la carga de cifrado de los servidores. EnterpriseOne

Muchos usuarios escalan el nivel de la máquina virtual EnterpriseOne JAVA (JVM) horizontalmente mediante un AWS Application Load Balancer.El balanceador de cargas actúa como único punto de contacto para los clientes y distribuye el tráfico entrante entre varios. JVMs De forma opcional, el balanceador de cargas puede distribuir el tráfico entre varias zonas de disponibilidad y aumentar la disponibilidad de. EnterpriseOne

El proceso descrito en este patrón configura el cifrado entre el navegador y el equilibrador de carga en lugar de cifrar el tráfico entre el equilibrador de carga y el. EnterpriseOne JVMs Este enfoque se denomina descarga de SSL. Al transferir el proceso de descifrado SSL del servidor EnterpriseOne web o de aplicaciones al Application Load Balancer, se reduce la carga para la aplicación. Tras la finalización del SSL en el equilibrador de cargas, el tráfico no cifrado se enruta a la aplicación en AWS.

Oracle JD Edwards EnterpriseOne es una solución de planificación de recursos empresariales (ERP) para organizaciones que fabrican, construyen, distribuyen, dan servicio o gestionan productos o activos físicos. JD Edwards EnterpriseOne es compatible con varios hardware, sistemas operativos y plataformas de bases de datos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un rol de AWS Identity and Access Management (IAM) con permisos para realizar llamadas de servicio de AWS y gestionar los recursos de AWS
- Un certificado SSL

Versiones de producto

- Este patrón se probó con Oracle WebLogic 12c, pero también puede utilizar otras versiones.

Arquitectura

Existen varios enfoques para realizar la descarga de SSL. Este patrón utiliza un equilibrador de carga de aplicación y un Oracle HTTP Server (OHS), como se ilustra en el siguiente diagrama.

El siguiente diagrama muestra el diseño de la JVM de JD Edwards EnterpriseOne, Application Load Balancer y Java Application Server (JAS).

Tools (Herramientas)

Servicios de AWS

- Los balanceadores de carga de aplicaciones distribuyen el tráfico de aplicaciones entrante entre varios destinos, como Amazon Elastic Compute Cloud (EC2 instancias de Amazon), en varias zonas de disponibilidad.
- AWS Certificate Manager (ACM) le ayuda a crear, almacenar y renovar claves y certificados SSL/TLS X.509 públicos y privados que protegen sus sitios web y aplicaciones de AWS.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.

Prácticas recomendadas

- Para conocer las prácticas recomendadas de ACM, consulte la documentación de ACM.

Epics

Configuración y OHS WebLogic

Tarea	Descripción	Habilidades requeridas
Instale y configure los componentes de Oracle.	1. Instale Fusion Middlewar e Infrastructure siguiendo	JDE CNC, administrador WebLogic

Tarea	Descripción	Habilidades requeridas
	el proceso de instalación estándar. Este programa le ayuda a instalar y configurar un WebLogic dominio. Para obtener instrucciones, consulte la documentación de Oracle. 2. Instale OHS siguiendo el proceso de instalación estándar. Para obtener instrucciones, consulte la documentación de Oracle. 3. Cuando se complete la instalación, inicie el asistente de configuración (archivo `config.sh`) para configurar el OHS. • Puede actualizar un dominio existente o crear uno nuevo. Este patrón supone que está actualizando un dominio existente. • Para ver las Plantillas disponibles, elija Oracle Enterprise Manager-Restricted JRF y Oracle HTTP Server (Restricted JRF). Al seleccionar estas opciones de archivos necesarios de Java (JRF), se elimina la conexión a una base de datos externa.	

Tarea	Descripción	Habilidades requeridas
	• En el caso de los servidores administrados, los clústeres, las plantilla s de servidores, los clústeres de coherencia, los equipos, la asignación de servidores a equipos, los destinos virtuales y las particiones, acepte los valores de configura ción predeterminados y seleccione Siguiente para pasar a la siguiente categoría. • Complete los detalles de configuración (por ejemplo, el host y el puerto del administrador, la dirección y el puerto de escucha y el nombre del servidor) de la instancia de OHS (por ejemplo, `ohs1`).	

Tarea	Descripción	Habilidades requeridas
Habilite el WebLogic complemento a nivel de dominio.	El WebLogic complemento es necesario para equilibrar la carga. Para habilitar el complemento: 1. Inicie sesión en la consola de WebLogic administración mediante el enlace: `http://<WeblogicServer>:<Adminport>/console` 2. Seleccione Bloquear y editar y, a continuación, seleccione Configuración, Aplicaciones web. 3. Seleccione el WebLogic complemento activado (casilla de verificación o opción desplegable). 4. Seleccione Guardar y activar los cambios.	JDE CNC, administrador WebLogic

Tarea	Descripción	Habilidades requeridas

Edite el archivo de configuración .	El `mod_wl_ohs.conf` archivo configura las solicitudes de proxy de OHS a. WebLogic
	
	1. Edite este archivo. Está ubicado en:
	
	`$ORACLE_HOME/user_projects/domains/`
	
	Por ejemplo:
	
	`/home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1`
	2. Agregue los valores de WebLogic host (`WebLogicHost`) y port (`WebLogicPort`) (este patrón asume localhost y el puerto 8000).
	3. Agregue los valores `WLProxySSL` y `WLProxySSLPassThrough` de la siguiente manera:
	
	`<VirtualHost *:8000>`
	`<Location /jde>`
	`WLSRequest On`
		JDE CNC, administrador WebLogic

Tarea	Descripción	Habilidades requeridas

	<pre>SetHandler weblogic-handler
	WebLogicHost localhost
	WebLogicPort 8000
	WLProxySSL On
	WLProxySSLPassThrough On
	</Location>
	</VirtualHost></pre>	

Tarea	Descripción	Habilidades requeridas
Inicie la OHS mediante Enterprise Manager.	1. Inicie sesión en Enterprise Manager Fusion Middlewar e mediante el enlace: `http://<WeblogicSe rver>:<Adminport>/ em/` 2. En Navegación de destino, en Servidor HTTP, seleccione la instancia de OHS (por ejemplo, `ohs1`). 3. Seleccione Apagar and Arrancar para reiniciar la instancia de OHS. 4. Cuando se complete la configuración de OHS, puede conectarse al cliente EnterpriseOne HTML utilizando el nombre de host del servidor HTTP con el puerto 8000 en lugar del nombre de host del EnterpriseOne servidor. • Enlace anterior: `http:// <Webserver>:80/ jde/owhtml` • Nuevo enlace: `http:// <HTTP server or web server>:8000/jde/o whtml` Si utiliza un puerto que no sea el puerto HTTP predeterminado de Oracle,	JDE CNC, administrador WebLogic

Tarea	Descripción	Habilidades requeridas

	edite el archivo `httpd.conf` para añadir un oyente para ese puerto en dos lugares:
	`#[Listen] OHS_LISTEN_PORT`
	`Listen 8000`
	y:
	`#`
	`ServerName <Weblogic Server1>:8000`	

Configure el Equilibrador de carga de aplicación

Tarea	Descripción	Habilidades requeridas
Establezca un grupo de destino.	1. Cree un grupo de destino para el puerto 8000 del servidor HTTP. 2. Registre los destinos en el grupo de objetivos con el mismo puerto. 3. Compruebe el estado de los objetivos para confirmar que están en buen estado. 4. Configure los ajustes de comprobación de estado según sea necesario. Para obtener más instrucciones, consulte la documenta	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	ción de Elastic Load Balancing .	
Configure el equilibrador de carga.	1. Cree un equilibrador de carga de aplicación con los atributos predeterminados y la nube privada virtual (VPC), los grupos de seguridad y las subredes necesarios. Para obtener más instrucciones, consulte la documentación de Elastic Load Balancing. 2. Añada una entrada de oyente para HTTPS 443 y reenvíela al grupo de destino que creó en el paso anterior. (Para obtener más instrucciones, consulte la documentación de Elastic Load Balancing). Un oyente HTTPS requiere un certificado SSL. Puede elegir un certificado de ACM o cargar uno. 3. Para ambos oyentes, habilite la adherencia siguiendo las instrucciones de la documentación de equilibrador de carga elástico.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Adición un registro de DNS de Route 53	(Opcional) Puede añadir un registro DNS de Amazon Route 53 para el subdominio. Este registro apuntaría a su equilibrador de carga de aplicación. Para obtener instrucciones, consulte la documentación de Route 53.	Administrador de AWS

Resolución de problemas

Problema	Solución
El servidor HTTP no aparece.	Si el servidor HTTP no aparece en la lista de Navegación de destino de la consola de Enterprise Manager, siga estos pasos: 1. En WebLogic Dominio, Administración, elija OHS Instances. 2. Elija Crear para crear una nueva instancia de OHS. 3. Proporcione un nombre de instancia y, a continuación, elija Aceptar para crear la instancia. Cuando se haya creado la instancia y se hayan activado los cambios, podrá ver el servidor HTTP en el panel de Navegación de destino.

Recursos relacionados

Documentación de AWS

- Equilibrador de carga de aplicación
- Trabajar con zonas públicas alojadas
- Uso de zonas alojadas privadas

Documentación de Oracle:

- Descripción general del complemento Oracle WebLogic Server Proxy
- Instalación WebLogic del servidor mediante el instalador de infraestructuras
- Instalación y configuración del servidor HTTP de Oracle

Connect to MGN data and control planes over a private network

Dipin Jain y Mike Kuznetsov, Amazon Web Services

Resumen

Este patrón explica cómo puede conectarse a un plano de AWS Transform MGN datos y un plano de control en una red privada y segura mediante puntos finales de VPC de interfaz.

MGN es una solución de elevación y traslado (realojamiento) altamente automatizada que simplifica, agiliza y reduce el costo de migrar aplicaciones a ellas. AWS Permite a las empresas volver a alojar una gran cantidad de servidores físicos, virtuales o en la nube sin problemas de compatibilidad, interrupciones en el rendimiento ni periodos de transición prolongados. MGN está disponible en. Consola de administración de AWS Esto permite una integración perfecta con otros Servicios de AWS AWS CloudTrail, como Amazon CloudWatch e AWS Identity and Access Management (IAM).

Puede conectarse desde un centro de datos de origen a un plano de datos, es decir, a una subred que sirva como área de almacenamiento para la replicación de datos en la VPC de destino Site-to-Site VPN , a través de una conexión privada mediante servicios o interconexión de VPC en MGN. AWS Direct Connect También puede usar puntos finales de VPC de interfaz alimentados por AWS PrivateLink para conectarse a un plano de control MGN a través de una red privada.

Requisitos previos y limitaciones

Requisitos previos

- Subred de área de almacenamiento: antes de configurar MGN, cree una subred para utilizarla como área de almacenamiento provisional para los datos replicados desde sus servidores de origen (es decir, un plano de datos). AWS Debe especificar esta subred en la plantilla de configuración de replicación cuando acceda por primera vez a la consola MGN. Puede anular esta subred para servidores de origen específicos en la plantilla de configuración de replicación. Si bien puede utilizar una subred existente en la suya Cuenta de AWS, le recomendamos que cree una nueva subred dedicada para este fin.
- Requisitos de red: los servidores de replicación que lance MGN en la subred de su área de ensayo deben poder enviar datos al punto final de la API de MGN`https://mgn.<region>.amazonaws.com/`, donde se encuentra el código del lugar en el Región de AWS que `<region>` se está replicando (por ejemplo,). `https://mgn.us-east-1.amazonaws.com` Las URL del servicio Amazon Simple Storage Service (Amazon S3) son necesarias para descargar el software MGN.

- El instalador del agente de AWS replicación debe tener acceso a la URL del bucket de Amazon Simple Storage Service (Amazon S3) Región de AWS del que esté utilizando con MGN.
- La subred del área de almacenamiento debe tener acceso a Amazon S3.
- Los servidores de origen en los que está instalado el agente de AWS replicación deben poder enviar datos a los servidores de replicación de la subred del área de ensayo y al punto final de la API de MGN ubicado en. `https://mgn.<region>.amazonaws.com/`

En la siguiente tabla se muestran los puertos necesarios.

Origen	Destino	Puerto	Para obtener más información, consulte
Su centro de datos de origen	La URL del servicio Amazon S3	443 (TCP)	Comunicación a través del puerto TCP 443
Su centro de datos de origen	Región de AWS-dirección de consola específica para MGN	443 (TCP)	Comunicación entre los servidores de origen y MGN a través del puerto TCP 443
Su centro de datos de origen	Subred de área de almacenamiento	1500 (TCP)	Comunicación entre los servidores de origen y la subred del área de almacenamiento a través del puerto TCP 1500
Subred de área de almacenamiento	Región de AWS-dirección de consola específica para MGN	443 (TCP)	Comunicación entre la subred del área de ensayo y MGN a través del puerto TCP 443

Subred de área de almacenamiento	La URL del servicio Amazon S3	443 (TCP)	Comunicación a través del puerto TCP 443
Subred de área de almacenamiento	Punto final de Amazon Elastic Compute Cloud (Amazon EC2) de la subred Región de AWS	443 (TCP)	Comunicación a través del puerto TCP 443

Limitaciones

Actualmente, MGN no está disponible en todos los sistemas operativos Regiones de AWS .

- Compatible Regiones de AWS
- Sistemas operativos compatibles

Arquitectura

El siguiente diagrama ilustra la arquitectura de red para una migración típica. Para obtener más información sobre esta arquitectura, consulte la documentación de MGN y el vídeo sobre la arquitectura del servicio y la arquitectura de red de MGN.

La siguiente vista detallada muestra la configuración de los puntos finales de la interfaz VPC en el área de ensayo de la VPC para conectar Amazon S3 y MGN.

Tools (Herramientas)

- AWS Transform MGNsimplifica, agiliza y reduce el costo de realojar las aplicaciones. AWS
- Los puntos finales de VPC de interfaz le permiten conectarse a servicios alimentados por AWS PrivateLink sin necesidad de una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o una conexión. AWS Direct Connect Las instancias de su VPC no necesitan direcciones IP públicas para comunicarse con los recursos del servicio. El tráfico entre su VPC y el otro servicio no sale de la red de Amazon.

Epics

Cree puntos de enlace para MGN, Amazon EC2 y Amazon S3

Tarea	Descripción	Habilidades requeridas
Configure el punto final de la interfaz para MGN.	El centro de datos de origen y la VPC del área de ensayo se conectan de forma privada al plano de control de MGN a través del punto final de la interfaz que se crea en la VPC del área de ensayo de destino. Para crear el punto de conexión: 1. Abra la consola de Amazon Virtual Private Cloud (Amazon VPC). 2. En el panel de navegación, seleccione Puntos de conexión, Crear puntos de conexión. 3. En Categoría de servicios, elija Servicios de AWS. 4. En Nombre del servicio, escriba `com.amazonaws.<region>.mgn`. En Tipo, seleccione Interfaz. 5. En VPC, seleccione el espacio provisional de la VPC de destino en la que se va a crear el punto de conexión.	Líder de migración

Tarea	Descripción	Habilidades requeridas
	6. En Subredes, seleccione las subredes en las que se van a crear las interfaces de red de punto de conexión. 7. Para activar el DNS privado en el punto de conexión de la interfaz, en la sección Configuración adicional, seleccione Habilitar el nombre DNS. 8. Seleccione un grupo de seguridad que permita la entrada desde la subred de VPC del área de ensayo a través de TCP 443. 9. Seleccione Crear punto de conexión. Para obtener más información, consulte Acceso y Servicio de AWS uso de un punto final de VPC de interfaz en la documentación de Amazon VPC.	

Tarea	Descripción	Habilidades requeridas
Configure el punto de conexión de interfaz para Amazon EC2.	La VPC del área de ensayo se conecta de forma privada a la API de Amazon EC2 a través del punto de conexión de interfaz que usted crea en la VPC del área de ensayo de destino. Para crear el punto de conexión, siga las instrucciones de la historia anterior. • En nombre del servicio, escriba `com.amazonaws.<region>.ec2` . En Tipo, seleccione Interfaz. • El grupo de seguridad debe permitir el tráfico HTTPS entrante desde la subred de VPC del área de ensayo a través del puerto 443. • En la sección Configuración adicional, seleccione Habilitar el nombre DNS.	Líder de migración

Tarea	Descripción	Habilidades requeridas
Configure el punto de conexión de interfaz para Amazon S3.	El centro de datos de origen y la VPC del área de ensayo se conectan de forma privada a la API de Amazon S3 a través del punto de conexión de interfaz que usted crea en la VPC del área de ensayo de destino. Para crear el punto de conexión, siga las instrucciones que se proporcionan en la primera historia. • En Nombre del servicio, escriba `com.amazonaws.<region>.s3` . En Tipo, seleccione Interfaz. • El grupo de seguridad de VPC debe permitir el tráfico HTTPS entrante desde la subred de VPC del área de ensayo a través del puerto 443. • En la sección Configuración adicional, desactive Habilitar nombre DNS. Los puntos de conexión de tipo interfaz de Amazon S3 no admiten nombres de DNS privados. **Note** Se utiliza un punto de conexión de interfaz porque las conexiones	Líder de migración

Tarea	Descripción	Habilidades requeridas
	de punto de conexión de puerta de enlace no se pueden ampliar más allá de la VPC. (Para obtener más información, consulte la documentación de AWS PrivateLink).	

Tarea	Descripción	Habilidades requeridas
Creación del punto de conexión de la puerta de enlace de Amazon S3.	Durante la fase de configuración, el servidor de replicación debe conectarse a un bucket de S3 para descargar las actualizaciones de software del servidor de AWS replicación. Sin embargo, los puntos de conexión de la interfaz Amazon S3 no admiten nombres de DNS privados y no hay forma de proporcionar un nombre de DNS de punto de conexión de Amazon S3 a un servidor de replicación. Para mitigar este problema, debe crear un punto de conexión de puerta de enlace de Amazon S3 en la VPC a la que pertenece la subred del área de ensayo y actualizar las tablas de rutas de la subred de almacenamiento provisional con las rutas pertinentes. Para obtener más información, consulte Crear un punto final de puerta de enlace en la AWS PrivateLink documentación.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Configure el DNS en las instalaciones para resolver los nombres DNS privados de los puntos de conexión.	Los puntos de enlace de la interfaz de MGN y Amazon EC2 tienen nombres de DNS privados que se pueden resolver en la VPC. Sin embargo, también debe configurar los servidores en las instalaciones para resolver los nombres DNS privados de estos puntos de conexión de la interfaz. Estos servidores se pueden configurar de varias formas. En este patrón, probamos esta funcionalidad reenviando las consultas de DNS locales al punto final de Amazon Route 53 Resolver entrada de la VPC del área de ensayo. Para obtener más informaci ón, consulte Resolución de consultas de DNS entre las VPC y su red en la documenta ción de Route 53.	Ingeniero de migraciones

Conéctese al plano de control MGN a través de un enlace privado

Tarea	Descripción	Habilidades requeridas
Instale el agente de AWS replicación mediante AWS PrivateLink.	1. Descargue el agente de AWS replicación en un depósito de S3 privado en la región de destino.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	2. Inicie sesión en los servidores de origen que desee migrar. El instalador del agente de AWS replicación necesita acceso de red a los puntos de conexión MGN y Amazon S3. Como su red local no está abierta a los puntos de enlace públicos de MGN y Amazon S3, debe instalar el agente con la ayuda de los puntos de enlace de la interfaz que creó en los pasos anteriores mediante. AWS PrivateLink A continuación se muestra un ejemplo para Linux: 1. Descargar el agente mediante el comando: `wget -O ./aws-replication-installer-init.py \ https://aws-application-migration-service-<aws_region>.bucket.<s3-endpoint-DNS-name>/latest/linux/aws-replication-installer-init.py`	

Tarea	Descripción	Habilidades requeridas
	Por ejemplo, si el nombre DNS del punto final de la interfaz Amazon S3 es `vpce-009c8b07adb052a11-qgf8q50y.s3.us-west-1.vpce.amazonaws.com` y Región de AWS es `us-west-1`, utilizaría el comando: `wget -O ./aws-replication-installer-init.py \ https://aws-application-migration-service-us-west-1.bucket.vpce-009c8b07adb052a11-qgf8q50y.s3.us-west-1.vpce.amazonaws.com/latest/linux/aws-replication-installer-init.py` **Note** `bucket` es una palabra clave estática que debe añadir antes del nombre DNS del punto de conexión de la interfaz de Amazon S3. Para obtener más informaci	

Tarea	Descripción	Habilidades requeridas

	ón, consulte la documentación de Amazon S3.
	2. Instalar el agente:
	• Si seleccionó Habilitar el nombre DNS al crear un punto final de interfaz para MGN, ejecute el comando:
	`sudo python3 aws-replication-installer-init.py \ --region <aws_region> \ --aws-access-key-id <access-key> \ --aws-secret-access-key <secret-key> \ --no-prompt \ --s3-endpoint <s3-endpoint-DNS-name>`
	• Si no seleccionó Habilitar el nombre DNS al crear el punto final de la interfaz para MGN, ejecute el comando:
	`sudo python3 aws-replication-installer-init.py \ --region <aws_region> \`	

Tarea	Descripción	Habilidades requeridas

	`--aws-access-key-id <access-key> \`
	`--aws-secret-access-key <secret-key> \`
	`--no-prompt \`
	`--s3-endpoint <s3-endpoint-DNS-name> \`
	`--endpoint <mgn-endpoint-DNS-name>`
	
	Para obtener más información, consulte las instrucciones de instalación AWS del Agente de replicación en la documentación de MGN.
	
	Una vez establecida la conexión con MGN e instalado el agente de AWS replicación, siga las instrucciones de la documentación de MGN para migrar los servidores de origen a la VPC y la subred de destino.	

Recursos relacionados

Documentación de MGN

- Conceptos
- Flujo de trabajo de migración

- Guía de inicio rápido
- Preguntas frecuentes
- Solución de problemas

Recursos adicionales

- Realojar sus aplicaciones en una arquitectura de varias cuentas AWS mediante puntos finales de interfaz de VPC (guía de orientación prescriptiva)AWS
- AWS Transform MGN — Una introducción técnica (tutorial sobre formación y certificación)AWS
- AWS Transform MGN arquitectura y arquitectura de red (vídeo)

Información adicional

Solución de problemas de instalaciones del agente de AWS replicación en servidores Linux

Si recibe un error gcc en un servidor Amazon Linux, configure el repositorio de paquetes y utilice el siguiente comando:

```
## sudo yum groupinstall "Development Tools"
```

Cree objetos de Infoblox con los recursos CloudFormation personalizados de AWS y Amazon SNS

Tim Sutton, Amazon Web Services

Resumen

Aviso: ya no AWS Cloud9 está disponible para nuevos clientes. Los clientes actuales de AWS Cloud9 pueden seguir utilizando el servicio con normalidad. Más información

El sistema de nombres de dominio (DNS), el protocolo de configuración dinámica de host (DHCP) y la administración de direcciones IP (Infoblox DDI) permiten centralizar y controlar de manera eficiente un entorno híbrido complejo. Con Infoblox DDI se pueden descubrir y registrar todos los activos de la red en una base de datos de Administrador de direcciones IP (IPAM) autorizada, además de administrar el DNS en las instalaciones y en la nube de Amazon Web Services (AWS) mediante los mismos dispositivos.

Este patrón describe cómo usar un recurso CloudFormation personalizado de AWS para crear objetos de Infoblox (por ejemplo, registros DNS u objetos de IPAM) mediante una llamada a la API WAPI de Infoblox. Para obtener más información sobre la WAPI de Infoblox, consulte la documentación de la WAPI en la documentación de Infoblox.

Al utilizar el enfoque de este patrón, puede obtener una vista unificada de los registros de DNS y las configuraciones de IPAM para sus entornos de AWS y en las instalaciones, además de eliminar los procesos manuales que crean registros y aprovisionan sus redes. Se puede utilizar el enfoque de este patrón para los casos de uso siguientes:

- Añadir un registro A después de crear una instancia de Amazon Elastic Compute Cloud (Amazon EC2)
- Cómo agregar un registro CNAME después de crear un Equilibrador de carga de aplicación
- Cómo agregar un objeto de red después de crear una nube privada virtual (VPC)
- Proporcionar el rango de redes siguiente y usar ese rango para crear subredes

También puede ampliar este patrón y utilizar otras funciones del dispositivo Infoblox, como agregar diferentes tipos de registros DNS o configurar Infoblox vDiscovery.

El patrón usa un hub-and-spoke diseño en el que el hub requiere conectividad con el dispositivo Infoblox en la nube de AWS o en las instalaciones y usa AWS Lambda para llamar a la

API de Infoblox. El radio se encuentra en la misma cuenta o en una cuenta diferente de la misma organización en AWS Organizations y llama a la función Lambda mediante un recurso CloudFormation personalizado de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Un dispositivo o una red de Infoblox existente, instalado en la nube de AWS, en las instalaciones o en ambos, y configurado con un usuario administrador que puede administrar las acciones de IPAM y DNS. Para obtener más información acerca de este tema, consulte About admin accounts (Acerca de las cuentas de administrador) en la documentación de Infoblox.
- Una zona de DNS autorizada existente a la que desee agregar registros del dispositivo Infoblox. Para obtener más información al respecto, consulte Configuring authoritative zones (Configurar zonas autorizadas) en la documentación de Infoblox.
- Dos cuentas de AWS activas en AWS Organizations. Una cuenta es la cuenta de hub y la otra es la cuenta de spoke.
- Las cuentas de hub y spoke deben estar en la misma región de AWS.
- La VPC de la cuenta de hub debe conectarse al dispositivo Infoblox; por ejemplo, mediante AWS Transit Gateway o interconexión de VPC.
- AWS Serverless Application Model (AWS SAM), instalado y configurado localmente con AWS Cloud9 o AWS. CloudShell
- Los archivos `ClientTest.yaml` y `Infoblox-Hub.zip` (adjuntos), descargados en el entorno local que contiene AWS SAM.

Limitaciones

- El token de servicio del recurso CloudFormation personalizado de AWS debe provenir de la misma región en la que se creó la pila. Se recomienda utilizar una cuenta de hub en cada región, en lugar de crear un tema de Amazon Simple Notification Service (Amazon SNS) en una región y llamar a la función de Lambda en otra región.

Versiones de producto

- Infoblox, versión 2.7

Arquitectura

En los siguientes diagramas se muestra el flujo de este patrón.

El diagrama muestra los siguientes componentes para la solución de este patrón:

1. CloudFormation Los recursos personalizados de AWS le permiten escribir una lógica de aprovisionamiento personalizada en las plantillas que AWS CloudFormation ejecuta al crear, actualizar o eliminar pilas. Al crear una pila, AWS CloudFormation envía una `create` solicitud a un tema de SNS que supervisa una aplicación que se ejecuta en una EC2 instancia.
2. La notificación de Amazon SNS del recurso CloudFormation personalizado de AWS se cifra mediante una clave específica de AWS Key Management Service (AWS KMS) y el acceso está restringido a las cuentas de su organización en Organizations. El tema SNS inicia el recurso de Lambda que llama a la API WAPI de Infoblox.
3. Amazon SNS invoca las siguientes funciones de Lambda que toman la URL de la WAPI de Infoblox, el nombre de usuario y la contraseña () de AWS Secrets Manager Amazon Resource Names () como variables de entorno: ARNs
   - `dnsapi.lambda_handler`— Recibe los `DNSValue` valores `DNSNameDNSType`, y del recurso CloudFormation personalizado de AWS y los utiliza para crear registros A de DNS y CNAME.
   - `ipaddr.lambda_handler`— Recibe los `Network Name` valoresVPCCIDR, `TypeSubnetPrefix`, y del recurso CloudFormation personalizado de AWS y los utiliza para añadir los datos de la red a la base de datos de IPAM de Infoblox o para proporcionar al recurso personalizado la siguiente red disponible que se pueda utilizar para crear nuevas subredes.
   - `describeprefixes.lambda_handler`: Llama a la API de AWS `describe_managed_prefix_lists` mediante el filtro `"com.amazonaws."+Region+".s3"` para recuperar el `prefix ID` necesario.

   > **Important**
   >
   > Estas funciones Lambda están escritas en Python y son similares entre sí, pero se llaman de forma diferente. APIs

4. Puede implementar la red de Infoblox como dispositivos de red físicos, virtuales o basados en la nube. Se puede implementar en las instalaciones o como un dispositivo virtual mediante una variedad de hipervisores, incluidos VMware ESXi Microsoft Hyper-V, Linux KVM y Xen. También

puede implementar la cuadrícula de Infoblox en la nube de AWS con una Imagen de máquina de Amazon (AMI).

5. El diagrama muestra una solución híbrida para la red de Infoblox que proporciona DNS e IPAM a los recursos en la nube de AWS y en las instalaciones.

Pila de tecnología

- AWS CloudFormation
- IAM
- AWS KMS
- AWS Lambda
- SAM de AWS
- AWS Secrets Manager
- Amazon SNS
- Amazon VPC

Tools (Herramientas)

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Organizations es un servicio de administración de cuentas que le permite agrupar varias cuentas de AWS en una organización que usted crea y administra de manera centralizada.
- AWS Secrets Manager le permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.

- AWS Serverless Application Model (AWS SAM) es un marco de código abierto que permite crear aplicaciones sin servidor en la nube de AWS.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Código

Puede usar la CloudFormation plantilla de AWS de `ClientTest.yaml` muestra (adjunta) para probar el centro de Infoblox. Puede personalizar la CloudFormation plantilla de AWS para incluir los recursos personalizados de la siguiente tabla.

Crear un registro A con el recurso personalizado de spoke de Infoblox	Valores devueltos:
	`infobloxref` : referencias de Infoblox
	Recurso de ejemplo:
	`ARECORDCustomResource:`
	`  Type: "Custom::InfobloxAPI"`
	`  Properties:`
	`  ServiceToken: !Sub arn:aws:sns:${AWS::Region}:${HubAccountID}:RunInfobloxDNSFunction`
	`  DNSName: 'arecordtest.company.com'`
	`  DNSType: 'ARecord'`
	`  DNSValue: '10.0.0.1'`

crear un registro de CNAME con el recurso personalizado de spoke de Infoblox

Valores devueltos:

`infobloxref` : referencias de Infoblox

Recurso de ejemplo:

```
CNAMECustomResource:

  Type: "Custom::InfobloxAPI"

  Properties:

    ServiceToken: !Sub arn:aws:sns:
${AWS::Region}:${HubAccountID}:Ru
nInfoblox

    DNSFunction

    DNSName: 'cnametest.company.com'

    DNSType: 'cname'

    DNSValue: 'aws.amazon.com'
```

crear un objeto de red utilizando el recurso personalizado de spoke de Infoblox	Valores devueltos:
	`infobloxref` : referencias de Infoblox
	`network`: Rango de red (igual a `VPCCIDR`)
	Recurso de ejemplo:
	`VPCCustomResource:`
	`  Type: 'Custom::InfobloxAPI'`
	`  Properties:`
	`  ServiceToken: !Sub arn:aws:sns:${AWS::Region}:${HubAccountID}:RunInfobloxNextSubnetFunction`
	`  VPCCIDR: !Ref VpcCIDR`
	`  Type: VPC`
	`  NetworkName: My-VPC`

Recuperar la subred disponible siguiente mediante el recurso personalizado de spoke de Infoblox	Valores devueltos:
	`infobloxref` : referencias de Infoblox
	`network` : El rango de redes de la subred
	Recurso de ejemplo:
	`Subnet1CustomResource:`
	`  Type: 'Custom::InfobloxAPI'`
	`  DependsOn: VPCCustomResource`
	`  Properties:`
	`  ServiceToken: !Sub  arn:aws:sns:${AWS::Region}:${HubAccountID}:RunInfobloxNextSubnetFunction`
	`  VPCCIDR: !Ref VpcCIDR`
	`  Type: Subnet`
	`  SubnetPrefix: !Ref SubnetPrefix`
	`NetworkName: My-Subnet`

Epics

Crear y configurar la VPC de la cuenta de hub

Tarea	Descripción	Habilidades requeridas
Crear una VPC con una conexión al dispositivo Infoblox.	Inicie sesión en la consola de administración de AWS de su cuenta de hub y cree una VPC siguiendo los pasos de Amazon VPC en la implementación de referencia de inicio	Administrador de red, administrador del sistema

Tarea	Descripción	Habilidades requeridas
	rápido de la nube de AWS en los inicios rápidos de AWS. **Important** La VPC debe tener conectividad HTTPS con el dispositivo Infoblox y se recomienda utilizar una subred privada para esta conexión.	

Tarea	Descripción	Habilidades requeridas
(Opcional) Cree los puntos de conexión de VPC para las subredes privadas.	Los puntos de conexión de VPC proporcionan conectividad a los servicios públicos para las subredes privadas. Se necesitan los puntos de conexión siguientes: • Un punto de enlace para Amazon Simple Storage Service (Amazon S3) que permite a Lambda comunicarse con AWS CloudFormation • Un punto de conexión de interfaz a Secrets Manager para permitir la conectividad con Secrets Manager • Un punto de conexión de interfaz a AWS KMS que permita el cifrado del tema de SNS y del secreto de Secrets Manager Para obtener más información acerca de la creación de puntos de conexión para las subredes privadas, consulte VPC endpoints (Puntos de conexión de VPC) de la documentación de Amazon VPC.	Administrador de red, administrador del sistema

Implementar el hub de Infoblox

Tarea	Descripción	Habilidades requeridas
Cree la plantilla SAM de AWS.	1. Ejecute el comando `unzip Infoblox-Hub.zip` en el entorno que contiene AWS SAM. 2. Ejecute el comando `cd Hub/` para cambiar su directorio al directorio `Hub`. 3. Ejecute el comando `sam build` para procesar el archivo de plantilla SAM de AWS, el código de la aplicación y cualquier archivo y dependencia específicos del idioma. El comando `sam build` también copia los artefactos de construcción en el formato y la ubicación esperados para la siguiente historia.	Desarrollador, administrador del sistema
Implemente la plantilla SAM de AWS.	El `sam deploy` comando toma los parámetros necesarios y los guarda en el `samconfig.toml` archivo, almacena la CloudFormation plantilla de AWS y las funciones de Lambda en un bucket de S3 y, a continuación, implementa la CloudFormation plantilla de AWS en su cuenta de hub.	Desarrollador, administrador del sistema

Tarea	Descripción	Habilidades requeridas

	El código de ejemplo siguiente muestra cómo implementar la plantilla AWS SAM:
	
	`$ sam deploy --guided`
	
	`Configuring SAM deploy`
	`==========`
	`==`
	`Looking for config file [samconfig.toml] : Found`
	`Reading default arguments : Success`
	`Setting default arguments for 'sam deploy'`
	`==========`
	`==========`
	`==========`
	`Stack Name [Infoblox-Hub]:`
	`AWS Region [eu-west-1]:`
	`Parameter InfobloxUsername:`
	`Parameter InfobloxPassword:`
	`Parameter InfobloxIPAddress [xxx.xxx.xx.xxx]:`
	`Parameter AWSOrganisationID [o-xxxxxxxxx]:`
	`Parameter VPCID [vpc-xxxxxxxxx]:`
	`Parameter VPCCIDR [xxx.xxx.xxx.xxx/16]:`	

Tarea	Descripción	Habilidades requeridas
	Parameter VPCSubnetID1 [subnet-xxx]: Parameter VPCSubnetID2 [subnet-xxx]: Parameter VPCSubnetID3 [subnet-xxx]: Parameter VPCSubnetID4 []: #Shows you resources changes to be deployed and require a 'Y' to initiate deploy Confirm changes before deploy [Y/n]: y #SAM needs permission to be able to create roles to connect to the resources in your template Allow SAM CLI IAM role creation [Y/n]: n Capabilities [['CAPABILITY_NAMED_IAM']]: Save arguments to configuration file [Y/n]: y SAM configuration file [samconfig.toml]: SAM configuration environment [default]: **Important** Debe utilizar la opción `--guided` cada vez,	

Tarea	Descripción	Habilidades requeridas
	ya que las credencia les de inicio de sesión de Infoblox no se almacenan en el archivo `samconfig .toml` .	

Recursos relacionados

- Cómo empezar a WAPIs usar Postman (blog de Infoblox)
- Provisioning vNIOS for AWS Using the BYOL Model (Aprovisionar vNIOS para AWS mediante el modelo BYOL) (documentación de Infoblox)
- quickstart-aws-vpc(repositorio) GitHub
- describe_managed_prefix_lists (documentación de AWS SDK para Python)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Cree una arquitectura IPAM jerárquica y multirregional mediante Terraform AWS

Donny Schreiber, Amazon Web Services

Resumen

La administración de direcciones IP (IPAM) es un componente esencial de la administración de redes y se vuelve cada vez más compleja a medida que las organizaciones escalan su infraestructura en la nube. Sin la IPAM adecuada, las organizaciones corren el riesgo de que se produzcan conflictos con las direcciones IP, se desperdicie espacio en las direcciones y se resuelvan problemas complejos que pueden provocar interrupciones y tiempo de inactividad en las aplicaciones. Este patrón demuestra cómo implementar una solución de IPAM integral para AWS entornos empresariales mediante Terraform. HashiCorp Ayuda a las organizaciones a crear una arquitectura de IPAM jerárquica y multirregional que facilita la administración centralizada de las direcciones IP en todos los componentes de la organización. Cuentas de AWSAWS

Este patrón lo ayuda a implementar el Administrador de direcciones IP de Amazon VPC con una sofisticada jerarquía de grupos de cuatro niveles: grupo de nivel superior, grupos regionales, grupos de unidades de negocio y grupos específicos del entorno. Esta estructura permite realizar una gobernanza adecuada de las direcciones IP y, al mismo tiempo, permite delegar la administración de direcciones IP en los equipos correspondientes de la organización. La solución utiliza AWS Resource Access Manager (AWS RAM) para compartir sin problemas los grupos de administradores de direcciones IP en toda la organización. AWS RAM centraliza y estandariza las especificaciones de IPAM, que los equipos pueden utilizar en todas las cuentas gestionadas.

Este patrón lo ayuda a lograr lo siguiente:

- Automatice la asignación de direcciones IP en todas las Regiones de AWS unidades de negocio y los entornos.
- Aplicar las políticas de red de la organización mediante la validación con programación.
- Escalar la infraestructura de red de manera eficiente a medida que evolucionan los requisitos de la empresa.
- Reducir la sobrecarga operativa mediante la administración centralizada de los espacios de direcciones IP.
- Acelerar las implementaciones de cargas de trabajo nativas en la nube con la asignación de rangos de CIDR de autoservicio.

- Evitar gestionar los conflictos mediante la validación y los controles basados en políticas.

Requisitos previos y limitaciones

Requisitos previos

- Uno o más Cuentas de AWS, administrados como una organización en AWS Organizations.
- Una cuenta de administración de redes o de centro de redes que servirá como administrador delegado del Administrador de direcciones IP.
- AWS Command Line Interface (AWS CLI), instalado y configurado.
- La versión 1.5 o posterior de Terraform instalada.
- AWS Proveedor de Terraform, configurado.
- Permisos para administrar el administrador de direcciones IP y las nubes privadas virtuales (VPCs) configuradas en AWS Identity and Access Management (IAM). AWS RAM

Limitaciones

- El Administrador de direcciones IP está sujeto a las cuotas de servicio. La cuota de servicio predeterminada para los grupos es de 50 por ámbito. Al ejecutar esta implementación en 6 regiones, 2 unidades de negocio y 4 entornos, se crearían 67 grupos. Por lo tanto, podría ser necesario incrementar la cuota.
- Al modificar o eliminar los grupos del Administrador de direcciones IP una vez asignados los recursos, podrían surgir problemas de dependencias. Primero debe liberar la asignación antes de poder eliminar el grupo.
- En el Administrador de direcciones IP, la supervisión de los recursos puede experimentar un ligero retraso a la hora de reflejar los cambios en los recursos. Este retraso puede ser de 20 minutos aproximadamente.
- El Administrador de direcciones IP no puede aplicar la unicidad de las direcciones IP en distintos ámbitos de forma automática.
- Las etiquetas personalizadas deben cumplir con las prácticas recomendadas en materia de etiquetado de AWS. Por ejemplo, cada clave debe ser única y no puede empezar por `aws:`.
- Hay ciertas consideraciones y limitaciones a la hora de integrar el Administrador de direcciones IP con cuentas externas a su organización.

Arquitectura

Arquitectura de destino

Configuración y jerarquía de grupos del Administrador de direcciones IP

En el siguiente diagrama se ilustran los constructos lógicos de la arquitectura de destino. Un ámbito es el contenedor de nivel más alto del Administrador de direcciones IP. Cada ámbito representa el espacio de direcciones IP de una única red. Los grupos son conjuntos de rangos continuos de direcciones IP (o rangos de CIDR) dentro del ámbito. Los grupos lo ayudan a organizar las direcciones IP según sus necesidades de enrutamiento y seguridad. En este diagrama se ilustran cuatro niveles jerárquicos de grupos: un grupo de nivel superior, grupos regionales, grupos de unidades de negocio y grupos de entornos.

Esta solución establece una jerarquía clara de grupos del Administrador de direcciones IP:

1. El grupo de nivel superior comprende todo el espacio de direcciones IP de la organización, como `10.176.0.0/12`.
2. Los grupos regionales son para las asignaciones específicas de una región, como `10.176.0.0/15` para `us-east-1`.
3. Los grupos de unidades de negocio son asignaciones específicas de dominio dentro de cada uno de ellos. Región de AWS Por ejemplo, la unidad de negocios de finanzas de la región `us-east-1` podría tener `10.176.0.0/16`.
4. Los grupos de entornos son asignaciones con una finalidad específica para diferentes entornos. Por ejemplo, la unidad de negocios de finanzas de la región `us-east-1` podría tener `10.176.0.0/18` para un entorno de producción.

Esta topología de implementación distribuye geográficamente los recursos del Administrador de direcciones IP y, al mismo tiempo, mantiene el control centralizado. Sus características son las siguientes:

- El administrador de direcciones IP se implementa en un único servidor principal. Región de AWS
- Las regiones adicionales se registran como regiones operativas, donde el Administrador de direcciones IP puede administrar los recursos.
- Cada región operativa recibe un grupo de direcciones dedicado del grupo de nivel superior.

- Los recursos de todas las regiones operativas se administran de forma centralizada a través del Administrador de direcciones IP en la región principal.
- Cada grupo regional tiene una propiedad de configuración regional vinculada a su región que lo ayuda a asignar los recursos de forma adecuada.

Validación avanzada del rango de CIDR

Esta solución está diseñada para evitar que se implementen configuraciones que no sean válidas. Al implementar los grupos a través de Terraform, se valida lo siguiente durante la fase de planificación de Terraform:

- Valida que todos los rangos de CIDR del entorno estén contenidos dentro de los rangos de CIDR de las unidades de negocio principales
- Confirma que todos los rangos de CIDR de la unidad de negocio estén contenidos dentro de los rangos de CIDR regionales principales
- Verifica que todos los rangos de CIDR regionales estén contenidos en los rangos de CIDR de nivel superior
- Comprueba si hay rangos de CIDR solapados dentro del mismo nivel jerárquico
- Valida la asignación adecuada de los entornos a sus respectivas unidades de negocio

Asignación de rangos de CIDR

El siguiente diagrama muestra un ejemplo de cómo los desarrolladores o administradores pueden crear direcciones IP nuevas VPCs y asignarlas desde los niveles del grupo.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. A través de la Consola de administración de AWS infraestructura como código (IaC) o mediante la infraestructura como código (IaC), un desarrollador o administrador solicita el siguiente rango de CIDR disponible en el grupo de `AY3` entornos. AWS CLI
2. El Administrador de direcciones IP asigna el siguiente rango de CIDR disponible en ese grupo a la VPC `AY3-4`. Este rango de CIDR ya no se puede utilizar.

Automatización y escala

Esta solución está diseñada para ofrecer escalabilidad de la siguiente manera:

- Expansión regional: para agregar nuevas regiones, amplíe la configuración de Terraform con entradas adicionales del grupo regional.
- Crecimiento de las unidades de negocio: para admitir las nuevas unidades de negocio, agréguelas al mapa de configuración de las unidades de negocio.
- Flexibilidad del entorno: configure distintos tipos de entornos, como entornos de desarrollo o producción, en función de las necesidades de la organización.
- Soporte multicuenta: comparta grupos entre todas las cuentas de su organización a través de. AWS RAM
- Aprovisionamiento automatizado de VPC: intégrelo con los flujos de trabajo de aprovisionamiento de VPC para automatizar la asignación de rangos de CIDR.

La estructura jerárquica también permite diferentes escalas de delegación y control, como las siguientes:

- Los administradores de red pueden administrar los grupos regionales y de nivel superior.
- Es posible que los equipos de TI de las unidades de negocio hayan delegado el control de sus grupos respectivos.
- Los equipos de aplicaciones pueden consumir direcciones IP de los grupos de entornos designados.

> **Note**
>
> También puede integrar esta solución con el Generador de cuentas de AWS Control Tower para Terraform (AFT). Para obtener más información, consulte Integración con AFT en la sección Información adicional de este patrón.

Tools (Herramientas)

Servicios de AWS

- Amazon le CloudWatch ayuda a supervisar las métricas de sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar Servicios de AWS mediante comandos en su shell de línea de comandos.

- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar múltiples cuentas Cuentas de AWS en una organización que puede crear y administrar de forma centralizada.
- AWS Resource Access Manager (AWS RAM) le ayuda a compartir sus recursos de forma segura Cuentas de AWS para reducir la sobrecarga operativa y ofrecer visibilidad y capacidad de auditoría.
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS. El Administrador de direcciones IP es una característica de Amazon VPC. Le ayuda a planificar, rastrear y monitorear las direcciones IP de sus cargas de AWS trabajo.

Otras herramientas

- HashiCorp Terraform es una herramienta de infraestructura como código (IaC) que facilita usar el código para aprovisionar y administrar los recursos y la infraestructura en la nube.

Repositorio de código

El código de este patrón está disponible en el repositorio de ejemplo de implementación de Terraform para el IPAM jerárquico. AWS GitHub La estructura del repositorio incluye lo siguiente:

- Módulo raíz: variables de entrada y orquestación de la implementación.
- Módulo de IPAM: implementación básica de la arquitectura que se describe en este patrón.
- Módulo de etiquetas: etiquetado estandarizado para todos los recursos.

Prácticas recomendadas

Tenga en cuenta las siguientes prácticas recomendadas para la planificación de redes:

- Planifique primero: planifique minuciosamente el espacio de direcciones IP antes de la implementación. Para obtener más información, consulte Planificar el aprovisionamiento de direcciones IP.
- Evite el solapamiento de rangos de CIDR: asegúrese de que los rangos de CIDR de cada nivel no se solapen.

- Reserve espacio en el búfer: asigne siempre rangos de CIDR más grandes de lo que necesite inmediatamente para adaptarse al crecimiento.
- Documente la asignación de direcciones IP: mantenga la documentación de la estrategia de asignación de direcciones IP.

Tenga en cuenta las siguientes prácticas recomendadas para la implementación:

- Comience con entornos que no sean de producción: haga implementaciones primero en entornos que no sean de producción.
- Utilice la administración de estados de Terraform: implemente el almacenamiento y el bloqueo de estados remotos. Para obtener más información, consulte State storage and locking en la documentación de Terraform.
- Implemente el control de versiones: controle las versiones de todo el código de Terraform.
- Implemente CI/CD la integración: utilice los canales de integración continua y entrega continua (CI/CD) para realizar despliegues repetibles.

Tenga en cuenta las siguientes prácticas operativas recomendadas:

- Habilite la importación automática: configure un grupo del Administrador de direcciones IP para detectar e importar automáticamente los recursos existentes. Siga las instrucciones que se indican en Edición de un grupo de IPAM para activar la importación automática.
- Supervise la utilización de direcciones IP: configure alarmas para los umbrales de utilización de direcciones IP. Para obtener más información, consulta Supervisar el IPAM con Amazon CloudWatch.
- Realice auditorías periódicas: audite periódicamente el uso y el cumplimiento de las direcciones IP. Para obtener más información, consulte Seguimiento del uso de direcciones IP en IPAM.
- Elimine las asignaciones sin utilizar: libere las asignaciones de direcciones IP cuando se retiren los recursos. Para obtener más información, consulte Eliminar el aprovisionamiento CIDRs de un grupo.

Tenga en cuenta las siguientes prácticas recomendadas en materia de seguridad:

- Implemente privilegios mínimos: utilice los roles de IAM con los permisos mínimos necesarios. Para obtener más información, consulte Prácticas recomendadas de seguridad en IAM y Identity and Access Management en IPAM.

- Utilice políticas de control de servicios: implemente políticas de control de servicios (SCPs) para imponer el uso del administrador de direcciones IP en su organización. Para obtener más información, consulte Exigir el uso de IPAM para la creación de VPC con. SCPs
- Controle el uso compartido de recursos: administre cuidadosamente el alcance del uso compartido de recursos del Administrador de direcciones IP en. AWS RAM Para obtener más información, consulte Compartir un grupo de IPAM mediante AWS RAM.
- Implemente el etiquetado: implemente el etiquetado obligatorio para todos los recursos relacionados con el Administrador de direcciones IP. Para obtener más información, consulte Estrategia de etiquetado en la sección Información adicional.

Epics

Configuración de una cuenta de administrador delegado para el Administrador de direcciones IP

Tarea	Descripción	Habilidades requeridas
Habilite las AWS Organizations funciones.	Asegúrese de que AWS Organizations tiene todas las funciones habilitadas. Para obtener instrucciones, consulte Habilitar todas las funciones para una organización AWS Organizations en la AWS Organizations documentación.	Administrador de AWS
Habilite el uso compartido de recursos en AWS RAM.	Con el AWS CLI, introduzca el siguiente comando para habilitar el uso compartido de AWS RAM recursos en su organización: `aws ram enable-sharing-with-aws-organization` Para obtener más información, consulte Habilitar el uso	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	compartido de recursos AWS Organizations en la AWS RAM documentación.	

Tarea	Descripción	Habilidades requeridas
Designe un administrador para el Administrador de direccion es IP.	Desde la cuenta de administr ación de la organización AWS CLI, introduzca el siguiente comando, donde `123456789 012` aparece el ID de la cuenta que administrará el Administrador de direcciones IP: `aws ec2 enable-ipam-organization-admin-account \ --delegated-admin-account-id 123456789 012` **Note** Generalmente, las cuentas de redes o centro de redes se usan como administr ador delegado del Administrador de direcciones IP. Para obtener más informaci ón, consulte Integrar el IPAM con las cuentas de una AWS organización en la documenta ción del Administrador de direcciones IP.	Administrador de AWS

Implementación de la infraestructura

Tarea	Descripción	Habilidades requeridas
Defina la arquitectura de red.	Defina y documente la arquitectura de red, incluidos los rangos de CIDR de las regiones, unidades de negocio y entornos. Para obtener más información, consulte Planificar el aprovisionamiento de direcciones IP en la documentación del Administrador de direcciones IP.	Ingeniero de redes
Clonar el repositorio.	1. Introduzca el siguiente comando para clonar el repositorio en la estación de trabajo local: `git clone https://github.com/aws-samples/sample-amazon-vpc-ipam-terraform.git` 2. Introduzca el siguiente comando para ir al directorio `terraform` .	DevOps ingeniero
Configure las variables.	1. Abra el archivo terraform.tfvars. 2. Configure las variables para la implementación del Administrador de direcciones IP. Para ver un ejemplo de un archivo completo, consulte terraform.tfvars.e	Ingeniero de redes, Terraform

Tarea	Descripción	Habilidades requeridas
	xample en el repositorio de código. 3. Guarde y cierre el archivo terraform.tfvars.	

Implemente los recursos del Administrador de direcciones IP.	1. Introduzca el comando siguiente para inicializar Terraform:
	`terraform init`
	2. Introduzca el comando siguiente para generar un plan de ejecución:
	`terraform plan`
	3. Revise el plan y valide los recursos y los component es de infraestructura que se van a crear.
	4. Introduzca el siguiente comando para implementar la infraestructura:
	`terraform apply`
	5. Cuando se le solicite, introduzca sí para confirmar la implementación.
	6. Espere hasta que se complete la implement ación.
		Terraform

Tarea	Descripción	Habilidades requeridas
Valide la implementación.	1. Inicie sesión en la consola del administrador de direcciones IP y Cuenta de AWS, a continuación, ábrala. 2. En el panel de navegación, elija Pools (Grupos). 3. En la lista de grupos, compruebe que se hayan creado los grupos que configuró. 4. Abra la consola de AWS RAM. 5. Compruebe que se hayan compartido los recursos del Administrador de direccion es IP. Siga las instrucci ones de Visualización de recursos compartidos que creó en la AWS RAM documentación.	AWS general, ingeniero de redes

Cree VPCs y configure la supervisión

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	Siga los pasos que se indican en Creación de una VPC en la documentación de Amazon VPC. Cuando llegue al paso donde debe elegir un rango de CIDR para la VPC, asigne el siguiente rango disponible de	AWS general, administrador de redes, ingeniero de redes

Tarea	Descripción	Habilidades requeridas
	uno de los grupos regionales, de unidades de negocio y de entornos.	
Valide la asignación de rangos de CIDR.	1. Abra la consola del Administrador de direcciones IP. 2. En el panel de navegación, elija Panel. 3. En el panel, compruebe que el rango de CIDR se haya asignado a la VPC que creó.	AWS general, administrador de redes, ingeniero de redes
Supervise el Administrador de direcciones IP.	Configure la supervisión y las alarmas relacionadas con la asignación de los recursos del Administrador de direcciones IP. Para obtener más información e instrucciones, consulta Supervisar el IPAM con Amazon CloudWatch y Supervisar el uso del CIDR por recurso en la documentación del administrador de direcciones IP.	AWS general

Tarea	Descripción	Habilidades requeridas
Imponga el uso del Administrador de direcciones IP.	Cree una política de control de servicios (SCP) AWS Organizations que exija a los miembros de su organización utilizar el administrador de direcciones IP al crear una VPC. Para obtener instrucciones, consulte Exigir el uso de IPAM para la creación de VPC en la SCPs documentación del Administrador de direcciones IP.	AWS general, administrador de AWS

Resolución de problemas

Problema	Solución
Se produce un error en Terraform y no se encuentra el recurso del Administrador de direcciones IP	Asegúrese de que la cuenta de administrador del administrador de direcciones IP esté debidamente delegada y de que su AWS proveedor esté autenticado en esa cuenta.
Se produce un error en la asignación de rangos de CIDR	Compruebe que el rango de CIDR solicitado se ajuste al rango disponible del grupo del Administrador de direcciones IP y no se solape con las asignaciones existentes.
AWS RAM problemas de uso compartido	Compruebe que el uso compartido de recursos esté habilitado en su AWS organización. Compruebe que el principal correcto, el Amazon Resource Name (ARN) de la organización, se utilice en el AWS RAM recurso compartido.

Problema	Solución
Errores de validación de la jerarquía de grupos	Asegúrese de que los rangos de CIDR del grupo secundario estén correctamente contenidos dentro de los rangos de CIDR del grupo principal y no se solapen con los grupos del mismo nivel.
Se ha superado el límite de cuota del Administrador de direcciones IP	Solicite un aumento de cuota para los grupos del Administrador de direcciones IP. Para obtener más información, consulte Solicitud de aumento de cuota en la Guía del usuario de Service Quotas.

Recursos relacionados

Servicio de AWS documentación

- Documentación del Administrador de direcciones IP de Amazon VPC
- AWS Resource Access Manager documentación
- AWS Organizations documentación

AWS publicaciones de blog

- Administración de grupos de IP en todas VPCs las regiones mediante Amazon VPC IP Address Manager
- Network address management and auditing at scale with Amazon VPC IP Address Manager

Videos y tutoriales

- AWS re:Invent 2022: prácticas recomendadas para el diseño de Amazon VPC y la IPAM (0) NET31
- AWS re:Invent 2022: diseño de VPC avanzado y nuevas capacidades (01) NET4

Información adicional

Integración con AFT

Puede integrar esta solución con AWS Control Tower Account Factory for Terraform (AFT) para asegurarse de que las cuentas recién aprovisionadas reciban automáticamente las configuraciones de red adecuadas. Al implementar esta solución de IPAM en su cuenta central de red, las nuevas cuentas creadas a través de AFT pueden hacer referencia a los grupos de administradores de direcciones IP compartidos al crearlos. VPCs

El siguiente ejemplo de código muestra la integración de AFT en la personalización de una cuenta mediante AWS Systems Manager Parameter Store:

```
# Get the IP Address Manager pool ID from Parameter Store
data "aws_ssm_parameter" "dev_ipam_pool_id" {
  name = "/org/network/ipam/finance/dev/pool-id"
}

# Create a VPC using the IP Address Manager pool
resource "aws_vpc" "this" {
  ipv4_ipam_pool_id   = data.aws_ssm_parameter.dev_ipam_pool_id.value
  ipv4_netmask_length = 24

  tags = {
    Name = "aft-account-vpc"
  }
}
```

Estrategia de etiquetado

La solución implementa una estrategia de etiquetado integral para simplificar la administración de los recursos. En el siguiente ejemplo de código se muestra cómo se usa:

```
# Example tag configuration
module "tags" {
  source = "./modules/tags"

  # Required tags
  product_name  = "enterprise-network"
  feature_name  = "ipam"
  org_id        = "finance"
  business_unit = "network-operations"
```

```
  owner         = "network-team"
  environment   = "prod"
  repo          = "https://github.com/myorg/ipam-terraform"
  branch        = "main"
  cost_center   = "123456"
  dr_tier       = "tier1"

  # Optional tags
  optional_tags = {
    "project"    = "network-modernization"
    "stack_role" = "infrastructure"
  }
}
```

Estas etiquetas se aplican automáticamente a todos los recursos del Administrador de direcciones IP. Esto simplifica la coherencia de la gobernanza, la asignación de costos y la administración de recursos.

Personaliza las CloudWatch alertas de Amazon para AWS Network Firewall

Jason Owens, Amazon Web Services

Resumen

El patrón te ayuda a personalizar las CloudWatch alertas de Amazon generadas por AWS Network Firewall. Puede utilizar reglas predefinidas o crear reglas personalizadas que determinen el mensaje, los metadatos y la gravedad de las alertas. A continuación, puedes actuar en función de estas alertas o automatizar las respuestas de otros servicios de Amazon, como Amazon EventBridge.

En este patrón, se generan reglas de firewall compatibles con Suricata. Suricata es un motor de detección de amenazas de código abierto. Primero debe crear reglas sencillas y, a continuación, probarlas para confirmar que las CloudWatch alertas se han generado y registrado. Una vez que haya probado correctamente las reglas, las modificará para definir los mensajes personalizados, los metadatos y la gravedad y, a continuación, volverá a probarlas para confirmar las actualizaciones.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.
- AWS Command Line Interface (AWS CLI) instalado y configurado en su estación de trabajo Linux, macOS o Windows. Para obtener más información, consulte Instalación o actualización de la versión de AWS CLI más reciente.
- AWS Network Firewall instalado y configurado para usar CloudWatch Logs. Para obtener más información, consulte Registrar el tráfico de red desde AWS Network Firewall.
- Una instancia de Amazon Elastic Compute Cloud (Amazon EC2) en una subred privada de una nube privada virtual (VPC) que está protegida por Network Firewall.

Versiones de producto

- Para la versión 1 de AWS CLI, utilice la versión 1.18.180 o posterior. Para la versión 2 de AWS CLI, utilice la 2.1.2 o una versión posterior.
- El archivo classification.config de la versión 5.0.2 de Suricata. Para obtener una copia de este archivo de configuración, consulte la sección Información adicional.

Arquitectura

El diagrama de la arquitectura muestra el flujo de trabajo siguiente:

1. Una EC2 instancia de Amazon en una subred privada realiza una solicitud mediante curl o Wget.
2. Network Firewall procesa el tráfico y genera una alerta.
3. Network Firewall envía las alertas registradas a CloudWatch Logs.

Tools (Herramientas)

Servicios de AWS

- Amazon le CloudWatch ayuda a supervisar las métricas de sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.
- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas y aplicaciones Servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar Servicios de AWS mediante los comandos de su consola de línea de comandos.
- AWS Network Firewalles un firewall de red gestionado y activo y un servicio de detección y prevención de intrusiones para nubes privadas virtuales () en el. VPCs Nube de AWS

Otras herramientas

- curl es una herramienta y biblioteca de línea de comandos de código abierto.
- GNU Wget es una herramienta de línea de comandos gratuita.

Epics

Crear las reglas y el grupo de reglas del firewall

Tarea	Descripción	Habilidades requeridas
Cree reglas.	1. En un editor de texto, cree una lista de reglas que desee agregar al firewall.	Administrador de sistemas de AWS, administrador de red

Tarea	Descripción	Habilidades requeridas

	Cada regla debe estar en una línea independiente. El valor del parámetro `classtype` proviene del archivo de configuración de clasificación predeterminado de Suricata. Para obtener el archivo de configuración completo, consulte la sección Información adicional. A continuación se muestran dos ejemplos de reglas.
	
	`alert http any any -> any any (content:"badstuff"; classtype:misc-activity; sid:3; rev:1;)`
	`alert http any any -> any any (content:"morebadstuff"; classtype:bad-unknown; sid:4; rev:1;)`
	
	2. Guarde las reglas en un archivo denominado `custom.rules` .	

Tarea	Descripción	Habilidades requeridas

Cree un grupo de reglas.	En AWS CLI, introduzca el siguiente comando. De este modo se crea el grupo de reglas.
	
	`# aws network-firewall create-rule-group \ --rule-group-name custom --type STATEFUL \ --capacity 10 --rules file://custom.rules \ --tags Key=environment,Value=development`
	
	El siguiente es un ejemplo de salida. Anote el `RuleGroup Arn` , que necesitará en un paso posterior.
	
	`{ "UpdateToken": "4f998d72-973c-490a-bed2-fc3460547e23", "RuleGroupResponse": { "RuleGroupArn": "arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom", "RuleGroupName": "custom", "RuleGroupId": "238a8259-9eaf-48bb-90af-5e690cf8c48b",`
		Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas

	<pre>"Type": "STATEFUL",
	"Capacity": 10,
	"RuleGroupStatus": "ACTIVE",
	"Tags": [
	{
	"Key": "environment",
	"Value": "development"
	}
	]
	}</pre>	

Actualizar la política de firewall

Tarea	Descripción	Habilidades requeridas

Obtenga el ARN de la política de firewall.	En AWS CLI, introduzca el siguiente comando. Esto devuelve el nombre de recurso de Amazon (ARN) de la política de firewall. Registre el ARN para su uso posterior en este patrón.
	<pre># aws network-firewall describe-firewall \
	--firewall-name aws-network-firewall-anfw \
	--query 'Firewall.FirewallPolicyArn'</pre>
		Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	A continuación se muestra un ejemplo de ARN que devuelve este comando. `"arn:aws:network-firewall:us-east-2:1234567890:firewall-policy/firewall-policy-anfw"`	

Tarea	Descripción	Habilidades requeridas

Actualice la política de firewall.	En un editor de texto, copie y pegue el siguiente código. Reemplace `<RuleGroupArn>` por el valor que registró en la sección Epics anterior. Guarde el archivo como `firewall-policy-anfw.json` .
	
	`{`
	`  "StatelessDefaultActions": [`
	`  "aws:forward_to_sfe"`
	`  ],`
	`  "StatelessFragmentDefaultActions": [`
	`  "aws:forward_to_sfe"`
	`  ],`
	`  "StatefulRuleGroupReferences": [`
	`  {`
	`  "ResourceArn": "<RuleGroupArn>"`
	`  }`
	`  ]`
	`}`
	
	Introduzca el comando siguiente en la AWS CLI. Este comando requiere un update token (actualizar token) para agregar las nuevas reglas. El token se usa para confirmar que la política no ha cambiado
		Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas

	desde la última vez que se recuperó.
	
	`UPDATETOKEN=(`aws network-firewall describe-firewall-policy \ --firewall-policy-name firewall-policy-anfw \ --output text --query UpdateToken`)`
	
	`aws network-firewall update-firewall-policy \ --update-token $UPDATETOKEN \ --firewall-policy-name firewall-policy-anfw \ --firewall-policy file://firewall-policy-anfw.json`	

Tarea	Descripción	Habilidades requeridas

Confirme las actualizaciones de la política.	(Opcional) Si desea confirmar que se añadieron las reglas y ver el formato de la política, introduzca el comando siguiente en la AWS CLI.
	`# aws network-firewall describe-firewall-policy \ --firewall-policy-name firewall-policy-anfw \ --query FirewallPolicy`
	El siguiente es un ejemplo de salida.
	`{ "StatelessDefaultActions": [ "aws:forward_to_sfe" ], "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ], "StatefulRuleGroupReferences": [ { "ResourceArn": "arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom" }`
		Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	<pre>] }</pre>	

Probar la funcionalidad de las alertas

Tarea	Descripción	Habilidades requeridas

Genere alertas para las pruebas.	1. Inicie sesión en una estación de trabajo de prueba dentro de la subred del firewall.
	2. Ingrese los comandos que deberían generar alertas. Puede utilizar, por ejemplo `wget` o `curl`.
	<pre>wget -U "badstuff"
	 http://www.amazon.
	com -o /dev/null</pre>
	<pre>curl -A "morebads
	tuff" http://ww
	w.amazon.com -o /
	dev/null</pre>
		Administrador de sistemas de AWS

Valide que las alertas estén registradas.	1. Abra la consola de CloudWatch . 2. Navegue hasta el grupo de registros y el flujo correctos. Para obtener más información, consulte Ver los datos de registro enviados a CloudWatch	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas

	Logs (documentación de CloudWatch Logs).
	3. Confirme que los eventos de registro son similares a los ejemplos siguientes. Los ejemplos muestran solo la parte relevante de la alerta.
	
	Ejemplo 1
	
	`"alert": { "action": "allowed", "signature_id": 3, "rev": 1, "signature": "", "category": "Misc activity", "severity": 3 }`
	
	Ejemplo 2
	
	`"alert": { "action": "allowed", "signature_id": 4, "rev": 1, "signature": "", "category": "Potentially Bad Traffic", "severity": 2`	

Tarea	Descripción	Habilidades requeridas
	`}`	

Actualizar las reglas y el grupo de reglas del firewall

Tarea	Descripción	Habilidades requeridas
Actualice las reglas del firewall.	1. Abra el archivo `custom.rules` en un editor de texto. 2. Cambie la primera regla para que sea similar a la siguiente. Esta regla debe escribirse en una sola línea del archivo. `alert http any any -> any any (msg:"Watch out - Bad Stuff!!"; content:"badstuff"; classtype:misc-activity; priority:2; sid:3; rev:2; metadata:custom-field-2 Danger!, custom-field More Info;)` De este modo, se realizan los siguientes cambios en la regla: • Se agrega una cadena msg (sitio web de Suricata) que proporciona información textual sobre la firma o la alerta. En la	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	alerta generada, esto se asigna a la firma. • Se ajusta la prioridad predeterminada (sitio web de Suricata) de `misc-activity` , que pasa de 3 a 2. Para ver los valores predeterminados de los distintos `classtypes` , consulte la sección Información adicional. • Se agregan metadatos personalizados (sitio web de Suricata) a la alerta. Se trata de información adicional que se agrega a la firma. Se recomienda utilizar pares clave-valor. • Se cambia la rev (sitio web de Suricata) de 1 a 2. Esto representa la versión de la firma.	

Tarea	Descripción	Habilidades requeridas

Actualice el grupo de reglas.	En AWS CLI, ejecute los siguientes comandos. Utilice el ARN de su política de firewall. Estos comandos obtienen un token de actualización y actualizan el grupo de reglas con los cambios de las reglas.
	`# UPDATETOKEN=(`aws network-firewall \ describe-rule-group \ --rule-group-arn arn:aws:network-firewall:us-east-2:123457890:stateful-rulegroup/custom \ --output text --query UpdateToken`)`
	`# aws network-firewall update-rule-group \ --rule-group-arn arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom \ --rules file://custom.rules \ --update-token $UPDATETOKEN`
	El siguiente es un ejemplo de salida.
	`{`
		Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	"UpdateToken": "7536939f-6a1d-414c-96d1-bb28110996ed", "RuleGroupResponse": { "RuleGroupArn": "arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom", "RuleGroupName": "custom", "RuleGroupId": "238a8259-9eaf-48bb-90af-5e690cf8c48b", "Type": "STATEFUL", "Capacity": 10, "RuleGroupStatus": "ACTIVE", "Tags": [{ "Key": "environment", "Value": "development" }] } }	

Probar la funcionalidad de la alerta actualizada

Tarea	Descripción	Habilidades requeridas
Genere una alerta para probarla.	1. Inicie sesión en una estación de trabajo de prueba dentro de la subred del firewall.	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	2. Ingrese un comando que genere una alerta. Por ejemplo, puede utilizar `curl`. `curl -A "badstuff" http://www.amazon.com -o /dev/null`	

Tarea	Descripción	Habilidades requeridas
Valide la alerta modificada.	1. Abra la consola de CloudWatch . 2. Navegue hasta el grupo de registros y el flujo correctos. 3. Confirme que el evento de registro sea similar al ejemplo siguiente. El ejemplo solo muestra la parte pertinente de la alerta. `"alert": { "action": "allowed", "signature_id": 3, "rev": 2, "signature": "Watch out - Bad Stuff!!", "category": "Misc activity", "severity": 2, "metadata": { "custom-field": [ "More Info" ], "custom-field-2": [ "Danger!" ] } }`	Administrador de sistemas de AWS

Recursos relacionados

Referencias

- Envía alertas desde AWS Network Firewall un canal de Slack (guíaAWS prescriptiva)
- Ampliando la prevención de amenazas AWS con Suricata (entrada del blog)AWS
- Modelos de despliegue para AWS Network Firewall (AWS entrada de blog)
- Suricata meta keyworks (Claves meta de Suricata) (documentación de Suricata)

Tutoriales y videos

- AWS Network Firewall taller

Información adicional

A continuación se muestra el archivo de configuración de clasificación de Suricata 5.0.2. Estas clasificaciones se utilizan al crear las reglas de firewall.

```
# config classification:shortname,short description,priority

config classification: not-suspicious,Not Suspicious Traffic,3
config classification: unknown,Unknown Traffic,3
config classification: bad-unknown,Potentially Bad Traffic, 2
config classification: attempted-recon,Attempted Information Leak,2
config classification: successful-recon-limited,Information Leak,2
config classification: successful-recon-largescale,Large Scale Information Leak,2
config classification: attempted-dos,Attempted Denial of Service,2
config classification: successful-dos,Denial of Service,2
config classification: attempted-user,Attempted User Privilege Gain,1
config classification: unsuccessful-user,Unsuccessful User Privilege Gain,1
config classification: successful-user,Successful User Privilege Gain,1
config classification: attempted-admin,Attempted Administrator Privilege Gain,1
config classification: successful-admin,Successful Administrator Privilege Gain,1

# NEW CLASSIFICATIONS
config classification: rpc-portmap-decode,Decode of an RPC Query,2
config classification: shellcode-detect,Executable code was detected,1
config classification: string-detect,A suspicious string was detected,3
config classification: suspicious-filename-detect,A suspicious filename was detected,2
```

```
config classification: suspicious-login,An attempted login using a suspicious username
 was detected,2
config classification: system-call-detect,A system call was detected,2
config classification: tcp-connection,A TCP connection was detected,4
config classification: trojan-activity,A Network Trojan was detected, 1
config classification: unusual-client-port-connection,A client was using an unusual
 port,2
config classification: network-scan,Detection of a Network Scan,3
config classification: denial-of-service,Detection of a Denial of Service Attack,2
config classification: non-standard-protocol,Detection of a non-standard protocol or
 event,2
config classification: protocol-command-decode,Generic Protocol Command Decode,3
config classification: web-application-activity,access to a potentially vulnerable web
 application,2
config classification: web-application-attack,Web Application Attack,1
config classification: misc-activity,Misc activity,3
config classification: misc-attack,Misc Attack,2
config classification: icmp-event,Generic ICMP event,3
config classification: inappropriate-content,Inappropriate Content was Detected,1
config classification: policy-violation,Potential Corporate Privacy Violation,1
config classification: default-login-attempt,Attempt to login by a default username and
 password,2

# Update
config classification: targeted-activity,Targeted Malicious Activity was Detected,1
config classification: exploit-kit,Exploit Kit Activity Detected,1
config classification: external-ip-check,Device Retrieving External IP Address
 Detected,2
config classification: domain-c2,Domain Observed Used for C2 Detected,1
config classification: pup-activity,Possibly Unwanted Program Detected,2
config classification: credential-theft,Successful Credential Theft Detected,1
config classification: social-engineering,Possible Social Engineering Attempted,2
config classification: coin-mining,Crypto Currency Mining Activity Detected,2
config classification: command-and-control,Malware Command and Control Activity
 Detected,1
```

Despliega recursos en una AWS Wavelength zona mediante Terraform

Zahoor Chaudhrey y Luca Iannario, Amazon Web Services

Resumen

AWS Wavelength lo ayuda a crear una infraestructura optimizada para aplicaciones de computación de periferia de acceso múltiple (MEC). Las Wavelength Zones son despliegues de AWS infraestructura que incorporan servicios de AWS cómputo y almacenamiento en las redes 5G de los proveedores de servicios de comunicaciones (CSP). El tráfico de aplicaciones de los dispositivos 5G llega a los servidores de aplicaciones que se ejecutan en zonas de Wavelength sin salir de la red de telecomunicaciones. Lo siguiente facilita la conectividad de red a través de Wavelength:

- Nubes privadas virtuales (VPCs): VPCs Cuenta de AWS pueden extenderse para abarcar varias zonas de disponibilidad, incluidas las Wavelength Zones. Las instancias de Amazon Elastic Compute Cloud (Amazon EC2) y los servicios relacionados aparecen como parte de tu VPC regional. VPCs se crean y administran en Amazon Virtual Private Cloud (Amazon VPC).
- Puerta de enlace del operador: una puerta de enlace del operador permite la conectividad desde la subred de la zona de longitud de onda a la red del CSP, Internet o Región de AWS a través de la red del CSP. Una puerta de enlace de operador tiene dos propósitos. Permite el tráfico entrante desde una red de CSP en una ubicación específica y permite el tráfico saliente a la red de telecomunicaciones e Internet.

Este patrón y el código Terraform asociado le ayudan a lanzar recursos, como EC2 instancias de Amazon, volúmenes de Amazon Elastic Block Store (Amazon EBS), subredes y una puerta de enlace VPCs portadora, en una Wavelength Zone.

Requisitos previos y limitaciones

Requisitos previos

- ¿Un activo Cuenta de AWS
- Un entorno de desarrollo integrado (IDE)
- Optar por la zona de Wavelength de destino
- AWS Command Line Interface (AWS CLI), instalado y configurado
- La versión 1.8.4 o posterior de Terraform instalada (documentación de Terraform)

- Terraform AWS Provider, versión 5.32.1 o posterior, configurada (documentación de Terraform)
- Git, instalado (GitHub)
- Permisos para crear recursos de Amazon VPC, Wavelength y Amazon EC2

Limitaciones

No todas son Regiones de AWS compatibles con Wavelength Zones. Para obtener más información, consulte Zonas de Wavelength disponibles en la documentación de Wavelength.

Arquitectura

El siguiente diagrama muestra cómo puede crear una subred y AWS recursos en una Wavelength Zone. VPCs que contienen una subred en una Wavelength Zone pueden conectarse a una puerta de enlace portadora. Una puerta de enlace de operador le permite conectarse a los siguientes recursos:

- Dispositivos 4G/LTE y 5G en la red del operador de telecomunicaciones.
- Acceso inalámbrico fijo para socios selectos de la zona de Wavelength. Para obtener más información, consulte Acceso múltiple AWS Wavelength.
- Tráfico saliente a recursos públicos de Internet.

Tools (Herramientas)

Servicios de AWS

- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.
- AWS Wavelengthextiende la Nube de AWS infraestructura a las redes 5G de los proveedores de telecomunicaciones. Le ayuda a crear aplicaciones que ofrecen latencias extremadamente bajas para dispositivos móviles y usuarios finales.

Otras herramientas

- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub Creating AWS Wavelength Infrastructure using Terraform. El código de Terraform implementa la siguiente infraestructura y recursos:

- Una VPC
- Una zona de Wavelength
- Una subred pública en la zona de Wavelength
- Una puerta de enlace de operador de la zona de Wavelength
- Una EC2 instancia de Amazon en la Wavelength Zone

Prácticas recomendadas

- Antes de la implementación, confirme que utiliza las últimas versiones de Terraform y la AWS CLI.
- Utilice una canalización de integración y entrega continuas (CI/CD) para implementar la IaC. Para obtener más información, consulte las prácticas recomendadas para administrar los archivos de estado de Terraform en AWS CI/CD Pipeline en los blogs. AWS

Epics

Aprovisione la infraestructura

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Introduzca el siguiente comando para clonar en su entorno el repositorio AWS Wavelength Creating Infrastructure using Terraform. `git clone git@github.com:aws-samples/terraform-waveleng th-infrastructure. git`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Actualice las variables.	1. Navegue hasta el repositorio clonado. `cd terraform-wavelength-infrastructure` 2. Con cualquier editor de texto, cree un archivo llamado terraform.tfvars en el directorio raíz. 3. Cree las siguientes variables e introduzca sus valores: • `region = <enter Region name>` • `vpc_cidr = <enter CIDR block used by VPC>` • `wavelength_subnet_cidr = <enter CIDR block for the subnet in the Wavelength Zone>` • `availabilityzone_wavelength = <enter Wavelength Zone name>` 4. Guarde el archivo terraform.tfvars.	DevOps ingeniero, Terraform

Tarea	Descripción	Habilidades requeridas
Inicialice la configuración.	Introduzca el comando siguiente para inicializar el directorio de trabajo. `terraform init`	DevOps ingeniero, Terraform
Obtenga una vista previa del plan Terraform.	Introduzca el siguiente comando para comparar el estado objetivo con el estado actual de su AWS entorno. Este comando genera una vista previa de los recursos que se configurarán. `terraform plan`	DevOps ingeniero, Terraform

Tarea	Descripción	Habilidades requeridas
Compruébelo e impleméntelo.	1. Revise los cambios de configuración en el plan de Terraform y confirme que desea implementarlos. 2. Introduzca el comando siguiente para aplicar el plan y crear la infraestr uctura. `terraform apply` 3. Introduzca `yes` para continuar. Terraform crea la arquitectura que se declara en los archivos de configura ción. Para obtener más información, consulte la sección Arquitectura de destino de este patrón.	DevOps ingeniero, Terraform

Validar y limpiar

Tarea	Descripción	Habilidades requeridas
Verifique la implementación de la infraestructura.	1. Si aún no tienes una EC2 instancia de Amazon en una subred pública Región de AWS, crea una. Para obtener instrucciones, consulte Lanzamiento de la instancia de Linux o Lanzamiento de la instancia de Windows. Utilizará esta instancia para probar	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	la conectividad desde la Región de AWS Wavelength Zone. 2. Pruebe la conectividad de la instancia de la Región de AWS a la instancia de la Wavelength Zone. Para obtener instrucciones, consulte Probar la conectividad en la documentación de Wavelength.	
(Opcional) Limpieza de la infraestructura.	Si necesita eliminar todos los recursos que aprovisionó Terraform, haga lo siguiente: 1. Escriba el siguiente comando. `terraform destroy` 2. Escriba `yes` para confirmar.	DevOps ingeniero, Terraform

Resolución de problemas

Problema	Solución
Conectividad con EC2 las instancias de Amazon en Región de AWS.	Consulte Solución de problemas de conexión a la instancia de Linux o Solución de problemas de conexión a la instancia de Windows.
Conectividad con las EC2 instancias de Amazon en la Wavelength Zone.	Consulte Solucionar problemas de conectividad SSH o RDP con mis EC2 instancias lanzadas en una Wavelength Zone.

Problema	Solución
Capacidad en la zona de Wavelength.	Consulte Cuotas y consideraciones para las zonas de Wavelength.
Conectividad móvil o de operador desde la red del operador a la Región de AWS.	1. Compruebe que la puerta de enlace del operador esté operativa. Haga lo siguiente: a. Abra la Consola de Amazon VPC. b. En el panel de navegación, selecciona Tu. VPCs c. Seleccione la VPC que contiene la zona de Wavelength. d. En el panel de detalles, para Puerta de enlace del operador, confirme que el valor está adjunto. 2. Compruebe que todas las direcciones IP elásticas adjuntas a las instancias de la zona de Wavelength estén operativas. Haga lo siguiente: a. Abre la EC2 consola de Amazon. b. En el panel de navegación, seleccione Instances (Instancias). c. Seleccione la instancia en la zona de Wavelength. d. Seleccione la pestaña Red. e. Confirme que la interfaz de red elástica tenga una dirección IP elástica adjunta. 3. Póngase en contacto con el equipo de soporte de la red del operador.

Recursos relacionados

- ¿Qué es AWS Wavelength?
- ¿Cómo AWS Wavelength funciona?

- Resiliencia en AWS Wavelength

Migración de registros DNS de forma masiva a una zona alojada privada de Amazon Route 53

Ram Kandaswamy, Amazon Web Services

Resumen

Este patrón automatiza la migración masiva de registros DNS a una zona alojada en Amazon Route 53. Utiliza un script de Python con el AWS SDK para Python (Boto3) para leer los datos de los registros de un archivo JSON almacenado en Amazon Simple Storage Service (Amazon S3) y crear los registros mediante programación mediante la API de Route 53.

Si su sistema de origen exporta archivos de zona BIND estándar, la función de importación nativa de Route 53 o cli53 (una herramienta CLI de código abierto mantenida por la comunidad y a la que no está AWS afiliada) pueden gestionar la migración sin necesidad de crear scripts personalizados. Sin embargo, en muchos entornos empresariales, los registros de DNS se encuentran en hojas de cálculo de Excel y no en archivos de zona. Las exportaciones de Excel suelen contener problemas de calidad de los datos, como espacios que no se dividen y caracteres Unicode, que las herramientas de importación estándar no resuelven. Este patrón corrige ese vacío: lee datos de Excel y limpia los datos para crear registros de principio a fin.

Utilice este patrón cuando necesite migrar una gran cantidad de registros DNS de un sistema existente a una zona alojada de Route 53 sin tener que crear cada registro manualmente a través de la consola.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Hoja de cálculo de Excel que contiene registros de zonas alojadas con columnas para el nombre de dominio completo (FQDN), el tipo de registro, el tiempo de vida (TTL) y el valor
- Python 3.12 o posterior (consulte Descargar Python)
- La biblioteca Python de pandas instalada () `pip3 install pandas`
- Familiaridad con los tipos de registros DNS, como los registros A, NAPTR y SRV (consulte Tipos de registros DNS compatibles)
- Familiaridad con el lenguaje Python y sus bibliotecas

Limitaciones

- Este patrón no utiliza todas las propiedades disponibles de la llamada a la `change_resource_record_sets` API. Amplíe el código según sea necesario para su caso de uso.
- En la hoja de cálculo de Excel, se supone que el valor de cada fila es único. Se espera que aparezcan varios valores para cada FQDN en la misma fila. Si no es así, modifique el código para concatenar varios valores para el mismo FQDN.
- Este patrón llama directamente a la API de Route 53 mediante Boto3. Puede mejorar el código para utilizar un AWS CloudFormation contenedor para los `update_stack` comandos `create_stack` y, además, utilizar los valores de JSON para rellenar los recursos de la plantilla.
- Si su sistema de origen puede exportar registros en formato de archivo de zona BIND, considere utilizar la función de importación de Route 53 en su lugar.
- Algunos AWS servicios no están disponibles en todos Regiones de AWS. Para conocer la disponibilidad regional, consulta AWSlos servicios por región. Para ver los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

1. El usuario carga una hoja de cálculo de Excel con los datos del registro de DNS en un bucket de Amazon S3.
2. Un script de Python que se ejecuta localmente (o en un IDE como Kiro) lee el archivo JSON del bucket de Amazon S3 mediante Boto3.
3. El script procesa los registros y llama a la operación de la `change_resource_record_sets` API de Route 53 para crear registros en la zona alojada.

Tools (Herramientas)

Servicios de AWS

- Route 53: proporciona la zona hospedada donde se crean los registros DNS. Este patrón utiliza las operaciones `create_hosted_zone` y `change_resource_record_sets` API.
- Amazon S3: almacena el archivo JSON que contiene los datos del registro DNS que se van a migrar.

Otras herramientas

- Kiro: un IDE con capacidades de inteligencia artificial para agentes, que se utiliza para desarrollar y ejecutar el script de migración de Python. Para obtener más información, consulte Kiro.
- pandas: una biblioteca de análisis de datos de Python que se utiliza para convertir la hoja de trabajo de Excel al formato JSON.

Prácticas recomendadas

- Pruebe con un pequeño subconjunto de 5 a 10 registros antes de ejecutar el script en todos los registros para comprobar el formato de los datos y corregir la creación de registros.
- Utilice la `UPSERT` acción en lugar de. `CREATE` La `UPSERT` acción crea un registro si no existe o lo actualiza si existe. Esto hace que el script sea idempotente y seguro para volver a ejecutarlo.
- Batch tus cambios para mantenerlos dentro de los límites de las `ChangeResourceRecordSets` solicitudes. Cuando usas la `UPSERT` acción, cada `ResourceRecord` elemento cuenta dos veces para alcanzar el máximo de 1000 elementos.
- Valide los datos antes de insertarlos. Compruebe que los FQDN terminan con un punto (`.`), que los valores TTL son enteros positivos y que los tipos de registro coinciden con los tipos de registros DNS admitidos.
- Realice una copia de seguridad de los registros existentes antes de realizar cambios masivos. Exporte los registros de la zona alojada actual utilizándolos `list_resource_record_sets` para proporcionar un punto de reversión.
- Implemente una lógica de reintentos con un retraso exponencial para gestionar los límites de velocidad de las API de Route 53. Para obtener más información, consulte Reintentos de error y retrocesos exponenciales en. AWS
- Siga el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte las mejores prácticas de seguridad y conceder privilegios mínimos en la documentación AWS Identity and Access Management (IAM).

Epics

Prepare los datos para la automatización

Tarea	Descripción	Habilidades requeridas
Cree un archivo de Excel para sus registros.	1. Exporte los registros de su sistema DNS actual. 2. Cree una hoja de cálculo de Excel con estas columnas: `FqdnNameRecordTyp e ,,Value,TTL`. 3. Para los registros NAPTR y SRV, utilice la función CONCAT de Excel para combinar varios valores de propiedades en la columna. `Value` 4. Compruebe que cada FQDN termine con un punto (`.`) y que los valores TTL sean enteros positivos. Fila de ejemplo: FqdnN Recor Valor TTL e somet A 192.0. 900 .exam org	Ingeniero de datos
Convierta los datos de la hoja de cálculo de Excel a JSON.	1. Compruebe que Python 3.12 o posterior esté instalado ejecutándolo	Ingeniero de datos, desarroll ador de Python

Tarea	Descripción	Habilidades requeridas

	`python3 --version` en el terminal.
	2. Instala la biblioteca de pandas ejecutándola `pip3 install pandas --user` en la terminal.
	3. Cree un archivo Python con el siguiente código para convertir la hoja de cálculo de Excel a JSON:
	`import pandas as pd`
	`data=pd.read_excel('./Book1.xls')`
	`data.to_json(path_or_buf='my.json',orient='records')`
	1. Ejecute el script. Compruebe que el archivo de salida `my.json` contiene los registros esperados.	

Cargue el archivo JSON en un bucket de Amazon S3.	1. Cree un bucket de Amazon S3 si aún no existe uno. Para obtener más información, consulte Crear un bucket en la documentación de Amazon S3. 2. Sube el `my.json` archivo al bucket.	Desarrollador de aplicaciones

Inserta registros en la zona alojada

Tarea	Descripción	Habilidades requeridas

Cree una zona alojada.	1. Cree un archivo Python con el siguiente código para crear una zona alojada. Reemplace <hosted-zone-name> <vpc-region> , y <vpc-id> con sus valores.
	
	`import boto3`
	`import random`
	
	`hostedZoneName ="xxx"`
	`vpcRegion = "us-east-1"`
	`vpcId="vpc-xxxx"`
	`route53_client = boto3.client('route53')`
	`response = route53_client.create_hosted_zone(`
	`Name= hostedZoneName,`
	`VPC={`
	`'VPCRegion': vpcRegion,`
	`'VPCId': vpcId`
	`},`
	`CallerReference=str(random.random()*100000),`
	`HostedZoneConfig={`
	`'Comment': "private hosted zone`
		Ingeniero en la nube, administrador de redes, con habilidades de Python

Tarea	Descripción	Habilidades requeridas

	<pre>created by automation",
	'PrivateZone': True
	}
	)
	
	print(response)</pre>
	1. Ejecute el script y anote el ID de la zona hospedada de la respuesta.
	
	También puede utilizar una herramienta de infraestructura como código (IaC), por ejemplo, AWS CloudFormation para reemplazar estos pasos por una plantilla que cree una pila con los recursos y propiedades adecuados. Para obtener más información, consulte AWS Route 53::HostedZone en la CloudFormation documentación.	

Tarea	Descripción	Habilidades requeridas

Lea los datos de JSON de Amazon S3.	1. Utilice este código para leer el bucket de Amazon S3 y cargarlo como un diccionario de Python.
	
	`import json`
	`import boto3`
	
	`s3_client = boto3.client('s3')`
	`fileobj = s3_client.get_object(`
	`Bucket='<your-bucket-name>',`
	`Key='my.json'`
	`)`
	
	`filedata = fileobj['Body'].read()`
	`contents = filedata.decode('utf-8')`
	`json_content = json.loads(contents)`
	
	1. Compruebe que `json_content` contiene los registros esperados imprimiendo las primeras entradas.
		Desarrollador de aplicaciones, desarrollador de Python

Tarea	Descripción	Habilidades requeridas

Limpie los valores de los datos e inserte registros.	1. Utilice este código para limpiar los valores de los datos e insertar registros en la zona alojada. `<hosted-zone-id>` Sustitúyalo por el ID de la zona alojada configurada anteriormente.
	
	`import unicodedata`
	`import time`
	
	`for item in json_cont`
	`ent:`
	`    fqn_name = unicodeda`
	`ta.normalize(`
	`        "NFKD",`
	`        item["Fqd`
	`nName"].replace("u'",`
	` "'").replace('\xa0',`
	` '').strip()`
	`    )`
	`    rec_type = item["Rec`
	`ordType"].replace(`
	`'\xa0', '').strip()`
	`    res_rec = {'Value':`
	` item["Value"].repl`
	`ace('\xa0', '').strip`
	`()}`
	
	`    change_response`
	` = route53_client.cha`
	`nge_resource_recor`
	`d_sets(`
	`        HostedZon`
	`eId='<hosted-zone-`
	`id>',`
	`        ChangeBatch={`
		Desarrollador de aplicaciones, con conocimientos de Python

Tarea	Descripción	Habilidades requeridas

	<pre>'Comment': 'Created by automation',
	'Changes': [
	{
	'Action': 'UPSERT',
	'ResourceRecordSet': {
	'Name': fqn_name,
	'Type': rec_type,
	'TTL': item["TTL"],
	'ResourceRecords': [res_rec]
	}
	}
	]
	}
	)
	time.sleep(1) # Delay to avoid PriorRequestNotComplete errors</pre> 1. Monitorice la salida en busca de errores. Si se produce una limitación, aumente el retraso o implemente un retroceso exponencial.	

Resolución de problemas

Problema	Solución
Error `PriorRequestNotComplete`	Añada un `time.sleep()` retraso de 1 a 2 segundos entre llamadas. `change_resource_record_sets` Route 53 procesa los cambios de forma asíncrona y es posible que aún se esté realizando un cambio anterior.
Error `InvalidChangeBatch`	Este error se produce al intentar crear un registro que ya existe mediante la acción. `CREATE` Úselo `UPSERT` en su lugar para hacer que el script sea idempotente.
Error de regulación (se ha superado el límite de velocidad)	Has superado las cinco solicitudes de API por segundo. Implemente un retroceso exponenci al con fluctuación de fase. Para obtener más información, consulte Reintentos de error y retroceso exponencial en. AWS
Los registros no se resuelven	Compruebe que la VPC esté asociada a la zona alojada y que la resolución de DNS esté habilitada en la VPC. Ambos `enableDnsSupport` y `enableDnsHostnames` deben estar configurados en. `true`
`InvalidInput` error en los valores de registro	Los datos contienen espacios ininterrumpidos (`\xa0`) o espacios en leading/trailing blanco. Aplique el código de limpieza de datos de la tarea «Limpiar valores de datos e insertar registros» antes de insertarlos.

Recursos relacionados

Referencias

- Crear registros mediante la importación de un archivo de zona (documentación de Route 53)

- create_hosted_zone (documentación de Boto3)
- change_resource_record_sets (documentación de Boto3)
- Tipos de registros DNS compatibles (documentación de Route 53)
- Error al volver a intentarlo y se ha producido un retraso exponencial en AWS

Tutoriales y videos

Diseño de DNS con Amazon Route 53 (vídeo)

Información adicional

En el caso de los registros NAPTR y SRV, el `Value` campo de la hoja de cálculo de Excel debe contener todos los componentes necesarios concatenados en una sola cadena. Utilice la función CONCAT de Excel para combinar las propiedades individuales (orden, preferencia, indicadores, servicio, expresión regular, reemplazo para NAPTR; prioridad, peso, puerto, objetivo para SRV) antes de exportar a JSON.

Si la migración incluye más de 1000 registros, divida el archivo JSON en lotes y procese cada lote por separado para mantenerse dentro de los límites de la API de Route 53. Al usar la `UPSERT` acción, cada `ResourceRecord` elemento cuenta dos veces para el máximo de 1000 elementos por solicitud. `ChangeResourceRecordSets`

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Cómo modificar los encabezados HTTP al migrar de F5 a un equilibrador de carga de aplicación en AWS

Sachin Trivedi, Amazon Web Services

Resumen

Cuando migra una aplicación que utiliza un equilibrador de carga de F5 a Amazon Web Services (AWS) y quiere usar un equilibrador de carga de aplicación en AWS, la migración de las reglas de F5 para las modificaciones de encabezados es un problema habitual. Un Application Load Balancer no admite modificaciones de encabezados, pero puedes usar Amazon CloudFront como red de entrega de contenido (CDN) y Lambda @Edge para modificar encabezados.

Este patrón describe las integraciones necesarias y proporciona un código de muestra para la modificación del encabezado mediante AWS CloudFront y Lambda @Edge.

Requisitos previos y limitaciones

Requisitos previos

- Aplicación en las instalaciones que usa un equilibrador de carga de F5 con una configuración que reemplaza el valor del encabezado HTTP mediante el uso de `if, else`. Para obtener más información sobre esta configuración, consulte Encabezado HTTP en la documentación del producto de F5.

Limitaciones

- Este patrón se aplica a la personalización del encabezado del equilibrador de carga de F5. Para otros equilibradores de carga de terceros, por favor consulte la documentación del equilibrador de carga para obtener información de soporte.
- Las funciones de Lambda que utilice para Lambda@Edge deben estar en la región Este de EE. UU. (Norte de Virginia).

Arquitectura

El siguiente diagrama muestra la arquitectura de AWS, incluyendo el flujo de integración entre la CDN y otros componentes de AWS.

Tools (Herramientas)

Servicios de AWS

- Equilibrador de carga de aplicación – Un equilibrador de carga de aplicación es un servicio de equilibrio de carga totalmente gestionado por AWS que funciona en la séptima capa del modelo de interconexión de sistemas abiertos (OSI). Equilibra el tráfico entre varios destinos y admite solicitudes de enrutamiento avanzadas basadas en encabezados y métodos HTTP, cadenas de consulta y enrutamiento basado en el host o en la ruta.
- Amazon CloudFront: Amazon CloudFront es un servicio web que acelera la distribución de su contenido web estático y dinámico, como .html, .css, .js y archivos de imagen, a sus usuarios. CloudFront entrega su contenido a través de una red mundial de centros de datos denominados ubicaciones perimetrales para reducir la latencia y mejorar el rendimiento.
- Lambda @Edge – Lambda @Edge es una extensión de AWS Lambda que le permite ejecutar funciones para personalizar el contenido que se entrega. CloudFront Puede crear funciones en la región EE.UU. Este (Virginia del Norte) y, después, asociarlas a una CloudFront distribución para replicar automáticamente el código en todo el mundo, sin aprovisionar ni administrar servidores. Esto reduce la latencia y mejora la experiencia del usuario.

Código

El siguiente código de ejemplo proporciona un plan para modificar los encabezados de CloudFront respuesta. Siga las instrucciones de la sección Epics para implementar el código.

```
exports.handler = async (event, context) => {
    const response = event.Records[0].cf.response;
    const headers = response.headers;


    const headerNameSrc = 'content-security-policy';
    const headerNameValue = '*.xyz.com';


    if (headers[headerNameSrc.toLowerCase()]) {
        headers[headerNameSrc.toLowerCase()] = [{
            key: headerNameSrc,
            value: headerNameValue,
```

```
        }];
        console.log(`Response header "${headerNameSrc}" was set to ` +
                    `"${headers[headerNameSrc.toLowerCase()][0].value}"`);
    }
    else {
            headers[headerNameSrc.toLowerCase()] = [{
            key: headerNameSrc,
            value: headerNameValue,
            }];
    }
    return response;
};
```

Epics

Crear una distribución

Tarea	Descripción	Habilidades requeridas
Cree una distribución CloudFront web.	En este paso, crea una CloudFront distribución para indicar desde CloudFront dónde quiere que se entregue el contenido y los detalles sobre cómo realizar el seguimiento y gestionar la entrega del contenido. Para crear una distribución mediante la consola, inicie sesión en la consola de administración de AWS, abra la CloudFront consola y, a continuación, siga los pasos de la CloudFront documentación.	Administrador de la nube

Creación e implementación de la funcion Lambda@Edge

Tarea	Descripción	Habilidades requeridas
Crear e implementar la funcion Lambda@Edge.	Puede crear una función Lambda @Edge mediante un esquema para modificar CloudFront los encabezad os de respuesta. (Hay otros blueprints disponibles para diferentes casos de uso; para obtener más información, consulte las funciones de ejemplo de Lambda @Edge en CloudFront la documenta ción). Para crear una función de Lambda@Edge: 1. Inicie sesión en la consola de administración de AWS y abra la consola de AWS Lambda en. https:// console.aws.amazon.com/ lambda/ 2. Asegúrese de estar en la región EE.UU. Este (Norte de Virginia). CloudFront los planos solo están disponibl es en esta región. 3. Elija Crear función. 4. Seleccione Usar un esquema y, a continuac ión, introduzca cloudfront en el campo de búsqueda Esquemas.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	5. Elija el cloudfront-modify-response-headerplano y, a continuación, elija Configurar. 6. En la página Información básica, facilite la siguiente información: a. Escriba un nombre de función. b. Para Execution Role (Rol de ejecución), elija Create a new role from AWS policy templates (Crear un rol a partir de las plantillas de políticas de AWS). c. Asocie el nombre del rol de AWS Identity and Access Management (IAM) correspondiente. 7. Elija Crear función. 8. En la sección Diseñador de la página, elija el nombre de la función. 9. En la sección Código de función, sustituya el código de plantilla por el código de muestra proporcionado anteriormente en este patrón, en la sección Código.	

Tarea	Descripción	Habilidades requeridas
	10. En el código de muestra, reemplace `xyz.com` por el nombre de su dominio. 11. Seleccione Save.	
Implemente la función de Lambda@Edge.	Siga las instrucciones del paso 4 del tutorial: Creación de una función Lambda @Edge sencilla de la CloudFront documentación de Amazon para configurar el CloudFront disparador e implementar la función.	Administrador de AWS

Recursos relacionados

CloudFront documentación

- Comportamiento de solicitudes y respuestas para orígenes personalizados
- Trabajo con distribuciones
- Funciones de ejemplo de Lambda@Edge
- Personalización en la periferia con Lambda@Edge
- Tutorial: Creación de una función de Lambda@Edge sencilla

Cree un informe con los hallazgos de Network Access Analyzer sobre el acceso entrante a Internet en múltiples Cuentas de AWS

Mike Virgilio, Amazon Web Services

Resumen

El acceso entrante no intencionado a AWS los recursos a través de Internet puede suponer un riesgo para el perímetro de datos de una organización. El Analizador de acceso a la red es una característica de Amazon Virtual Private Cloud (Amazon VPC) que ayuda a identificar el acceso de red no deseado a sus recursos en Amazon Web Services (AWS). Puede utilizar el Analizador de acceso a la red para especificar sus requisitos de acceso a la red e identificar posibles rutas de red que no cumplan los requisitos especificados. Puede utilizar el Analizador de acceso a la red para hacer lo siguiente:

1. Identifique AWS los recursos a los que se puede acceder a Internet a través de pasarelas de Internet.
2. Compruebe que sus nubes privadas virtuales (VPCs) estén segmentadas adecuadamente, por ejemplo, aislando los entornos de producción y desarrollo y separando las cargas de trabajo transaccionales.

Network Access Analyzer analiza las condiciones de accesibilidad end-to-end de la red y no solo un componente individual. Para determinar si un recurso es accesible desde Internet, Network Access Analyzer evalúa la puerta de enlace de Internet, las tablas de enrutamiento de VPC, las listas de control de acceso a la red (ACLs), las direcciones IP públicas en las interfaces de red elásticas y los grupos de seguridad. Si alguno de estos componentes impide el acceso a Internet, en Analizador de acceso a la red no genera ningún resultado. Por ejemplo, si una instancia de Amazon Elastic Compute Cloud (Amazon EC2) tiene un grupo de seguridad abierto que permite el tráfico desde, `0/0` pero la instancia se encuentra en una subred privada que no se puede enrutar desde ninguna puerta de enlace de Internet, Network Access Analyzer no generará ningún hallazgo. Esto proporciona resultados de alta fidelidad para que pueda identificar los recursos a los que realmente se puede acceder desde Internet.

Cuando ejecuta el Analizador de acceso a la red, utiliza los Ámbitos de acceso a la red para especificar sus requisitos de acceso a la red. Esta solución identifica las rutas de red entre una puerta de enlace de Internet y una interfaz de red elástica. En este patrón, se implementa la solución

de forma centralizada Cuenta de AWS en la organización, gestionada por ellas AWS Organizations, y esta analiza todas las cuentas de la organización Región de AWS, si las hay.

Esta solución se diseñó teniendo en cuenta lo siguiente:

- Las AWS CloudFormation plantillas reducen el esfuerzo necesario para implementar los AWS recursos en este patrón.
- Puede ajustar los parámetros de las CloudFormation plantillas y del script naa-script.sh en el momento de la implementación para personalizarlos para su entorno.
- Los scripts de Bash aprovisionan y analizan automáticamente los alcances de acceso a la red para varias cuentas, en paralelo.
- Un script de Python procesa los resultados, extrae los datos y, a continuación, consolida los resultados. Puede optar por revisar el informe consolidado de los resultados del Analizador de acceso a la red en formato CSV o en AWS Security Hub CSPM. Un ejemplo del informe CSV está disponible en la sección de Información adicional de este patrón.
- Puede corregir los resultados o excluirlos de futuros análisis agregándolos al archivo naa-exclusions.csv.

Requisitos previos y limitaciones

Requisitos previos

- Y Cuenta de AWS para alojar servicios y herramientas de seguridad, gestionados como una cuenta de miembro de una organización en AWS Organizations. En este patrón, esta cuenta se denomina cuenta de seguridad.
- En la cuenta de seguridad, debe tener una subred privada con acceso saliente a Internet. Para obtener instrucciones, consulte Crear una subred en la documentación de Amazon VPC. Puede establecer el acceso a Internet mediante una puerta de enlace NAT o un punto de conexión de VPC de interfaz.
- Acceso a la cuenta AWS Organizations de administración o a una cuenta para la que se hayan delegado permisos de CloudFormation administrador. Para obtener instrucciones, consulte Registrar un administrador delegado en la CloudFormation documentación.
- Habilite el acceso confiable entre AWS Organizations y. CloudFormation Para obtener instrucciones, consulte Habilitar el acceso confiable con AWS Organizations en la CloudFormation documentación.

- Si vas a subir los resultados a Security Hub CSPM, Security Hub CSPM debe estar habilitado en la cuenta y en el lugar donde Región de AWS se aprovisiona la instancia de Amazon. EC2 Para obtener más información, consulte Configuración AWS Security Hub CSPM.

Limitaciones

- Las rutas de red entre cuentas no se analizan actualmente debido a las limitaciones de las característica del Analizador de acceso a la red.
- El objetivo Cuentas de AWS debe gestionarse como una organización en. AWS OrganizationsSi no la utiliza AWS Organizations, puede actualizar la CloudFormation plantilla naa-execrole.yaml y el script naa-script.sh para su entorno. En su lugar, proporciona una lista de las regiones en las que desea Cuenta de AWS IDs ejecutar el script.
- La CloudFormation plantilla está diseñada para implementar la EC2 instancia de Amazon en una subred privada con acceso saliente a Internet. El AWS Systems Manager agente (agente SSM) requiere acceso saliente para llegar al punto final del servicio Systems Manager, y usted necesita acceso saliente para clonar el repositorio de código e instalar las dependencias. Si quieres usar una subred pública, debes modificar la plantilla naa-resources.yaml para asociar una dirección IP elástica a la instancia de Amazon. EC2

Arquitectura

Arquitectura de destino

Opción 1: Acceder a los resultados de un bucket de Amazon S3

El diagrama muestra el proceso siguiente:

1. Si ejecutas la solución manualmente, el usuario se autentica en la EC2 instancia de Amazon mediante el Administrador de sesiones y, a continuación, ejecuta el script naa-script.sh. Este script del intérprete de comandos lleva a cabo los pasos del 2 al 7.

   Si ejecuta la solución automáticamente, el script naa-script.sh se iniciará automáticamente según la programación que haya definido en la expresión cron. Este script del intérprete de comandos lleva a cabo los pasos del 2 al 7. Para obtener más información, consulte Automatizar y escalar al final de esta sección.

2. La EC2 instancia de Amazon descarga el archivo naa-exception.csv más reciente del bucket de Amazon S3. Este archivo se utiliza más adelante en el proceso, cuando el Script de Python procesa las exclusiones.
3. La EC2 instancia de Amazon asume la función `NAAEC2Role` AWS Identity and Access Management (IAM), que otorga permisos para acceder al bucket de Amazon S3 y para asumir las funciones de `NAAExecRole` IAM en las demás cuentas de la organización.
4. La EC2 instancia de Amazon asume la función de `NAAExecRole` IAM en la cuenta de administración de la organización y genera una lista de las cuentas de la organización.
5. La EC2 instancia de Amazon asume la función de `NAAExecRole` IAM en las cuentas de los miembros de la organización (denominadas cuentas de carga de trabajo en el diagrama de arquitectura) y realiza una evaluación de seguridad en cada cuenta. Los resultados se almacenan como archivos JSON en la EC2 instancia de Amazon.
6. La EC2 instancia de Amazon usa un script de Python para procesar los archivos JSON, extraer los campos de datos y crear un informe CSV.
7. La EC2 instancia de Amazon carga el archivo CSV en el bucket de Amazon S3.
8. Una EventBridge regla de Amazon detecta la carga del archivo y utiliza un tema de Amazon SNS para enviar un correo electrónico en el que se notifica al usuario que el informe está completo.
9. El usuario descarga el archivo CSV del bucket de Amazon S3. El usuario importa los resultados a la plantilla de Excel y revisa los resultados.

Opción 2: acceda a los resultados en AWS Security Hub CSPM

El diagrama muestra el proceso siguiente:

1. Si ejecutas la solución manualmente, el usuario se autentica en la EC2 instancia de Amazon mediante el Administrador de sesiones y, a continuación, ejecuta el script naa-script.sh. Este script del intérprete de comandos lleva a cabo los pasos del 2 al 7.

   Si ejecuta la solución automáticamente, el script naa-script.sh se iniciará automáticamente según la programación que haya definido en la expresión cron. Este script del intérprete de comandos lleva a cabo los pasos del 2 al 7. Para obtener más información, consulte Automatizar y escalar al final de esta sección.
2. La EC2 instancia de Amazon descarga el archivo naa-exception.csv más reciente del bucket de Amazon S3. Este archivo se utiliza más adelante en el proceso, cuando el Script de Python procesa las exclusiones.

3. La EC2 instancia de Amazon asume la función de `NAAEC2Role` IAM, que otorga permisos para acceder al bucket de Amazon S3 y para asumir las funciones de `NAAExecRole` IAM en las demás cuentas de la organización.
4. La EC2 instancia de Amazon asume la función de `NAAExecRole` IAM en la cuenta de administración de la organización y genera una lista de las cuentas de la organización.
5. La EC2 instancia de Amazon asume la función de `NAAExecRole` IAM en las cuentas de los miembros de la organización (denominadas cuentas de carga de trabajo en el diagrama de arquitectura) y realiza una evaluación de seguridad en cada cuenta. Los resultados se almacenan como archivos JSON en la EC2 instancia de Amazon.
6. La EC2 instancia de Amazon usa un script de Python para procesar los archivos JSON y extraer los campos de datos para importarlos a Security Hub CSPM.
7. La EC2 instancia de Amazon importa los resultados del Network Access Analyzer a Security Hub CSPM.
8. Una EventBridge regla de Amazon detecta la importación y utiliza un tema de Amazon SNS para enviar un correo electrónico en el que se notifica al usuario que el proceso se ha completado.
9. El usuario consulta los resultados en Security Hub CSPM.

Automatizar y escalar

Puede programar esta solución para que ejecute el script naa-script.sh automáticamente según una programación personalizada. Para establecer una programación personalizada, modifique el parámetro en la plantilla naa-resources.yaml. CloudFormation `CronScheduleExpression` Por ejemplo, el valor predeterminado de `0 0 * * 0` ejecuta la solución todos los domingos a medianoche. Un valor de `0 0 * 1-12 0` ejecutaría la solución a medianoche del primer domingo de cada mes. Para obtener más información sobre el uso de expresiones cron, consulte Expresiones cron y de frecuencia en la documentación de Systems Manager.

Si desea ajustar la programación una vez implementada la pila `NAA-Resources`, puede editarla manualmente en `/etc/cron.d/naa-schedule`.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática escalable en el Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.

- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, AWS Lambda funciones, puntos finales de invocación HTTP que utilizan destinos de API o buses de eventos en otros. Cuentas de AWS
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar múltiples cuentas Cuentas de AWS en una organización que usted crea y administra de forma centralizada.
- AWS Security Hub CSPMproporciona una visión completa del estado de su seguridad en AWS. También le ayuda a comparar su AWS entorno con los estándares y las mejores prácticas del sector de la seguridad.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Systems Manager lo ayuda a administrar las aplicaciones y la infraestructura que se ejecutan en la Nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo necesario para detectar y resolver problemas operativos y le ayuda a administrar sus AWS recursos de forma segura y a escala. Este patrón utiliza el Administrador de sesiones, una capacidad de Administrador de sistemas.

Repositorio de código

El código de este patrón está disponible en el repositorio de análisis de cuentas múltiples GitHub de Network Access Analyzer. El repositorio de código contiene los siguientes archivos:

- naa-script.sh: este script bash se utiliza para iniciar un análisis del Network Access Analyzer de varios Cuentas de AWS, en paralelo. Como se define en la CloudFormation plantilla naa-resources.yaml, este script se implementa automáticamente en la carpeta `/usr/local/naa` de la instancia de Amazon. EC2
- naa-resources.yaml: utilizas esta CloudFormation plantilla para crear una pila en la cuenta de seguridad de la organización. Esta plantilla implementa todos los recursos necesarios para esta cuenta a fin de respaldar la solución. Esta pila debe implementarse antes que la plantilla naa-execrole.yaml.

> **Note**
>
> Si esta pila se elimina y se vuelve a implementar, debe volver a crear el conjunto de pilas `NAAExecRole` para recuperar las dependencias entre cuentas entre los roles de IAM.

- naa-execrole.yaml: usa esta CloudFormation plantilla para crear un conjunto de pilas que despliegue la función de IAM en todas las cuentas de la organización, incluida la cuenta de administración. `NAAExecRole`
- naa-processfindings.py: la secuencia de comandos naa-script.sh llama automáticamente a esta secuencia de comandos de Python para procesar las salidas JSON de Network Access Analyzer, excluir cualquier recurso de funcionalidad comprobada en el archivo naa-exclusions.csv y, a continuación, generar un archivo CSV con los resultados consolidados o importarlos a Security Hub CSPM.

Epics

Preparación para la implementación

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código.	1. En una interfaz de la línea de comandos, cambie el directorio de trabajo a la ubicación en la que desee almacenar los archivos de muestra. 2. Introduzca el siguiente comando: `git clone https://github.com/aws-samples/network-access-analyzer-multi-account-analysis.git`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Revise las plantillas.	1. En el repositorio clonado, abra los archivos naa-resources.yaml y naa-execrole.yaml. 2. Revise los recursos creados por estas plantillas y ajuste las plantillas según sea necesario para su entorno. Para obtener más información, consulte Trabajar con plantillas en la CloudFormation documentación. 3. Guarde y cierre los archivos naa-resources.yaml y naa-execrole.yaml.	AWS DevOps

Crea las CloudFormation pilas

Tarea	Descripción	Habilidades requeridas
Aprovisione recursos en la cuenta de seguridad.	Con la plantilla naa-resources.yaml, se crea una CloudFormation pila que despliega todos los recursos necesarios en la cuenta de seguridad. Para obtener instrucciones, consulta Cómo crear una pila en la documentación. CloudFormation Tenga en cuenta lo siguiente al implementar esta plantilla:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	1. En la página Especific ar plantilla, seleccione la Plantilla está lista y, a continuación, cargue el archivo naa-resources.yaml . 2. En la página Especificar detalles de pila, en Nombre de la pila, introduzca `NAA-Resources` . 3. En la sección Parámetros, introduzca lo siguiente: • `VPCId`: seleccione una VPC en la cuenta. • `SubnetId`: seleccione una subred privada que tenga acceso a Internet. **Note** Si seleccion as una subred pública, es posible que a la EC2 instancia de Amazon no se le asigne una dirección IP pública porque la CloudFormation plantilla, de forma predeterminada, no aprovisio na ni adjunta	

Tarea	Descripción	Habilidades requeridas
	una dirección IP elástica. • `InstanceType` —— Deje el tipo de instancia predeterminado. • `InstanceImageId` : deje el valor predeterm inado. • `KeyPairName` : si utiliza SSH para acceder, especifique el nombre de un par de claves existente. • `PermittedSSHInboun d` : si utiliza SSH para el acceso, especifiq ue un bloque CIDR permitido. Si no utiliza SSH, mantenga el valor predeterminado de `127.0.0.1` . • `BucketName` : El valor predeterminado es `naa-<accountID>- <region>` . Puede modificarlo según sea necesario. Si especifica un valor personalizado, el ID de cuenta y la región se añaden automátic amente al valor especific ado.	

Tarea	Descripción	Habilidades requeridas
	• `EmailAddress` —— Especifique una dirección de correo electrónico para una notificación de Amazon SNS cuando se complete el análisis. **Note** La configuración de la suscripción a Amazon SNS debe confirmar se antes de completar el análisis o no se enviará ninguna notificación. • `NAAEC2Role` : mantenga el nombre predeterminado a menos que sus convenciones de nomenclatura requieran un nombre diferente para este rol de IAM. • `NAAExecRole` —— Mantenga el nombre predeterminado a menos que se utilice otro nombre al implementar naa-execr ole.yaml • `Parallelism` : especifique el número de	

Tarea	Descripción	Habilidades requeridas
	evaluaciones paralelas que se van a realizar. • `Regions`— Especifique Regiones de AWS lo que desea analizar. • `ScopeNameValue` —– Especifique la etiqueta que se asignará al ámbito. Esta etiqueta se utiliza para determinar el alcance de acceso a la red. • `ExclusionFile` —– Especifique el nombre del archivo de exclusión . Las entradas de este archivo se excluirán de los resultados. • `FindingsToCSV` – Especifique si los resultados deben enviarse a CSV. Los valores aceptados son: `true` y `false`. • `FindingsToSecurityHub` — Especifique si los resultados deben importarse a Security Hub CSPM. Los valores aceptados son: `true` y `false`. • `EmailNotificationsForSecurityHub` —	

Tarea	Descripción	Habilidades requeridas
	Especifique si la importación de los resultados a Security Hub CSPM debe generar notificaciones por correo electrónico. Los valores aceptados son: `true` y `false`. • `ScheduledAnalysis` –– Si desea que la solución se ejecute automáticamente según una programación, introduzca `true` y, a continuación, personali ce la programación en el parámetro `CronSched uleExpression` . Si no desea ejecutar la solución automátic amente, introduzca `false`. • `CronScheduleExpres sion` –– Si ejecuta la solución automátic amente, introduzca una expresión cron para definir la programac ión. Para obtener más información, consulte Automatizar y escalar en la sección Arquitectura de este patrón.	

Tarea	Descripción	Habilidades requeridas
	1. En la página de revisión, seleccione Los siguiente s recursos requieren capacidades: [AWS::IAM ::Role] y, a continuación, elija Crear pila. 2. Una vez que la pila se haya creado correctamente, en la CloudFormation consola, en la pestaña Outputs, copia el `NAAEC2Role` Amazon Resource Name (ARN). Este ARN se utiliza más adelante al implementar el archivo naa-execrole.yaml.	

Tarea	Descripción	Habilidades requeridas
Facilitar el rol de IAM en las cuentas de los miembros.	En la cuenta AWS Organizations de administración o en una cuenta con permisos de administrador delegados CloudFormation, utilice la plantilla naa-execrole.yaml para crear un conjunto de pilas. CloudFormation El conjunto de pilas implementa el rol de IAM de `NAAExecRole` para todas las cuentas de miembros de la organización. Para obtener instrucciones, consulta Cómo crear un conjunto de pilas con permisos administrados por el servicio en la documentación. CloudFormation Tenga en cuenta lo siguiente al implementar esta plantilla: 1. En Preparación de la plantilla, seleccione La plantilla está lista y, a continuación, cargue el archivo naa-execrole.yaml. 2. En la página Especificar StackSet detalles, asigne un nombre al conjunto de pilas. `NAA-ExecRole` 3. En la sección Parámetros, introduzca lo siguiente: • `AuthorizedARN` : introduzca el ARN de	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`NAAEC2Role` que copió al crear la pila de `NAA-Resources` . • `NAARoleName` —— Mantenga el valor predeterminado de `NAAExecRole` a menos que se haya utilizado otro nombre al implementar el archivo naa-resources.yaml. 4. En Permisos, seleccione Permisos administrados por servicios. 5. En la página Cómo establecer opciones de implementación, en Destinos de implementación, seleccione Implementación en organización y acepte todos los valores predeterminados. **Note** Si quiere que las pilas se implementen en en todas las cuentas de miembros de forma simultánea, establezca el número máximo de cuentas simultáne	

Tarea	Descripción	Habilidades requeridas
	as y la tolerancia a errores en un valor alto, por ejemplo `100`. 6. En Regiones de implement ación, elige la región en la que se despliega la EC2 instancia de Amazon para Network Access Analyzer. Como los recursos de IAM son globales y no regionale s, se implementa el rol de IAM en todas las regiones activas. 7. En la página de revisión, seleccione Acepto que AWS CloudFormation podría crear recursos de IAM con nombres personali zados y, a continuación, elija Crear. StackSet 8. Supervise la pestaña Instancias de pila (para ver el estado de las cuentas individuales) y la pestaña Operaciones (para ver el estado general) para determinar cuándo se ha completado la implement ación.	

Tarea	Descripción	Habilidades requeridas
Facilite el rol de IAM en la cuenta de administración.	Con la plantilla naa-execrole.yaml, se crea una CloudFormation pila que implementa la función de `NAAExecRole` IAM en la cuenta de administración de la organización. El conjunto de pilas que creó anteriormente no implementa el rol de IAM en la cuenta de administración. Para obtener instrucciones, consulta Cómo crear una pila en la documentación. CloudFormation Tenga en cuenta lo siguiente al implementar esta plantilla: 1. En la página Especificar plantilla, seleccione La plantilla está lista y, a continuación, cargue el archivo naa-execrole.yaml. 2. En la página Especificar detalles de pila, en Nombre de la pila, introduzca `NAA-ExecRole` . 3. En la sección Parámetros, introduzca lo siguiente: • `AuthorizedARN` : introduzca el ARN de `NAAEC2Role` que copió al crear la pila de `NAA-Resources` .	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• `NAARoleName` —— Mantenga el valor predeterminado de `NAAExecRole` a menos que se haya utilizado otro nombre al implement ar el archivo naa-resou rces.yaml. 4. En la página de revisión, seleccione Los siguiente s recursos requieren capacidades: [AWS::IAM ::Role] y, a continuación, elija Crear pila.	

Realice el análisis

Tarea	Descripción	Habilidades requeridas
Personalice el script del intérprete de comandos.	1. Inicie sesión en la cuenta de seguridad de la organización. 2. Con Session Manager, conéctese a la EC2 instancia de Amazon para Network Access Analyzer que aprovisionó anteriorm ente. Para obtener instrucci ones, consulte Conexión a la instancia de Linux mediante Session Manager. Si no puede conectars e, consulte la sección de	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	solución de problemas de este patrón.
	3. Introduzca los siguiente s comandos para abrir el archivo naa-script.sh para editarlo:
	`sudo -i`
	`cd /usr/local/naa`
	`vi naa-script.sh`
	4. Revise y modifique los parámetros y variables ajustables de este script según sea necesario para su entorno. Para obtener más informaci ón sobre las opciones de personalización, consulte los comentarios al principio del script.
	Por ejemplo, en lugar de obtener una lista de todas las cuentas de los miembros de la organización a partir de la cuenta de administr ación, puede modificar el Cuenta de AWS IDs script para especificar qué cuentas desea escanear o puede hacer referencia a un archivo externo que contenga estos parámetros. Regiones de AWS	

Tarea	Descripción	Habilidades requeridas
	5. Guarde y cierre el archivo naa-script.sh.	

Tarea	Descripción	Habilidades requeridas

Analice las cuentas de destino.	1. Introduzca los comandos siguientes. De esta forma, se ejecuta el script naa-script.sh:
	
	`sudo -i`
	`cd /usr/local/naa`
	`screen`
	`./naa-script.sh`
	
	Tenga en cuenta lo siguiente:
	• El comando `screen` permite que el script continúe ejecutándose en caso de que se agote el tiempo de espera de la conexión o se pierda el acceso a la consola.
	• Cuando comience el escaneo, puede forzar la separación de la pantalla pulsando Ctrl+A D. La pantalla se separa y puede cerrar la conexión de la instancia mientras se realiza el análisis.
	• Para reanudar una sesión separada, conéctese a la instancia, introduzca `sudo -i` y, a continuación, introduzca `screen -r`.
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	2. Supervise el resultado en busca de errores para asegurarse de que el script funciona correctamente. Para ver un ejemplo de producción, consulte la sección de Información adicional de este patrón. 3. Espere a que el análisis finalice. Si configuró las notificaciones por correo electrónico, recibirá un correo electrónico cuando los resultados se carguen en el bucket de Amazon S3 o se importen a Security Hub CSPM.	
Opción 1: Recupere los resultados del bucket de Amazon S3.	1. Descargue el archivo CSV del bucket `naa-<accountID>-<region>` . Para obtener instrucciones, consulte Descargar un objeto en la documentación de Amazon S3. 2. Elimine el archivo CSV del bucket de Amazon S3. Esta es una práctica recomendada para la optimización de costos. Para obtener instrucciones, consulte Eliminar objetos en la documentación de Amazon S3.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Opción 2: Revise los resultados en Security Hub CSPM.	1. Abra la consola CSPM de Security Hub. 2. En el panel de navegación, seleccione Findings (Resultados). 3. Revise los resuñtados del Analizador de acceso a la red. Para obtener instrucciones, consulte Visualización de listas de búsqueda y detalles en la documentación de CSPM de Security Hub. **Note** Para buscar resultados, añada un título que empiece por filtrar e introducir `Network Access Analyzer`.	AWS DevOps

Corregir y excluir los resultados

Tarea	Descripción	Habilidades requeridas
Corrija los resultados.	Corrija cualquier resultado que desee abordar. Para obtener más información y las mejores prácticas sobre cómo crear un perímetro alrededor de sus	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	AWS identidades, recursos y redes, consulte Cómo crear un perímetro de datos en AWS (AWS documento técnico).	

Tarea	Descripción	Habilidades requeridas
Excluya los recursos con rutas de red de funcionalidad comprobada.	Si el Analizador de acceso a la red genera resultados sobre los recursos a los que se debería acceder desde Internet, puede agregar estos recursos a una lista de exclusión. La próxima vez que se ejecute el Analizador de acceso a la red, no generará ningún resultado para ese recurso. 1. Navegue hasta `/usr/local/naa` y, a continuación, abra el script naa-script.sh. Anote el valor de la variable `S3_EXCLUSION_FILE` . 2. Si el valor de la variable `S3_EXCLUSION_FILE` es `true`, descargue el archivo naa-exclusions.csv del bucket `naa-<accountID>-<region>` . Para obtener instrucciones, consulte Descargar un objeto en la documentación de Amazon S3. Si el valor de la variable `S3_EXCLUSION_FILE` es `false`, navegue hasta `/usr/local/naa` y, a continuación, abra el archivo naa-exclusions.csv.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Note Si el valor de la variable `S3_EXCLUSION_FILE` es `false`, el script utiliza una versión local del archivo de exclusiones. Si más adelante cambia el valor a `true`, el script sobrescribirá la versión local con el archivo del bucket de Amazon S3. 3. En el archivo naa-exclusions.csv, introduzca los recursos que desee excluir. Introduzca un recurso en cada línea y utilice el siguiente formato. `<resource_id>,<secgroup_id>,<sgrule_cidr>,<sgrule_portrange>,<sgrule_protocol>` El siguiente es un recurso de ejemplo.	

Tarea	Descripción	Habilidades requeridas
	`eni-1111aaaaa2222bbbb,sg-3333ccccc4444dddd,0.0.0.0/0,80 to 80,tcp` 4. Guarde y cierre el archivo naa-exclusions.csv. 5. Si descargó el archivo naa-exclusions.csv del bucket de Amazon S3, cargue la nueva versión. Para más instrucciones, consulte Cargar objetos en la documentación de Amazon S3.	

(Opcional) Actualizar el script naa-script.sh

Tarea	Descripción	Habilidades requeridas
Actualice el script naa-script.sh.	Si quiere actualizar el script naa-script.sh a la última versión del repositorio, haga lo siguiente: 1. Conéctese a la EC2 instancia de Amazon mediante el Administrador de sesiones. Para obtener instrucciones, consulte Conexión a la instancia de Linux mediante Session Manager.	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	2. Introduzca el siguiente comando:
	`sudo -i`
	3. Navegue hasta el directorio de scripts naa-script.sh:
	`cd /usr/local/naa`
	4. Introduzca el siguiente comando para guardar el script local de forma que pueda combinar los cambios personalizados en la versión más reciente:
	`git stash`
	5. Introduzca el siguiente comando para obtener la versión más reciente del script:
	`git pull`
	6. Introduzca el siguiente comando para combinar el script personalizado con la versión más reciente del script:
	`git stash pop`	

(Opcional) Limpieza

Tarea	Descripción	Habilidades requeridas
Elimine todos los recursos implementados.	Puede dejar los recursos implementados en las cuentas. Si desea desaprovisionar todos los recursos, haga lo siguiente: 1. Elimine la pila `NAA-ExecRole` aprovisionada en la cuenta de administración. Para obtener instrucciones, consulte Eliminar una pila en la CloudFormation documentación. 2. Elimine el conjunto de pilas `NAA-ExecRole` aprovisionado en la cuenta de administración de la organización o en la cuenta de administrador delegado. Para obtener instrucciones, consulte Eliminar un conjunto de pilas en la CloudFormation documentación. 3. Elimine todos los objetos del bucket `naa-<accountID>-<region>` de Amazon S3. Para obtener instrucciones, consulte Eliminar objetos en la	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	documentación de Amazon S3. 4. Elimine la pila `NAA-Resources` aprovisionada en la cuenta de seguridad . Para obtener instrucciones, consulte Eliminar una pila en la CloudFormation documentación.	

Resolución de problemas

Problema	Solución
No se puede conectar a la EC2 instancia de Amazon mediante el administrador de sesiones.	El agente SSM debe poder comunicarse con el punto de conexión de Systems Manager. Haga lo siguiente: 1. Valide que la subred en la que se implement a la EC2 instancia de Amazon tenga acceso a Internet. 2. Reinicia la EC2 instancia de Amazon.
Al implementar el conjunto de pilas, la CloudFormation consola le solicitará que lo haga`Enable trusted access with AWS Organizations to use service-managed permissions` .	Esto indica que no se ha habilitado el acceso de confianza entre AWS Organizations y CloudFormation. Se requiere acceso de confianza para implementar el conjunto de pilas gestionado por servicios. Seleccione el botón para activar el acceso de confianza. Para obtener más información, consulte Habilitar el acceso confiable en la CloudFormation documentación.

Recursos relacionados

- Nuevo: Amazon VPC Network Access Analyzer (entrada de blog)AWS
- AWS Re:inForce 2022: valide los controles efectivos de acceso a la red el (02 AWS) (vídeo) NIS2
- Demostración - Análisis de la ruta de datos de ingreso a Internet en toda la organización mediante un Analizador de acceso a la red (video)

Información adicional

Ejemplo de salida de consola

En el siguiente ejemplo se muestra el resultado de generar la lista de cuentas de destino y analizar las cuentas de destino.

```
[root@ip-10-10-43-82 naa]# ./naa-script.sh
download: s3://naa-<account ID>-us-east-1/naa-exclusions.csv to ./naa-exclusions.csv

AWS Management Account: <Management account ID>

AWS Accounts being processed...
<Account ID 1> <Account ID 2> <Account ID 3>

Assessing AWS Account: <Account ID 1>, using Role: NAAExecRole
Assessing AWS Account: <Account ID 2>, using Role: NAAExecRole
Assessing AWS Account: <Account ID 3>, using Role: NAAExecRole
Processing account: <Account ID 1> / Region: us-east-1
Account: <Account ID 1> / Region: us-east-1 - Detecting Network Analyzer scope...
Processing account: <Account ID 2> / Region: us-east-1
Account: <Account ID 2> / Region: us-east-1 - Detecting Network Analyzer scope...
Processing account: <Account ID 3> / Region: us-east-1
Account: <Account ID 3> / Region: us-east-1 - Detecting Network Analyzer scope...
Account: <Account ID 1> / Region: us-east-1 - Network Access Analyzer scope detected.
Account: <Account ID 1> / Region: us-east-1 - Continuing analyses with Scope ID.
 Accounts with many resources may take up to one hour
Account: <Account ID 2> / Region: us-east-1 - Network Access Analyzer scope detected.
Account: <Account ID 2> / Region: us-east-1 - Continuing analyses with Scope ID.
 Accounts with many resources may take up to one hour
Account: <Account ID 3> / Region: us-east-1 - Network Access Analyzer scope detected.
Account: <Account ID 3> / Region: us-east-1 - Continuing analyses with Scope ID.
 Accounts with many resources may take up to one hour
```

Ejemplos de informes CSV

Las siguientes imágenes son ejemplos de la producción de CSV.

Configurar la resolución de DNS para redes híbridas en un entorno de cuentas múltiples AWS

Anvesh Koganti, Amazon Web Services

Resumen

Este patrón proporciona una solución integral para configurar la resolución de DNS en entornos de redes híbridas que incluyen varias cuentas de Amazon Web Services (AWS). Permite la resolución de DNS bidireccional entre las redes locales y el entorno a través de puntos finales. AWS Amazon Route 53 Resolver El patrón presenta dos soluciones para permitir la resolución de DNS en una arquitectura centralizada de varias cuentas:

- La configuración básica no utiliza los perfiles de Route 53. Ayuda a optimizar los costos de las implementaciones pequeñas y medianas de menor complejidad.
- La configuración mejorada utiliza los perfiles de Route 53 para simplificar las operaciones. Es la mejor opción para implementaciones de DNS más grandes o complejas.

> **Note**
>
> Consulte la sección Limitaciones para conocer las limitaciones y cuotas del servicio antes de la implementación. Al tomar la decisión, tenga en cuenta factores como los gastos generales de administración, los costos, la complejidad operativa y la experiencia del equipo.

Requisitos previos y limitaciones

Requisitos previos

- Un entorno de AWS varias cuentas con Amazon Virtual Private Cloud (Amazon VPC) implementado en cuentas de carga de trabajo y de servicios compartidos (preferiblemente configuradas a través de la Torre de Control de AWS AWS siguiendo las prácticas recomendadas para la estructura de cuentas).
- Conectividad híbrida existente (AWS Direct Connect o AWS Site-to-Site VPN) entre su red local y el entorno. AWS
- Emparejamiento de Amazon VPC o Nube de AWS WAN para conectividad de red de capa 3 entre. AWS Transit Gateway VPCs (Esta conectividad es necesaria para el tráfico de aplicaciones.

No es necesaria para que funcione la resolución de DNS. La resolución de DNS funciona independientemente de la conectividad de red entre los VPCs.)

- Servidores DNS que se ejecutan en el entorno en las instalaciones.

Limitaciones

- Los puntos finales, las reglas y los perfiles de Route 53 Resolver son construcciones regionales y, en el caso de las organizaciones globales, es posible que deban replicarse en varios Regiones de AWS .
- Para obtener una lista completa de las cuotas de servicio de Route 53 Resolver, las zonas alojadas privadas y los perfiles, consulte la sección Quotas en la documentación de Route 53.

Arquitectura

Pila de tecnología de destino

- Puntos de conexión entrantes y salientes de Route 53
- Reglas de Route 53 Resolver para el reenvío condicional
- AWS Resource Access Manager (AWS RAM)
- Zona alojada privada de Route 53

Arquitectura de destino

Puntos de conexión entrantes y salientes

En el siguiente diagrama, se muestra el flujo de resolución de DNS desde el entorno local AWS hasta el entorno local. Esta es la configuración de conectividad para las resoluciones salientes en las que el dominio se aloja en las instalaciones. A continuación se presenta información general del proceso que implica la configuración de esto. Para más información, consulte la sección Epics.

1. Implemente puntos de conexión de Route 53 Resolver salientes en la VPC de servicios compartidos.
2. Cree reglas de Route 53 Resolver (reglas de reenvío) en la cuenta de servicios compartidos para los dominios alojados en las instalaciones.

3. Comparta las reglas y VPCs asócielas con otras cuentas que alojen los recursos necesarios para resolver los dominios alojados de forma local. Esto se puede hacer de maneras distintas según el caso de uso, como se describe más adelante en esta sección.

Una vez configurada la conectividad, los pasos necesarios para la resolución saliente son los siguientes:

1. La instancia de Amazon Elastic Compute Cloud (Amazon EC2) envía una solicitud de resolución de DNS `db.onprem.example.com` al solucionador de Route 53 de la VPC a la dirección de la VPC+2.
2. Route 53 Resolver comprueba las reglas del Resolver y reenvía la solicitud al servidor DNS local IPs mediante el punto final de salida.
3. El punto final saliente reenvía la solicitud al DNS local. IPs El tráfico pasa por la conectividad de red híbrida establecida entre la VPC de servicios compartidos y el centro de datos en las instalaciones.
4. El servidor DNS en las instalaciones responde al punto de conexión saliente, que luego reenvía la respuesta al solucionador de Route 53 Resolver de la VPC. El Resolver devuelve la respuesta a la instancia. EC2

El siguiente diagrama muestra el flujo de resolución de DNS desde el entorno local hasta AWS. Esta es la configuración de conectividad para las resoluciones entrantes en las que el dominio se aloja en AWS. A continuación se presenta información general del proceso que implica la configuración de esto. Para más información, consulte la sección Epics.

1. Implemente puntos de conexión entrantes de Resolver en la VPC de servicios compartidos.
2. Cree zonas alojadas privadas en la cuenta de servicios compartidos (enfoque centralizado).
3. Asocie las zonas alojadas privadas a la VPC de servicios compartidos. Comparta y asocie estas zonas con varias cuentas VPCs para la resolución de VPC-to-VPC DNS. Esto se puede hacer de maneras distintas según el caso de uso, como se describe más adelante en esta sección.

Una vez configurada la conectividad, los pasos necesarios para la resolución entrante son los siguientes:

1. El recurso en las instalaciones envía una solicitud de resolución de DNS para `ec2.prod.aws.example.com` al servidor DNS en las instalaciones.
2. El servidor DNS en las instalaciones reenvía la solicitud al punto de conexión de Resolver entrante de la VPC de servicios compartidos a través de la conexión de red híbrida.
3. El punto de conexión de Resolver entrante busca la solicitud en la zona alojada privada asociada con la ayuda Route 53 Resolver de VPC y obtiene la dirección IP adecuada.
4. Estas direcciones IP se devuelven al servidor DNS en las instalaciones, que devuelve la respuesta al recurso en las instalaciones.

Esta configuración permite que los recursos locales resuelvan los nombres de dominio AWS privados al enrutar las consultas a través de los puntos finales entrantes hasta la zona alojada privada adecuada. En esta arquitectura, las zonas alojadas privadas están centralizadas en una VPC de servicios compartidos, lo que permite la administración central del DNS por parte de un solo equipo. Estas zonas se pueden asociar VPCs a muchas para abordar el caso de uso de la resolución de VPC-to-VPC DNS. Como alternativa, puede delegar la propiedad y la administración del dominio DNS en cada una de ellas Cuenta de AWS. En ese caso, cada cuenta administra sus propias zonas alojadas privadas y asocia cada zona a la VPC central de servicios compartidos para lograr una resolución unificada con el entorno en las instalaciones. Este enfoque descentralizado queda fuera del alcance de este patrón. Para obtener más información, consulte Escalar la administración de DNS en varias cuentas y VPCs en el documento técnico Opciones de DNS en la nube híbrida para Amazon VPC.

Al establecer los flujos de resolución de DNS fundamentales mediante puntos de conexión de Resolver, debe determinar cómo administrar el uso compartido y la asociación de las reglas de Resolver y las zonas alojadas privadas en sus Cuentas de AWS. Puede abordarlo de dos maneras: mediante el uso compartido autogestionado, AWS RAM para compartir las reglas de Resolver y las asociaciones directas de zonas alojadas privadas, como se detalla en la sección Configuración básica, o mediante los perfiles de Route 53, como se explica en la sección Configuración mejorada. La elección depende de las preferencias de administración del DNS y de los requisitos operativos de su organización. Los siguientes diagramas de arquitectura ilustran un entorno escalado que incluye varias cuentas VPCs diferentes, lo que representa una implementación empresarial típica.

Configuración básica

En la configuración básica, la implementación de la resolución de DNS híbrida en un AWS entorno con varias cuentas se utiliza AWS RAM para compartir las reglas de reenvío de Resolver y las asociaciones de zonas alojadas privadas para gestionar las consultas de DNS entre las instalaciones

y los recursos. AWS Este método utiliza puntos de conexión de Route 53 Resolver centralizados en una VPC de servicios compartidos que está conectada a la red en las instalaciones para gestionar la resolución de DNS entrante y saliente de manera eficiente.

- Para la resolución de llamadas salientes, las reglas de reenvío de Resolver se crean en la cuenta de Shared Services y, a continuación, se comparten con otras personas mediante. Cuentas de AWS AWS RAM Este uso compartido está limitado a cuentas en la misma región. A continuación, las cuentas de destino pueden asociar estas reglas a las suyas VPCs y habilitar los recursos que contienen VPCs para resolver los nombres de dominio locales.
- Para la resolución entrante, las zonas alojadas privadas se crean en la cuenta de servicios compartidos y se asocian a la VPC de servicios compartidos. Luego, estas zonas se pueden asociar VPCs a otras cuentas mediante la API de Route 53 o la AWS Command Line Interface (AWS CLI). AWS SDKs Los recursos asociados VPCs pueden entonces resolver los registros de DNS definidos en las zonas alojadas privadas, lo que crea una vista de DNS unificada en todo el AWS entorno.

En el diagrama siguiente se muestran los flujos de resolución de DNS en esta configuración básica.

Esta configuración funciona bien cuando se trabaja con una infraestructura de DNS a una escala limitada. Sin embargo, su administración puede resultar difícil a medida que crece el entorno. La sobrecarga operativa que supone administrar la forma en que se comparten y se asocian VPCs individualmente las reglas de las zonas alojadas privadas y del Resolver aumenta considerablemente con la escala. Además, las cuotas de servicio, como el límite de asociación de 300 VPC por zona alojada privada, pueden convertirse en factores restrictivos en las implementaciones a gran escala. La configuración mejorada aborda estos desafíos.

Configuración mejorada

Los perfiles de Route 53 ofrecen una solución simplificada para administrar la resolución de DNS en redes híbridas en varias Cuentas de AWS. En lugar de administrar las zonas alojadas privadas y las reglas de Resolver de forma individual, puede agrupar las configuraciones de DNS en un único contenedor que se pueda compartir y aplicar fácilmente en varias cuentas VPCs y cuentas de una región. Esta configuración mantiene la arquitectura centralizada del punto de conexión de Resolver en una VPC de servicios compartidos y, al mismo tiempo, simplifica considerablemente la administración de las configuraciones de DNS.

En el diagrama siguiente se muestran los flujos de resolución de DNS en una configuración mejorada.

Los perfiles de Route 53 le permiten empaquetar las asociaciones de zonas alojadas privadas, las reglas de reenvío de Resolver y las reglas de firewall de DNS en una sola unidad que se puede compartir. Puede crear perfiles en la cuenta de Shared Services y compartirlos con las cuentas de los miembros mediante AWS RAM. Cuando se comparte un perfil y se aplica a Target VPCs, el servicio gestiona automáticamente todas las asociaciones y configuraciones necesarias. Esto reduce de manera significativa los gastos generales operativos de la administración del DNS y proporciona una escalabilidad excelente para los entornos en crecimiento.

Automatización y escala

Utilice herramientas de infraestructura como código (IaC), como CloudFormation Terraform, para aprovisionar y administrar automáticamente los puntos finales, las reglas, las zonas alojadas privadas y los perfiles de Route 53 Resolver. Integre la configuración de DNS con flujos de integración continua y entrega continua (CI/CD) para lograr coherencia, repetibilidad y actualizaciones rápidas.

Tools (Herramientas)

Servicios de AWS

- AWS Resource Access Manager (AWS RAM) le ayuda a compartir sus recursos de forma segura Cuentas de AWS para reducir los gastos operativos y ofrecer visibilidad y auditabilidad.
- Amazon Route 53 Resolverresponde de forma recursiva a las consultas de DNS procedentes de AWS los recursos y está disponible de forma predeterminada en todos ellos. VPCs Puede crear puntos de enlace de Resolver y reglas de reenvío condicional para resolver los espacios de nombres DNS entre su centro de datos local y el suyo. VPCs
- Una zona alojada privada de Amazon Route 53 es un contenedor que aloja información acerca de cómo desea que responda Route 53 a las consultas de DNS de un dominio y sus subdominios.
- Los perfiles de Amazon Route 53 le permiten aplicar y gestionar configuraciones de Route 53 relacionadas con el DNS en muchas VPCs y diferentes Cuentas de AWS configuraciones de forma simplificada.

Prácticas recomendadas

En esta sección, se proporcionan algunas de las prácticas recomendadas para la optimización de Route 53 Resolver. Representan un subconjunto de las prácticas recomendadas de Route 53. Para obtener información completa, consulte Best practices for Amazon Route 53.

Evite las configuraciones en bucle con los puntos finales de Resolver

- Diseñe la arquitectura de DNS para evitar el enrutamiento recursivo y planifique con detenimiento las asociaciones de VPC. Cuando una VPC aloja un punto de conexión entrante, evite asociarlo a las reglas de Resolver que podrían crear referencias circulares.
- AWS RAM Utilízalos estratégicamente cuando compartas los recursos de DNS entre cuentas para mantener limpias las rutas de enrutamiento.

Para más información, consulte Avoid loop configurations with Resolver endpoints en la documentación de Route 53.

Escalado de puntos de conexión de Resolver

- En el caso de los entornos que requieren un número elevado de consultas por segundo (QPS), tenga en cuenta que hay un límite de 10 000 QPS por ENI en un punto de conexión. ENIs Se pueden añadir más a un punto final para escalar el QPS del DNS.
- Amazon CloudWatch proporciona `InboundQueryVolume` y `OutboundQueryVolume` métricas (consulta la CloudWatch documentación). Le recomendamos que configure reglas de supervisión que le avisen si el umbral supera un valor determinado (por ejemplo, el 80 % de 10 000 QPS).
- Configure reglas de grupos de seguridad con estado para los puntos de conexión de Resolver para evitar que los límites de seguimiento de la conexión provoquen una limitación de las consultas de DNS durante un tráfico de gran volumen. Para obtener más información sobre cómo funciona el seguimiento de conexiones en los grupos de seguridad, consulte el seguimiento de conexiones de los grupos de EC2 seguridad de Amazon en la EC2 documentación de Amazon.

Para más información, consulte Resolver endpoint scaling en la documentación de Route 53.

Cómo proporcionar alta disponibilidad para puntos de enlace de Resolver

- Cree puntos de conexión de entrada con las direcciones IP al menos en dos zonas de disponibilidad para la redundancia.

- Aprovisionamiento de interfaces de red adicionales para garantizar la disponibilidad durante el mantenimiento o los picos de tráfico.

Para más información, consulte High availability for Resolver endpoints en la documentación de Route 53.

Epics

Implementación de puntos de conexión de Route 53 Resolver

Tarea	Descripción	Habilidades requeridas
Cree un punto de conexión entrante.	Route 53 Resolver utiliza un punto de conexión de entrada para recibir las consultas de DNS de los solucionadores en las instalaciones. Para obtener instrucciones, consulte Reenviar las consultas de DNS entrantes a su cuenta VPCs en la documentación de Route 53. Anote la dirección IP del punto de conexión entrante.	Administrador de la nube, administrador de AWS
Implemente un punto de conexión saliente.	Route 53 Resolver utiliza un punto de conexión de salida para enviar las consultas de DNS de los soluciona dores en las instalaciones. Para obtener instrucciones, consulte Reenvío de consultas de DNS de salida a su red en la documentación de Route 53. Anote el ID del punto de conexión de salida.	Administrador de la nube, administrador de AWS

Configuración y uso compartido de zonas alojadas privadas de Route 53

Tarea	Descripción	Habilidades requeridas
Cree una zona alojada privada para un dominio alojado en AWS.	Esta zona contiene los registros DNS de los recursos AWS de un dominio hospedado (por ejemplo`prod.aws.example.com`) que deben resolverse desde el entorno local. Para obtener instrucciones, consulte Crear una zona alojada privada en la documentación de Route 53. Al crear una zona alojada privada, debe asociar una VPC a la zona alojada que es responsabilidad de la misma cuenta. Seleccione la VPC de servicios compartidos para este fin.	Administrador de la nube, administrador de AWS
Configuración básica: asocie la zona alojada privada a otras VPCs cuentas.	Si utiliza la configuración básica (consulte la sección Arquitectura): Para permitir que los recursos de la cuenta VPCs del miembro resuelvan los registros DNS de esta zona alojada privada, debe asociar los suyos VPCs a la zona alojada. Debe autorizar la asociación y, a continuación, crearla mediante programación. Para obtener instrucci	Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	ones, consulte Associating an Amazon VPC and a private hosted zone that you created with different Cuentas de AWS en la documentación de Route 53.	

Tarea	Descripción	Habilidades requeridas
Configuración mejorada: configure y comparta los perfiles de Route 53.	Si utiliza la configuración mejorada (consulte la sección Arquitectura): 1. Cree un perfil de Route 53 y asóciele las zonas alojadas privadas correspondientes. Para obtener instrucciones, consulte Creating Route 53 Profiles en la documentación de Route 53. 2. Se utiliza AWS RAM para compartir el perfil con las cuentas de los miembros y, a continuación, asociar el perfil compartido a Target VPCs. Para obtener instrucciones, consulte Compartir un perfil de Route 53 y Asociar un perfil de Route 53 VPCs en la documentación de Route 53. **Note** Según la estructura de su organización y los requisitos de DNS, es posible que deba crear y administrar varios perfiles para cuentas	Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	o cargas de trabajo distintas.	

Configuración y uso compartido de las reglas de reenvío de Route 53 Resolver

Tarea	Descripción	Habilidades requeridas
Cree una regla de reenvío para un dominio alojado en las instalaciones	Esta regla indicará a Route 53 Resolver que reenvíe las consultas de DNS para los dominios en las instalaciones (como `onprem.example.com`) a los solucionadores de DNS en las instalaciones. Para crear esta regla, necesitará las direcciones IP de los solucionadores de DNS en las instalaciones y el ID del punto de conexión saliente. Para obtener instrucciones, consulte Creación de reglas de reenvío en la documentación de Route 53.	Administrador de la nube, administrador de AWS
Configuración básica: comparte y asocia la regla de reenvío a la tuya VPCs en otras cuentas.	Si utiliza la configuración básica: Para que la regla de reenvío entre en vigor, debes compartir y asociar la regla a la tuya VPCs en otras cuentas. Luego, Route 53 Resolver toma en cuenta la	Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	regla al resolver un dominio. Para obtener instrucciones, consulte Compartir reglas de Resolver con otras Cuentas de AWS personas y usar reglas compartidas y Asociar reglas de reenvío a una VPC en la documentación de Route 53.	

Tarea	Descripción	Habilidades requeridas
Configuración mejorada: configure y comparta los perfiles de Route 53.	Si utiliza la configuración mejorada: 1. Si ya creó un perfil de Route 53 en los pasos anteriores, puede utilizar el mismo perfil. De lo contrario, cree un perfil de Route 53 y asóciele las reglas de reenvío de Resolver pertinentes. Para obtener instrucciones, consulte Creating Route 53 Profiles en la documentación de Route 53. 2. Se utiliza AWS RAM para compartir el perfil con las cuentas de los miembros y, a continuación, asociar el perfil compartido a Target. VPCs Para obtener instrucciones, consulte Compartir un perfil de Route 53 y asociar un perfil de Route 53 VPCs en la documentación de Route 53. **Note** Según la estructura de su organización y los requisitos de DNS, es posible que deba crear	Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	y administrar varios perfiles para cuentas o cargas de trabajo distintas.	

Configure los resolutores de DNS locales para la integración AWS

Tarea	Descripción	Habilidades requeridas
Configure el reenvío condicional en los solucionadores de DNS en las instalaciones.	Para que las consultas de DNS se envíen AWS desde el entorno local para su resolución, debe configurar el reenvío condicional en los solucionadores de DNS locales para que apunten a la dirección IP del punto final entrante. Esto indica a los solucionadores de DNS que reenvíen todas las consultas de DNS del dominio AWS hospedado (por ejemplo, para `prod.aws.example.com`) a la dirección IP del punto final de entrada para que Route 53 Resolver las resuelva.	Administrador de red

Verifique la resolución del end-to-end DNS en un entorno híbrido

Tarea	Descripción	Habilidades requeridas
Pruebe la resolución de DNS desde AWS el entorno local.	Desde una instancia en una VPC que tenga la regla	Administrador de red

Tarea	Descripción	Habilidades requeridas
	de reenvío asociada, haga una consulta de DNS para un dominio alojado en las instalaciones (por ejemplo, para `db.onprem.example.com`).	
Pruebe la resolución de DNS desde el entorno local hasta. AWS	Desde un servidor local, realice la resolución de DNS para un dominio AWS hospedado (por ejemplo, para). `ec2.prod.aws.example.com`	Administrador de red

Recursos relacionados

- Opciones de DNS en la nube híbrida para Amazon VPC (documento técnico)AWS
- Working with private hosted zones (documentación de Route 53)
- Getting started with Route 53 Resolver (documentación de Route 53)
- Simplifique la administración del DNS en un entorno de varias cuentas con Route 53 Resolver (entrada del blog)AWS
- Unifique la administración de DNS mediante perfiles de Amazon Route 53 con múltiples VPCs y Cuentas de AWS (AWS entrada de blog)
- Migración de su entorno DNS multicuenta a los perfiles de Amazon Route 53 (AWS entrada del blog)
- Uso de los perfiles de Amazon Route 53 para AWS entornos escalables con varias cuentas (AWS entrada del blog)

Verifique que los equilibradores de carga ELB requieran la terminación de TLS

Priyanka Chaudhary, Amazon Web Services

Resumen

En la nube de Amazon Web Services (AWS), Elastic Load Balancing (ELB) distribuye automáticamente el tráfico entrante de las aplicaciones entre varios destinos, como instancias de Amazon Elastic Compute Cloud EC2 (Amazon), contenedores, direcciones IP y funciones de AWS Lambda. Los equilibradores de carga emplean oyentes para definir los puertos y protocolos que usa el equilibrador de carga para aceptar el tráfico de los usuarios. Los balanceadores de carga de aplicaciones toman las decisiones de enrutamiento en la capa de aplicación y utilizan los protocolos. HTTP/HTTPS Los equilibradores de carga clásicos toman las decisiones de enrutamiento en la capa de transporte, mediante los protocolos TCP o Secure Sockets Layer (SSL), o en la capa de aplicación, mediante HTTP/HTTPS.

Este patrón proporciona un control de seguridad que examina varios tipos de eventos para los equilibradores de carga de aplicaciones y los equilibradores de carga clásicos. Cuando se invoca la función, AWS Lambda inspecciona el evento y se asegura de que el equilibrador de carga sea compatible.

La función inicia un evento de Amazon CloudWatch Events en las siguientes llamadas a la API: CreateLoadBalancerCreateLoadBalancerListeners, DeleteLoadBalancerListeners, CreateLoadBalancerPolicy, SetLoadBalancerPoliciesOfListener, CreateListenerDeleteListener, y ModifyListener. Cuando el evento detecta uno de estos APIs, llama a AWS Lambda, que ejecuta un script de Python. El script de Python evalúa si el oyente contiene un certificado SSL y si la política que se aplica utiliza seguridad de la capa de transporte (TLS). Si se determina que la política de SSL es distinta de TLS, la función envía una notificación de Amazon Simple Notification Service (Amazon SNS) al usuario con la información pertinente.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa

Limitaciones

- Este control de seguridad no comprueba los equilibradores de carga existentes, a menos que se realice una actualización en los dispositivos de escucha del equilibrador de carga.
- Este control de seguridad es regional. Debe implementarlo en cada región de AWS que desee supervisar.

Arquitectura

Arquitectura de destino

Automatización y escala

- Si utiliza AWS Organizations, puede utilizar AWS Cloudformation StackSets para implementar esta plantilla en varias cuentas que desee supervisar.

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual.
- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS.
- AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable que se puede utilizar para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.

Código

Este patrón incluye los siguientes archivos adjuntos:

- `ELBRequirestlstermination.zip`: el código de Lambda para el control de seguridad.
- `ELBRequirestlstermination.yml`— La CloudFormation plantilla que configura el evento y la función Lambda.

Epics

Configuración del bucket de S3

Tarea	Descripción	Habilidades requeridas
Defina el bucket de S3.	En la consola Amazon S3, elija o cree un bucket de S3 para alojar el archivo .zip de código de Lambda. Este bucket de S3 debe estar en la misma región de AWS que el equilibrador de carga que desea evaluar. Un nombre de bucket de S3 es globalmente único y todas las cuentas de AWS comparten el espacio de nombres. El nombre de bucket de S3 no puede incluir barras a la izquierda.	Arquitecto de la nube
Cargue el código de Lambda.	Cargue el código de Lambda (archivo `ELBRequirestlstermination.zip`) que se proporciona en la sección Adjuntos en el bucket de S3.	Arquitecto de la nube

Implemente la plantilla CloudFormation

Tarea	Descripción	Habilidades requeridas
Lance la CloudFormation plantilla de AWS.	Abra la CloudFormation consola de AWS en la misma región de AWS que su bucket de S3 e implemente la plantilla adjunta`ELBRequirestlstermination.yml` . Para obtener más información sobre la implementación de CloudFormation plantillas de AWS, consulte Crear una pila en la CloudFormation consola de AWS en la CloudFormation documentación.	Arquitecto de la nube
Complete los parámetros de la plantilla.	Al lanzar la plantilla, se le solicitará la siguiente información: • Bucket de S3: especifique el bucket creado o seleccionado en la primera Epic. Aquí es donde cargó el código de Lambda adjunto (archivo `ELBRequirestlstermination.zip`). • Clave S3: especifique la ubicación del archivo .zip de Lambda en el bucket de S3 (por ejemplo, `ELBRequirestlstermination.zip` o). `controls/ELBRequirestlsterm`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	`ination.zip` No incluya barras a la izquierda . • Correo electrónico de notificación: proporcione una dirección de correo electrónico activa en la que desea recibir las notificac iones de Amazon SNS. • Nivel de registro Lambda: especifique el nivel y la frecuencia de registro de la función de Lambda. Utilice Info para registrar mensajes informativos detallados sobre el progreso, Error para los eventos de error que pudieran continuar con la implementación y Advertencia en caso de situaciones potencialmente dañinas.	

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la CloudFormation plantilla se implementa correctamente, envía un correo electrónico de suscripci ón a la dirección de correo electrónico que proporcionó. Debe confirmar esta suscripci	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	ón de correo electrónico para recibir las notificaciones de infracciones.	

Recursos relacionados

- Creación de una pila en la CloudFormation consola de AWS (CloudFormation documentación de AWS)
- ¿Qué es AWS Lambda? (documentación de AWS Lambda)
- ¿Qué es un equilibrador de carga clásico? (documentación del ELB)
- ¿Qué es un equilibrador de carga de aplicación? (documentación del ELB)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Visualización de los registros y las métricas de AWS Network Firewall mediante Splunk

Ivo Pinto, Amazon Web Services

Resumen

Muchas organizaciones utilizan Splunk Enterprise como una herramienta centralizada de agregación y visualización de registros y métricas de diferentes fuentes. Este patrón le ayuda a configurar Splunk para obtener registros y métricas de AWS Network Firewall de Amazon CloudWatch Logs mediante el complemento Splunk para AWS.

Para ello, cree un rol de AWS Identity and Access Management (IAM) de solo lectura. El complemento Splunk para AWS utiliza esta función para acceder CloudWatch. Debe configurar el complemento Splunk para que AWS extraiga métricas y registros. CloudWatch Por último, debe crear visualizaciones en Splunk a partir de los datos de registro y las métricas recuperados.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Splunk
- Una instancia de Splunk Enterprise, versión 8.2.2 o posterior
- Una cuenta de AWS activa
- Network Firewall, instalado y configurado para enviar CloudWatch registros a Logs

Limitaciones

- Splunk Enterprise debe implementarse como un clúster de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la nube de AWS.
- La recopilación de datos mediante un rol de IAM detectado automáticamente para Amazon EC2 no está permitida en las regiones de AWS China.

Arquitectura

En el siguiente diagrama se ilustra lo siguiente:

1. Network Firewall publica CloudWatch registros en Logs.
2. Splunk Enterprise recupera métricas y registros de. CloudWatch

Para rellenar métricas y registros de ejemplo en esta arquitectura, una carga de trabajo genera tráfico que pasa a través del punto de conexión de Network Firewall para ir a Internet. Esto se logra mediante el uso de tablas de rutas. Si bien este patrón utiliza una única instancia de Amazon EC2 como carga de trabajo, se puede aplicar a cualquier arquitectura siempre que Network Firewall esté configurado para enviar registros a CloudWatch Logs.

Esta arquitectura también utiliza una instancia de Splunk Enterprise en otra nube privada virtual (VPC). Sin embargo, la instancia de Splunk puede estar en otra ubicación, por ejemplo, en la misma VPC que la carga de trabajo, siempre que pueda llegar a. CloudWatch APIs

Tools (Herramientas)

Servicios de AWS

- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas, aplicaciones y servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- AWS Network Firewall es un servicio de detección y prevención de intrusiones y firewall de red gestionado y con estado para la VPCs nube de AWS.

Otras herramientas

- Splunk le permite monitorear, visualizar y analizar los datos de registro.

Epics

Creación de un rol de IAM

Tarea	Descripción	Habilidades requeridas
Creación de la política de IAM.	Siga las instrucciones de la sección Creación de políticas	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	mediante el editor JSON para crear la política de IAM que conceda acceso de solo lectura a los datos y las métricas de los CloudWatch registros. CloudWatch Pegue la siguiente política de en el editor JSON. `{ "Statement": [ { "Action": [ "cloudwatch:List*", "cloudwatch:Get*", "network-firewall: List*", "logs:Describe*", "logs:Get*", "logs:List*", "logs:StartQuery", "logs:StopQuery", "logs:TestMetricFi lter", "logs:FilterLogEve nts", "network-firewall: Describe*" ],`	

Tarea	Descripción	Habilidades requeridas
	<pre>"Effect": "Allow", "Resource": "*" }], "Version": "2012-10-17" }</pre>	
Cree un rol de IAM nuevo.	Siga las instrucciones de Crear un rol para delegar permisos a un servicio de AWS para crear el rol de IAM al que utiliza el complemento Splunk para AWS para acceder. CloudWatch En Políticas de permisos, elija la política que creó anteriormente.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Asigne el rol de IAM a las instancias de EC2 en el clúster de Splunk.	1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/. 2. En el panel de navegación, seleccione Instances (Instancias). 3. Seleccione las instancias de EC2 en el clúster de Splunk. 4. Elija Acciones, Seguridad y, a continuación, Modificar rol de IAM. 5. Seleccione el rol de IAM que creó anteriormente y, a continuación, elija Guardar.	Administrador de AWS

Instale el complemento de Splunk para AWS.

Tarea	Descripción	Habilidades requeridas
Instale el complemento .	1. En el panel de control de Splunk, vaya a Splunk Apps. 2. Busque el complemento de Splunk para Amazon Web Services. 3. Elija Instalar. 4. Proporcione las credenciales de Splunk.	Administrador de Splunk
Configure las credenciales de AWS.	1. En el panel de control de Splunk, vaya a Splunk Add-on for AWS.	Administrador de Splunk

Tarea	Descripción	Habilidades requeridas
	2. Elija Configuración. 3. En la columna Autodisco vered IAM Role, seleccion e el rol de IAM que creó anteriormente. Para más información, consulte Find an IAM role within your Splunk platform instance en la documentación de Splunk.	

Configure el acceso de Splunk a CloudWatch

Tarea	Descripción	Habilidades requeridas
Configure la recuperación de los registros de Network Firewall desde los CloudWatc h registros.	1. En el panel de control de Splunk, vaya a Splunk Add-on for AWS. 2. Elija Input. 3. Elija Create New Input. 4. En la lista, elija Tipo de datos personalizado y, a continuación, seleccione CloudWatch Registros. 5. Proporcione el nombre, la cuenta de AWS, la región de AWS y el grupo de registros de sus registros de Network Firewall. 6. Seleccione Save.	Administrador de Splunk

Tarea	Descripción	Habilidades requeridas
	De manera predeterminada, Splunk recupera los datos del registro cada 10 minutos. Se trata de un parámetro configurable en Advanced Settings. Para obtener más información, consulte Configurar una entrada de CloudWatch registros mediante Splunk Web en la documentación de Splunk.	

Tarea	Descripción	Habilidades requeridas
Configure la recuperación de las métricas de Network Firewall desde CloudWatch.	1. En el panel de control de Splunk, vaya a Splunk Add-on for AWS. 2. Elija Input. 3. Elija Create New Input. 4. En la lista, elija CloudWatch. 5. Proporcione el nombre, la cuenta de AWS, la región de AWS para las métricas de Network Firewall. 6. Junto a Metric Configuration, elija Edit in advanced mode. 7. (Opcional) Elimine todos los espacios de nombres preconfigurados. 8. Elija Agregar espacio de nombres y, a continuación, asígnele el nombre AWS/.NetworkFirewall 9. En Dimension Value, agregue lo siguiente. `[{"AvailabilityZone":[".*"],"Engine":[".*"],"FirewallName":[".*"]}]` 10. En Metrics, elija All. 11. En Metric Statistics, elija Sum. 12. Seleccione Aceptar.	Administrador de Splunk

Tarea	Descripción	Habilidades requeridas
	13. Seleccione Save. De manera predeterminada, Splunk recupera los datos de las métricas cada 5 minutos. Se trata de un parámetro configurable en Advanced Settings. Para obtener más información, consulte Configurar una CloudWatch entrada mediante Splunk Web en la documentación de Splunk.	

Creación de visualizaciones de Splunk mediante consultas

Tarea	Descripción	Habilidades requeridas
Vea las direcciones IP de origen principal.	1. En el panel de control de Splunk, vaya a Search & Reporting. 2. En el cuadro enter search here, introduzca lo siguiente. `sourcetype="aws:cloudwatchlogs" | top event.src_ip` Esta consulta muestra una tabla de las direcciones IP de origen con más tráfico, en orden descendente.	Administrador de Splunk

Tarea	Descripción	Habilidades requeridas
	3. Para obtener una representación gráfica, elija Visualization.	
Vea las estadísticas de los paquetes.	1. En el panel de control de Splunk, vaya a Search & Reporting. 2. En el cuadro enter search here, introduzca lo siguiente. `sourcetype="aws:cloudwatch"| timechart sum(Sum) by metric_name` Esta consulta muestra una tabla con las métricas `DroppedPackets`, `PassedPackets` y `ReceivedPackets` por minuto. 3. Para obtener una representación gráfica, elija Visualization.	Administrador de Splunk

Tarea	Descripción	Habilidades requeridas
Vea los puertos de origen más utilizados.	1. En el panel de control de Splunk, vaya a Search & Reporting. 2. En el cuadro enter search here, introduzca lo siguiente . `sourcetype="aws:cloudwatchlogs" | top event.dest_port` Esta consulta muestra una tabla de los puertos de origen con más tráfico, en orden descendente. 3. Para obtener una representación gráfica, elija Visualization.	Administrador de Splunk

Recursos relacionados

Documentación de AWS

- Creación de un rol para delegar permisos a un servicio de AWS (documentación de IAM)
- Creación de políticas de IAM (documentación de IAM)
- Logging and monitoring in AWS Network Firewall (documentación de Network Firewall)
- Route table configurations for AWS Network Firewall (documentación de Network Firewall)

Publicaciones del blog de AWS

- AWS Network Firewall deployment models

AWS Marketplace

- Splunk Enterprise Amazon Machine Image (AMI)

Más patrones

- Acceda a un host bastión mediante Session Manager y Amazon EC2 Instance Connect
- Acceda a las aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS Fargate PrivateLink, AWS y un Network Load Balancer
- Acceda a las aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS PrivateLink y un Network Load Balancer
- Centralice la resolución de DNS mediante AWS Managed Microsoft AD Microsoft Active Directory local
- Cree un portal para microinterfaces mediante Angular AWS Amplify y Module Federation
- Implemente una API de Amazon API Gateway en un sitio web interno mediante puntos de conexión privados y un Equilibrador de carga de aplicación
- Implemente controles de acceso basados en atributos de detección para subredes públicas mediante AWS Config
- Implementación de controles de acceso preventivos basados en atributos para las subredes públicas
- Habilite conexiones cifradas para instancias de base de datos de PostgreSQL en Amazon RDS
- Amplíe VRFs su alcance a AWS mediante AWS Transit Gateway Connect
- Migre una carga de trabajo de F5 BIG-IP a F5 BIG-IP VE en Nube de AWS
- Migración de los controladores de entrada NGINX al activar el Modo automático de Amazon EKS
- Preserve el espacio IP enrutable en los diseños de VPC de varias cuentas para subredes que no son de carga de trabajo
- Impedir el acceso a Internet de las cuentas mediante una política de control de servicios
- Enviar alertas desde AWS Network Firewall a un canal de Slack
- Sirva contenido estático en un bucket de Amazon S3 a través de una VPC mediante Amazon CloudFront
- Configure la recuperación ante desastres para Oracle JD Edwards EnterpriseOne con AWS Elastic Disaster Recovery
- Utilice las consultas de BMC Discovery para extraer datos de migración para planificar la migración
- Uso de Network Firewall para capturar los nombres de dominio de DNS de la indicación del nombre del servidor para el tráfico saliente

Entrega de contenido

Temas

- Envíe AWS WAF registros a Splunk mediante AWS Firewall Manager Amazon Data Firehose
- Sirva contenido estático en un bucket de Amazon S3 a través de una VPC mediante Amazon CloudFront
- Más patrones

Envíe AWS WAF registros a Splunk mediante AWS Firewall Manager Amazon Data Firehose

Michael Friedenthal, Aman Kaur Gandhi, y JJ Johnson, Amazon Web Services

Resumen

Históricamente, había dos formas de mover los datos a Splunk: una arquitectura de inserción o una arquitectura de extracción. Una arquitectura de extracción ofrece garantías de entrega de los datos mediante reintentos, pero requiere recursos dedicados en Splunk que recopilen los datos. Las arquitecturas de extracción no suelen funcionar en tiempo real debido a las encuestas. Una arquitectura de inserción suele tener una latencia más baja, es más escalable y reduce la complejidad y los costos operativos. Sin embargo, no garantiza la entrega y, por lo general, requiere agentes.

La integración de Splunk con Amazon Data Firehose proporciona datos de streaming en tiempo real a Splunk a través de un recopilador de eventos HTTP (HEC). Esta integración ofrece las ventajas de las arquitecturas de inserción y extracción: garantiza la entrega de datos mediante reintentos, es prácticamente en tiempo real, es de baja latencia y tiene poca complejidad. El HEC envía los datos de forma rápida y eficiente a través de HTTP o HTTPS directamente a Splunk. HECs están basados en fichas, lo que elimina la necesidad de codificar las credenciales en una aplicación o en los archivos auxiliares.

En una AWS Firewall Manager política, puede configurar el registro de todo el tráfico de ACL AWS WAF web en todas sus cuentas y, a continuación, puede utilizar una transmisión de entrega de Firehose para enviar los datos de registro a Splunk para su supervisión, visualización y análisis. Esta solución proporciona los siguientes beneficios:

- Administración y registro centralizados del tráfico de ACL AWS WAF web en todas sus cuentas
- Integración de Splunk con una sola Cuenta de AWS
- Escalabilidad
- Entrega de datos de registro prácticamente en tiempo real
- Optimización de costos mediante el uso de una solución sin servidor, de forma que no tenga que pagar por los recursos no utilizados.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS que forma parte de una organización en AWS Organizations.
- Debe tener los siguientes permisos para habilitar el registro con Firehose:
  - `iam:CreateServiceLinkedRole`
  - `firehose:ListDeliveryStreams`
  - `wafv2:PutLoggingConfiguration`
- AWS WAF y su web ACLs debe estar configurada. Para obtener instrucciones, consulte Primeros pasos con AWS WAF.
- AWS Firewall Manager debe estar configurado. Para obtener instrucciones, consulte los AWS Firewall Manager prerequisites.
- Se AWS WAF deben configurar las políticas de seguridad de Firewall Manager para. Para obtener instrucciones, consulte Introducción a las AWS Firewall ManagerAWS WAF políticas.
- Splunk debe configurarse con un punto de conexión HTTP público al que pueda acceder Firehose.

Limitaciones

- Cuentas de AWS Deben gestionarse en una sola organización en AWS Organizations.
- La ACL web debe estar en la misma región que la transmisión de entrega. Si vas a capturar registros para Amazon CloudFront, crea el flujo de entrega Firehose en la región EE.UU. Este (Norte de Virginia),. `us-east-1`
- El complemento Splunk para Firehose está disponible para las implementaciones de pago de Splunk Cloud, las implementaciones distribuidas de Splunk Enterprise y las implementaciones de Splunk Enterprise de instancia única. Este complemento no es compatible con las implementaciones de prueba gratuitas de Splunk Cloud.

Arquitectura

Pila de tecnología de destino

- Firewall Manager
- Firehose
- Amazon Simple Storage Service (Amazon S3)

- AWS WAF
- Splunk

Arquitectura de destino

La siguiente imagen muestra cómo puede utilizar el Firewall Manager para registrar de forma centralizada todos los AWS WAF datos y enviarlos a Splunk a través de Firehose.

1. La AWS WAF web ACLs envía los datos de registro del firewall al Firewall Manager.
2. Firewall Manager envía los datos de registro a Firehose.
3. El flujo de entrega de Firehose reenvía los datos de registro a Splunk y a un bucket de S3. El bucket de S3 actúa como respaldo en caso de que se produzca un error en el flujo de entrega de Firehose.

Automatización y escala

Esta solución está diseñada para escalar y adaptarse a todos los AWS WAF sitios ALCs web de la organización. Puedes configurar todas las páginas web ACLs para que usen la misma instancia de Firehose. Sin embargo, si quiere configurar y usar varias instancias de Firehose, puede hacerlo.

Tools (Herramientas)

Servicios de AWS

- AWS Firewall Manageres un servicio de administración de seguridad que le ayuda a configurar y administrar de forma centralizada las reglas de firewall en todas sus cuentas y aplicaciones en AWS Organizations.
- Amazon Data Firehose le ayuda a entregar datos de streaming en tiempo real a otros Servicios de AWS puntos de enlace HTTP personalizados y puntos de enlace HTTP propiedad de proveedores de servicios externos compatibles, como Splunk.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS WAF es un firewall de aplicación web que lo ayuda a supervisar las solicitudes HTTP y HTTPS que se reenvían a los recursos de su aplicación web protegida.

Otras herramientas

- Splunk le permite monitorear, visualizar y analizar los datos de registro.

Epics

Configurar Splunk

Tarea	Descripción	Habilidades requeridas
Instale la aplicación Splunk para. AWS	1. Inicie sesión en su programa de envío intensivo de Splunk. La URL predeterminada es `http://<IP address>:8000` . 2. En el panel de navegación de la izquierda, junto a Aplicaciones, seleccione el botón de engranaje. 3. Seleccione Buscar más aplicaciones. 4. Busque la opción AWS. 5. En el caso de la aplicación Splunk para AWS, selecciona Instalar. 6. Introduzca sus credenciales de inicio de sesión en Splunk.com, acepte los términos y condiciones y, a continuación, seleccione Iniciar sesión e instalar. 7. Seleccione Listo.	Administrador de seguridad, administrador de Splunk
Instala el complemento para. AWS WAF	Repita las instrucciones anteriores para instalar el complemento AWS Web	Administrador de seguridad, administrador de Splunk

Tarea	Descripción	Habilidades requeridas
	Application Firewall para Splunk.	

Tarea	Descripción	Habilidades requeridas
Instale y configure el complemento Splunk para Firehose.	1. Instale y configure el complemento Splunk para Firehose. Como parte de la instalación y la configuración, si es necesario para su plataforma Splunk, debe configurar un recopilador de eventos HTTP y preparar la infraestructura para enviar los datos de registro a sus indexadores. Consulte las instrucciones correspondientes a su implementación de Splunk: • Implementación de Splunk Cloud (documentación de Splunk) • Implementación distribuida de Splunk Enterprise (documentación de Splunk) • Implementación de Splunk Enterprise en una sola instancia (documentación de Splunk) **Important** Detenga este procedimiento después de haber instalado y configurado el complemento	Administrador de seguridad, administrador de Splunk

Tarea	Descripción	Habilidades requeridas
	Splunk. No continúe con las instrucciones para configurar Firehose para enviar datos a la plataforma Splunk. 2. Anote el token del recopilador de eventos HTTP y el punto de conexión HTTP. Necesitará este valor más adelante, cuando configure el flujo de entrega.	

Creación de un flujo de entrega de Firehose

Tarea	Descripción	Habilidades requeridas
Conceda a Firehose acceso a un destino de Splunk	Configure la política de acceso que permite a Firehose acceder a un destino de Splunk y hacer una copia de seguridad de los datos de registro en un bucket de S3. Para más información, consulte Concesión a Firehose de acceso a un destino de Splunk.	Administrador de seguridad
Cree un flujo de entrega de Firehose.	En la misma cuenta ACLs para la que administras la web AWS WAF, crea un flujo de entrega en Firehose. Es obligatorio contar con un rol de IAM al crear un flujo de	Administrador de seguridad

Tarea	Descripción	Habilidades requeridas
	entrega. Firehose asume ese rol de IAM y obtiene acceso al bucket de S3 especificado. Para obtener instrucciones, consulte Crear un flujo de entrega. Tenga en cuenta lo siguiente: • El nombre de flujo de entrega debe empezar por `aws-waf-logs-` . • Para el origen, elija Direct PUT. • En Modo de copia de seguridad de S3, seleccione Hacer copia de seguridad de todos los eventos y, a continuación, elija un bucket existente o cree uno nuevo. • Para el destino, siga las instrucciones en Configuración de los ajustes de destino de Splunk en la documentación de Firehose. Para obtener información sobre los valores de los puntos de conexión de Splunk y los tipos de puntos de conexión, consulte Configure Amazon Data Firehose en la documentación de Splunk.	

Tarea	Descripción	Habilidades requeridas
	Repita este proceso para cada token que haya configurado en el recopilador de eventos HTTP.	
Pruebe el flujo de entrega.	Pruebe el flujo de entrega para comprobar que está configurado correctamente. Para obtener instrucciones, consulte Prueba con Splunk en la documentación de Kinesis Data Firehose.	Administrador de seguridad

Configurar Firewall Manager para registrar datos

Tarea	Descripción	Habilidades requeridas
Configure las políticas de Firewall Manager.	Las políticas de Firewall Manager deben configura rse para permitir el registro y reenviar los registros al flujo de entrega correcto de Firehose. Para obtener más información e instrucciones, consulta Cómo configurar el registro de una AWS WAF política.	Administrador de seguridad

Recursos relacionados

AWS resources

- Registro del tráfico de ACL web (AWS WAF documentación)
- Configuración del registro para una AWS WAF política (AWS WAF documentación)

- Tutorial: envío de registros de flujos de VOC a Splunk con Amazon Data Firehose (documentación de Firehose)
- How do I push VPC flow logs to Splunk using Amazon Data Firehose? (Centro de AWS conocimiento)
- Alimentación de datos en Splunk mediante Amazon Data Firehose (entrada del blog)AWS

Documentación de Splunk

- Splunk Add-on for Amazon Data Firehose

Sirva contenido estático en un bucket de Amazon S3 a través de una VPC mediante Amazon CloudFront

Angel Emmanuel Hernandez Cebrian, Amazon Web Services

Resumen

Cuando publicas contenido estático alojado en Amazon Web Services (AWS), el enfoque recomendado es utilizar un depósito de Amazon Simple Storage Service (S3) como origen y utilizar CloudFront Amazon para distribuir el contenido. Esta solución tiene dos ventajas principales: la comodidad de almacenar en caché el contenido estático en ubicaciones periféricas y la posibilidad de definir listas de control de acceso web (web ACLs) para la CloudFront distribución, lo que le ayuda a proteger las solicitudes de contenido con una configuración y una sobrecarga administrativa mínimas.

Sin embargo, el enfoque estándar recomendado tiene una limitación arquitectónica común. En algunos entornos, puede ser deseable que los dispositivos de firewall virtual se implementen en una nube privada virtual (VPC) para inspeccionar todo el contenido, incluido el contenido estático. El enfoque estándar no dirige el tráfico a través de la VPC para su inspección. Este patrón proporciona una solución arquitectónica alternativa. Se sigue utilizando una CloudFront distribución para ofrecer contenido estático en un bucket de S3, pero el tráfico se enruta a través de la VPC mediante un Application Load Balancer. A continuación, una función de AWS Lambda recupera y devuelve el contenido del bucket de S3.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Contenido estático del sitio web alojado en un bucket de S3.

Limitaciones

- Los recursos de este patrón deben estar en una sola región de AWS, pero se pueden aprovisionar en diferentes cuentas de AWS.
- Los límites se aplican al tamaño máximo de solicitud y respuesta que la función de Lambda puede, respectivamente, recibir y enviar. Para obtener más información, consulte Límites en Funciones de Lambda como destinos (documentación de Elastic Load Balancing).

- Al usar este enfoque, es importante encontrar un buen equilibrio entre el rendimiento, la escalabilidad, la seguridad y la rentabilidad. A pesar de la alta escalabilidad de Lambda, si el número de invocaciones simultáneas de Lambda supera la cuota máxima, algunas solicitudes se limitarán. Para más información, consulte las cuotas de Lambda (documentación de Lambda). También debe tener en cuenta los precios de uso de Lambda. Para minimizar las invocaciones a Lambda, asegúrese de definir correctamente la caché de la distribución. CloudFront Para obtener más información, consulte Optimización del almacenamiento en caché y la disponibilidad (documentación)CloudFront .

Arquitectura

Pila de tecnología de destino

- CloudFront
- Amazon Virtual Private Cloud (Amazon VPC)
- Equilibrador de carga de aplicación
- Lambda
- Amazon S3

Arquitectura de destino

La siguiente imagen muestra la arquitectura sugerida cuando es necesario utilizarla CloudFront para servir contenido estático desde un bucket de S3 a través de una VPC.

1. El cliente solicita la URL de CloudFront distribución para incluir un archivo de sitio web concreto en el bucket de S3.
2. CloudFront envía la solicitud a AWS WAF. AWS WAF filtra la solicitud mediante la web ACLs aplicada a la CloudFront distribución. Si se determina que la solicitud es válida, el flujo continúa. Si se determina que la solicitud no es válida, el cliente recibe un error 403.
3. CloudFront comprueba su caché interna. Si hay una clave válida que coincida con la solicitud entrante, el valor asociado se devuelve al cliente como respuesta. Si no es así, el flujo continúa.
4. CloudFront reenvía la solicitud a la URL del Application Load Balancer especificado.
5. El equilibrador de carga de aplicación tiene un oyente asociado a un grupo objetivo basado en una función de Lambda. El equilibrador de carga de aplicación invoca la función de Lambda.

6. La función de Lambda se conecta al bucket de S3, realiza una operación `GetObject` en él y devuelve el contenido como respuesta.

Automatización y escala

Para automatizar la implementación de contenido estático mediante este enfoque, cree CI/CD canalizaciones para actualizar los buckets de Amazon S3 que alojan sitios web.

La función de Lambda escala automáticamente para gestionar las solicitudes concurrentes, dentro de las cuotas y limitaciones del servicio. Para obtener más información, consulte Escalado de función de Lambda y Cuotas de Lambda (documentación de Lambda). Para los demás servicios y características de AWS, como CloudFront el Application Load Balancer, AWS los escala automáticamente.

Tools (Herramientas)

- Amazon CloudFront acelera la distribución de tu contenido web al distribuirlo a través de una red mundial de centros de datos, lo que reduce la latencia y mejora el rendimiento.
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos. En este patrón, se emplea un equilibrador de carga de aplicación, aprovisionado mediante Elastic Load Balancing, para dirigir el tráfico a la función de Lambda.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Epics

Se utiliza CloudFront para ofrecer contenido estático de Amazon S3 a través de una VPC

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	Cree una VPC para alojar los recursos implementados en este patrón, como el equilibrador de carga de aplicación y la función de Lambda. Para obtener instrucciones, consulte Crear una VPC (documentación de Amazon VPC).	Arquitecto de la nube
Cree una ACL web de AWS WAF.	Cree una ACL web de AWS WAF. Más adelante en este patrón, se aplica esta ACL web a la CloudFront distribución. Para obtener instrucciones, consulte Crear una ACL web (documentación de AWS WAF).	Arquitecto de la nube
Crear la función de Lambda.	Cree la función de Lambda que sirva el contenido estático alojado en el bucket de S3 como sitio web. Use el código que se proporciona en la sección de Información adicional de este patrón. Personalice el código para identificar su bucket de S3 de destino.	AWS general
Cargar la función de Lambda.	Introduzca el siguiente comando para cargar el	AWS general

Tarea	Descripción	Habilidades requeridas
	código de la función de Lambda en un archivo .zip en Lambda. `aws lambda update-function-code \ --function-name \ --zip-file fileb://lambda-alb-s3-website.zip`	
Cree un Equilibrador de carga de aplicación.	Cree un equilibrador de carga de aplicación con acceso a Internet que apunte a la función de Lambda. Para obtener instrucciones, consulte Crear un grupo de destino para la función de Lambda (documentación de Elastic Load Balancing). Para una configuración de alta disponibilidad, cree el equilibrador de carga de aplicación y adjúntelo a subredes privadas en distintas zonas de disponibilidad.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Cree una CloudFront distribución.	Cree una CloudFront distribución que apunte al Application Load Balancer que creó. 1. Inicie sesión en la consola de administración de AWS y abra la CloudFront consola en la https://console.aws.amazon.com/cloudfront/versión 3/home. 2. Seleccione Create Distribution (Crear distribución). 3. En la primera página del Create Distribution Wizard (Asistente de creación de distribuciones), en la sección Web, elija Get Started (Empezar). 4. Especifique la configuración de su distribución. Para obtener más información, consulte Valores que especifica cuando crea o actualiza una distribución. Tenga en cuenta lo siguiente: a. Establezca el equilibrador de carga de aplicación como origen. b. En la configuración de distribución, elija la web existente ACLs que desee aplicar a través de AWS WAF. Para más	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	información, consulte ACL web de AWS WAF. 5. Guarde los cambios. 6. Una CloudFront vez creada la distribución, el valor de la columna Estado de la distribución cambia de InProgressa Implement ada. Si decidió habilitar la distribución, estará lista para procesar solicitudes cuando el estado cambie a Deployed (Implementado).	

Recursos relacionados

Documentación de AWS

- Optimización del almacenamiento en caché y la disponibilidad (CloudFront documentación)
- Funciones de Lambda como destinos (documentación de Elastic Load Balancing)
- Cuotas de Lambda (documentación de Lambda)

Sitios web de servicios de AWS

- Equilibrador de carga de aplicación
- Lambda
- CloudFront
- Amazon S3
- AWS WAF
- Amazon VPC

Información adicional

Código

El siguiente ejemplo de función de Lambda está escrito en Node.js. Esta función de Lambda actúa como un servidor web que realiza una operación `GetObject` en un bucket de S3 que contiene los recursos del sitio web.

```
/**

 * This is an AWS Lambda function created for demonstration purposes.

 * It retrieves static assets from a defined Amazon S3 bucket.

 * To make the content available through a URL, use an Application Load Balancer with a
 Lambda integration.
 *
 * Set the S3_BUCKET environment variable in the Lambda function definition.
 */

var AWS = require('aws-sdk');

exports.handler = function(event, context, callback) {

    var bucket = process.env.S3_BUCKET;
    var key = event.path.replace('/', '');

    if (key == '') {
        key = 'index.html';
    }

    // Fetch from S3
    var s3 = new AWS.S3();
    return s3.getObject({Bucket: bucket, Key: key},
       function(err, data) {

            if (err) {
                return err;
            }

            var isBase64Encoded = false;
            var encoding = 'utf8';
```

```
            if (data.ContentType.indexOf('image/') > -1) {
                isBase64Encoded = true;
                encoding = 'base64'
            }

            var resp = {
                statusCode: 200,
                headers: {
                    'Content-Type': data.ContentType,
                },
                body: new Buffer(data.Body).toString(encoding),
                isBase64Encoded: isBase64Encoded
            };

            callback(null, resp);
        }
    );
};
```

Más patrones

- Comprueba la versión de registro de acceso, HTTPS y TLS en una CloudFront distribución de Amazon
- Implemente una aplicación basada en gRPC en un clúster de Amazon EKS y acceda a ella con un Equilibrador de carga de aplicación
- Implementación de controles de acceso preventivos basados en atributos para las subredes públicas
- Despliega recursos en una AWS Wavelength zona mediante Terraform
- Implemente las automatizaciones de seguridad para la AWS WAF solución mediante Terraform
- Configuración de un router de celdas sin servidor para una arquitectura basada en celdas
- Uso de Amazon Q Developer como asistente de codificación para aumentar la productividad
- Visualización de los registros y las métricas de AWS Network Firewall mediante Splunk

&Almacenamiento de bases de datos

Temas

- Bases de datos
- Almacenamiento y copia de seguridad

Bases de datos

Temas

- Acceda a tablas locales de Microsoft SQL Server desde Microsoft SQL Server en Amazon EC2 mediante servidores enlazados
- Agregue HA a Oracle PeopleSoft en Amazon RDS Custom mediante una réplica de lectura
- Análisis de las dependencias de los objetos para realizar migraciones parciales de bases de datos de Oracle a PostgreSQL
- Evaluar el rendimiento de las consultas para migrar bases de datos de SQL Server a MongoDB Atlas en AWS
- Automatice blue/green las implementaciones de las bases de datos globales de Amazon Aurora mediante los principios de la IaC
- Automatice la replicación de las instancias de Amazon RDS en Cuentas de AWS
- Automatice las tareas de bases de datos en SQL Server Express en Amazon EC2 mediante un programador AWS Lambda de tareas
- Automatización de la conmutación por error y la conmutación por recuperación entre regiones mediante DR Orchestrator Framework
- Realice copias de seguridad automáticas de las bases de datos de SAP HANA mediante Systems Manager y EventBridge
- Generación automática de un modelo de PynamoDB y funciones CRUD para Amazon DynamoDB mediante una aplicación de Python
- Bloquee el acceso público a Amazon RDS mediante Cloud Custodian
- Configure la autenticación de Windows para Amazon RDS for Microsoft SQL Server mediante AWS Managed Microsoft AD
- Configurar el acceso entre cuentas a Amazon DynamoDB
- Configurar el enrutamiento de solo lectura en los grupos de disponibilidad de Always On en SQL Server on AWS
- Conectar mediante un túnel SSH en pgAdmin
- Convertir consultas JSON de Oracle en SQL de bases de datos PostgreSQL
- Copie tablas de Amazon DynamoDB entre cuentas mediante AWS Backup
- Copiar tablas de Amazon DynamoDB entre cuentas mediante una implementación personalizada
- Crear informes detallados de costos y uso para Amazon RDS y Amazon Aurora

- Implemente instancias de clústeres de conmutación por error de SQL Server en Amazon EC2 y Amazon FSx mediante Terraform
- Emule las matrices PL/SQL asociativas de Oracle en Amazon Aurora PostgreSQL y Amazon RDS for PostgreSQL
- Habilite conexiones cifradas para instancias de base de datos de PostgreSQL en Amazon RDS
- Cifrar una instancia de base de datos de Amazon RDS para PostgreSQL existente
- Imponga el etiquetado automático de las bases de datos de Amazon RDS en el lanzamiento
- Estime el costo de una tabla de DynamoDB para la capacidad bajo demanda
- Costos de almacenamiento estimados para una tabla de Amazon DynamoDB
- Calcule el tamaño del motor de Amazon RDS para una base de datos de Oracle mediante informes de AWR
- Exporte tablas de Amazon RDS for SQL Server a un bucket de S3 mediante AWS DMS
- Gestionar bloques anónimos en instrucciones SQL dinámicas en Aurora PostgreSQL
- Ayudar a reforzar el etiquetado en DynamoDB
- Implemente recuperación de desastres entre regiones con AWS DMS y Amazon Aurora
- Migración de funciones y procedimientos de Oracle con más de 100 argumentos a PostgreSQL
- Migre una base de datos de Oracle a Amazon RDS mediante la importación directa de Oracle Data Pump a través de un enlace de base de datos
- Migración de las cargas de trabajo de Redis a Redis Enterprise Cloud en AWS
- Migración de SAP HANA a AWS mediante SAP HSR con el mismo nombre de host
- Migre el grupo de disponibilidad Always On de Microsoft SQL Server mediante AWS Transform MGN
- Migración de SQL Server a AWS mediante grupos de disponibilidad distribuidos
- Migrar una base de datos relacional a MongoDB Atlas en AWS
- Migre un entorno MongoDB autohospedado a MongoDB Atlas en AWS
- Migración de una base de datos de Oracle a Amazon DynamoDB mediante AWS DMS
- Migre de Oracle 8i o 9i a Amazon RDS para Oracle con AWS DMS SharePlex
- Migración de una base de datos MySQL en las instalaciones a Amazon EC2
- Supervise GoldenGate los registros de Oracle mediante Amazon CloudWatch
- Redefina la plataforma de Oracle Database Enterprise Edition a Standard Edition 2 en Amazon RDS para Oracle

- Replicar bases de datos de unidades centrales en AWS mediante Precisely Connect
- Programe trabajos para Amazon RDS para PostgreSQL y Aurora PostgreSQL mediante Lambda y Secrets Manager
- Envíe notificaciones para una instancia de base de datos de Amazon RDS para SQL Server mediante un servidor SMTP en las instalaciones y el Correo de base de datos
- Configurar la recuperación de desastres para SAP en IBM Db2 en AWS
- Configure una CI/CD canalización para la migración de bases de datos mediante Terraform
- Configure un clúster de conmutación por error de Microsoft SQL Server en Amazon EC2 FSx mediante Windows File Server
- Configure una HA/DR arquitectura para Oracle E-Business Suite en Amazon RDS Custom con una base de datos en espera activa
- Transmita datos desde IBM Db2, SAP, Sybase y otras bases de datos a MongoDB Atlas en AWS
- Funciones de transición para una PeopleSoft aplicación de Oracle en Amazon RDS Custom for Oracle
- Descarga de datos de un clúster de Amazon Redshift entre las cuentas a Amazon S3
- Patrones de migración de bases de datos según carga de trabajo
- Más patrones

Acceda a tablas locales de Microsoft SQL Server desde Microsoft SQL Server en Amazon EC2 mediante servidores enlazados

Tirumala Dasari y Eduardo Valentim, Amazon Web Services

Resumen

Este patrón describe cómo acceder a las tablas de bases de datos de Microsoft SQL Server locales que se ejecutan en Microsoft Windows, desde bases de datos de Microsoft SQL Server que se ejecutan o alojan en instancias de Windows o Linux de Amazon Elastic Compute Cloud (Amazon EC2) mediante servidores vinculados.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Amazon EC2 con Microsoft SQL Server ejecutándose en la AMI de Amazon Linux (Amazon Machine Image)
- AWS Direct Connect entre el servidor Microsoft SQL Server (Windows) local y la instancia de Windows o Linux EC2

Versiones de producto

- Servidor SQL 2016 o posterior

Arquitectura

Pila de tecnología de origen

- Base de datos Microsoft SQL Server en las instalaciones que se ejecuta en Windows
- Amazon EC2 con Microsoft SQL Server ejecutándose en una AMI de Windows o una AMI de Linux

Pila de tecnología de destino

- Amazon EC2 con Microsoft SQL Server ejecutándose en la AMI de Amazon Linux
- Amazon EC2 con Microsoft SQL Server ejecutándose en una AMI de Windows

Arquitectura de base de datos de origen y destino

Tools (Herramientas)

- Microsoft SQL Server Management Studio (SSMS) es un entorno integrado para administrar infraestructuras de SQL Server. Proporciona una interfaz de usuario y un grupo de herramientas con editores de scripts enriquecidos que interactúan con SQL Server.

Epics

Cómo cambiar el modo de autenticación a Windows para SQL Server en Windows SQL Server

Tarea	Descripción	Habilidades requeridas
Conéctese a Windows SQL Server mediante SSMS.		Administrador de base de datos
Cambie el modo de autenticación a Windows en SQL Server desde el menú contextual (haga clic con el botón derecho) de la instancia de Windows SQL Server.		Administrador de base de datos

Reiniciar el servicio Windows MSSQL

Tarea	Descripción	Habilidades requeridas
Reinicie el servicio SQL.	1. En el Explorador de objetos de SSMS, seleccione la instancia de SQL Server. 2. Abra el menú contextual (con el botón derecho). 3. Elija Reiniciar.	Administrador de base de datos

Crear un nuevo inicio de sesión y seleccionar las bases de datos a las que acceder en Windows SQL Server

Tarea	Descripción	Habilidades requeridas
En la pestaña Seguridad, abra el menú contextual (haga clic con el botón derecho) de Inicio de sesión y seleccione un nuevo inicio de sesión.		Administrador de base de datos
En la pestaña General, seleccione la autenticación de SQL Server, introduzca un nombre de usuario, introduzc a la contraseña y, a continuac ión, confirme la contraseñ a y desactive la opción de cambiarla la próxima vez que inicie sesión.		Administrador de base de datos
En la pestaña Funciones del servidor, seleccione Público.		Administrador de base de datos
En la pestaña de asignacio nes de usuario, seleccione la base de datos y el esquema a los que desee acceder y, a continuación, resalte la base de datos para seleccionar los roles de la base de datos.	Seleccione public y db_datare ader para acceder a los datos de las tablas de la base de datos.	Administrador de base de datos
Pulse Aceptar para crear un usuario.		Administrador de base de datos

Agregue la IP de Windows SQL Server al archivo host de Linux SQL Server

Tarea	Descripción	Habilidades requeridas
Conéctese a la caja de Linux SQL Server a través de la ventana del terminal.		Administrador de base de datos
Abra el archivo /etc/hosts y añada la dirección IP del equipo Windows con SQL Server.		Administrador de base de datos
Guarde el archivo de hosts.		Administrador de base de datos

Crear un servidor vinculado en Linux SQL Server

Tarea	Descripción	Habilidades requeridas
Cree un servidor vinculado mediante los procedimientos almacenados master.sys.sp_addlinkedserver y master.dbo.sp_addlinkedsrvlogin.	Para obtener más información sobre el uso de estos procedimientos almacenados, consulte la sección de Información adicional.	Administrador de base de datos, desarrollador

Verifique el servidor vinculado y las bases de datos creados en SSMS

Tarea	Descripción	Habilidades requeridas
En Linux SQL Server en SSMS, vaya a servidores vinculados y actualice.		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Expanda los servidores y catálogos vinculados creados en el panel izquierdo.	Verá las bases de datos de SQL Server seleccionadas con tablas y vistas.	Administrador de base de datos

Verificar que puede acceder a las tablas de bases de datos de Windows SQL Server

Tarea	Descripción	Habilidades requeridas
En la ventana de consulta de SSMS, ejecute la siguiente consulta: "seleccionar los primeros 3 * de [sqllin]. dms_sample_win.dbo .mlb_data".	Tenga en cuenta que la cláusula FROM utiliza una sintaxis de cuatro partes: computer.database.schema.table (por ejemplo, SELECT name "SQL2 databases » FROM [sqllin] .master.sys.databases). En nuestro ejemplo, creamos un alias para SQL2 en el archivo de hosts, por lo que no es necesario escribir el nombre real de NetBIOS entre corchetes. Si utiliza los nombres de NetBIOS reales, tenga en cuenta que AWS utiliza de forma predeterminada los nombres de NetBIOS, como Win-xxxx, y SQL Server requiere corchetes para los nombres con guiones.	Administrador de base de datos, desarrollador

Recursos relacionados

- Notas de la versión de SQL Server en Linux

Información adicional

Uso de procedimientos almacenados para crear servidores vinculados

SSMS no admite la creación de servidores vinculados para Linux SQL Server, por lo que debe usar estos procedimientos almacenados para crearlos:

```
EXEC master.sys.sp_addlinkedserver @server= N'SQLLIN' , @srvproduct= N'SQL Server'
EXEC master.dbo.sp_addlinkedsrvlogin
 @rmtsrvname=N'SQLLIN',@useself=N'False',@locallogin=NULL,@rmtuser=N'username',@rmtpassword='Te
```

Nota 1: Introduzca las credenciales de inicio de sesión que creó anteriormente en Windows SQL Server en el procedimiento almacenado `master.dbo.sp_addlinkedsrvlogin`.

Nota 2: El nombre `@server`, `SQLLIN` y el nombre de la entrada del archivo host `172.12.12.4 SQLLIN` deben ser los mismos.

Puede utilizar este proceso para crear servidores vinculados en los siguientes casos:

- De Linux SQL Server a Windows SQL Server a través de un servidor vinculado (como se especifica en este patrón)
- De Windows SQL Server a Linux SQL Server a través de un servidor vinculado
- De Linux SQL Server a otro servidor SQL de Linux a través de un servidor vinculado

Agregue HA a Oracle PeopleSoft en Amazon RDS Custom mediante una réplica de lectura

Sampath Kathirvel, Amazon Web Services

Resumen

Para ejecutar la solución de planificación de recursos PeopleSoft empresariales (ERP) de Oracle en Amazon Web Services (AWS), puede utilizar Amazon Relational Database Service (Amazon RDS) o Amazon RDS Custom for Oracle, que admite aplicaciones heredadas, personalizadas y empaquetadas que requieren acceso al sistema operativo y al entorno de base de datos subyacentes. Para conocer los factores clave a tener en cuenta durante la planificación de una migración, consulte Estrategias de migración de bases de datos de Oracle en Recomendaciones de AWS.

En el momento de escribir este artículo, RDS Custom para Oracle no admite la opción Multi-AZ, que está disponible para Amazon RDS para Oracle como una solución de alta disponibilidad que utiliza la replicación del almacenamiento. En su lugar, este patrón logra la alta disponibilidad mediante el uso de una base de datos en espera que crea y mantiene una copia física de la base de datos principal. El patrón se centra en los pasos para ejecutar una base de datos de PeopleSoft aplicaciones en Amazon RDS Custom with HA mediante Oracle Data Guard para configurar una réplica de lectura.

Este patrón también cambia la réplica de lectura al modo de solo lectura. Tener la réplica de lectura en modo de solo lectura ofrece ventajas adicionales:

- Descargar las cargas de trabajo de solo lectura de la base de datos principal
- Permitir la reparación automática de los bloques dañados mediante la recuperación de bloques en buen estado de la base de datos en espera mediante la característica Oracle Active Data Guard
- Uso de la capacidad Far Sync para mantener sincronizada la base de datos remota en espera sin la sobrecarga de rendimiento asociada a la transmisión de registros redo a larga distancia.

El uso de una réplica en modo de solo lectura requiere la opción Oracle Active Data Guard, que tiene un costo adicional, ya que se trata de una característica de Oracle Database Enterprise Edition con licencia independiente.

Requisitos previos y limitaciones

Requisitos previos

- Una PeopleSoft aplicación existente en Amazon RDS Custom. Si no tiene una aplicación, consulte el patrón Migrate Oracle PeopleSoft to Amazon RDS Custom.
- Un único nivel PeopleSoft de aplicación. Sin embargo, puede adaptar este patrón para que funcione con varios niveles de aplicación.
- Amazon RDS Custom está configurado con al menos 8 GB de espacio de intercambio.
- Una licencia de base de datos de Oracle Active Data Guard para convertir la réplica de lectura en modo de solo lectura y utilizarla para transferir las tareas de elaboración de informes al modo de espera. Para obtener más información, consulte la Lista de precios de Oracle Technology Commercial.

Limitaciones

- Limitaciones generales y configuraciones no compatibles con RDS Custom para Oracle
- Limitaciones asociadas a las Réplicas de lectura de Amazon RDS Custom para Oracle

Versiones de producto

- Para ver las versiones de la base de datos de Oracle compatibles con Amazon RDS Custom, consulte RDS Custom para Oracle.
- Para ver las clases de instancias de la base de datos de Oracle compatibles con Amazon RDS Custom, consulte Compatibilidad de clases de instancias de base de datos con RDS Custom para Oracle.

Arquitectura

Pila de tecnología de destino

- Amazon RDS Custom para Oracle
- AWS Secrets Manager
- Oracle Active Data Guard
- PeopleSoft Aplicación Oracle

Arquitectura de destino

El siguiente diagrama muestra una instancia de base de datos de Amazon RDS Custom y una réplica de lectura de Amazon RDS Custom. La réplica de lectura utiliza Oracle Active Data Guard para replicar en otra zona de disponibilidad. También puede usar la réplica de lectura para descargar el tráfico de lectura en la base de datos principal y para generar informes.

Para ver una arquitectura representativa con Oracle PeopleSoft en AWS, consulte Configurar una PeopleSoft arquitectura de alta disponibilidad en AWS.

Tools (Herramientas)

Servicios de AWS

- Amazon RDS Custom para Oracle es un servicio de base de datos administrado para aplicaciones heredadas, personalizadas y empaquetadas que requieren acceso al sistema operativo y al entorno de base de datos subyacentes.
- AWS Secrets Manager le permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación. En este patrón, recupera las contraseñas de usuario de la base de datos de Secrets Manager para `RDS_DATAGUARD` con el nombre secreto `do-not-delete-rds-custom-+<<RDS Resource ID>>+-dg`.

Otras herramientas

- Oracle Data Guard le ayuda a crear, mantener, gestionar y supervisar las bases de datos en espera.

Prácticas recomendadas

Para lograr un objetivo de cero pérdidas de datos (RPO=0), utilice el modo de protección Data Guard `MaxAvailability`, con la configuración `SYNC+NOAFFIRM` redo transport para mejorar el rendimiento. Para obtener más información sobre cómo seleccionar el modo de protección de la base de datos, consulte la sección Información adicional.

Epics

Crear la réplica de lectura

Tarea	Descripción	Habilidades requeridas
Crear la réplica de lectura.	Para crear una réplica de lectura de la instancia de base de datos de Amazon RDS Custom, siga las instrucciones de la documentación de Amazon RDS y utilice la instancia de base de datos de Amazon RDS Custom que creó (consulte la sección Requisitos previos) como base de datos de origen. De forma predeterminada, la réplica de lectura de Amazon RDS Custom se crea como una copia física en espera y está en el estado montado. Esto tiene la intención de garantizar el cumplimiento de la licencia de Oracle Active Data Guard. Este patrón incluye código para configurar una base de datos de contenedores multiusuario (CDB) o una instancia que no sea de CDB.	Administrador de base de datos

Cambie el modo de protección de Oracle Data Guard a MaxAvailability

Tarea	Descripción	Habilidades requeridas
Acceda a la configuración del agente Data Guard en la base de datos principal.	En este ejemplo, la réplica de lectura de Amazon RDS Custom es `RDS_CUSTOM_ORCL_D` para la instancia que no es de CDB y `RDS_CUSTOM_RDSCDB_B` para la instancia de CDB. Las bases de datos que no son de CDB son `orcl_a` (principal) y `orcl_d` (en espera). Los nombres de las bases de datos para CDB son `rdscdb_a` (principal) y `rdscdb_b` (en espera). Puede conectarse a la réplica de lectura personalizada de RDS directamente o a través de la base de datos principal. Puede encontrar el nombre del servicio de red de su base de datos en el archivo `tnsnames.ora` ubicado en el directorio `$ORACLE_HOME/network/admin`. RDS Custom para Oracle rellena automáticamente estas entradas para su base de datos principal y sus réplicas de lectura. La contraseña del usuario `RDS_DATAGUARD` se	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	guarda en AWS Secrets Manager, con el nombre secreto `do-not-delete-rds-custom-+<<RDS Resource ID>>+-dg`. Para obtener más información sobre cómo conectarse a una instancia personalizada de RDS mediante la clave SSH (Secure Shell) recuperada de Secrets Manager, consulte Conexión a una instancia de base de datos personalizada de RDS mediante SSH.
	
	Para acceder a la configuración del agente de Oracle Data Guard a través de la línea de comandos de Data Guard (`dgmgrl`), utilice el siguiente código.
	
	No CDB
	
	`$ dgmgrl RDS_DATAGUARD@RDS_CUSTOM_ORCL_D`
	`DGMGRL for Linux: Release 19.0.0.0.0 - Production on Fri Sep 30 22:44:49 2022`
	`Version 19.10.0.0.0`
	`Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.`	

Tarea	Descripción	Habilidades requeridas
	Welcome to DGMGRL, type "help" for informati on. Password: Connected to "ORCL_D" Connected as SYSDG. DGMGRL> DGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Average Apply Rate: 11.00 KByte/s Instance(s): ORCL SUCCESS DGMGRL> CDB -bash-4.2$ dgmgrl C##RDS_DATAGUARD@R DS_CUSTOM_RDSCDB_B DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 11 20:24:11 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.	

Tarea	Descripción	Habilidades requeridas
	Welcome to DGMGRL, type "help" for information. Password: Connected to "RDSCDB_B" Connected as SYSDG. DGMGRL> DGMGRL> show database rdscdb_b Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 2.00 KByte/s Real Time Query: OFF Instance(s): RDSCDB Database Status: SUCCESS DGMGRL>	

Tarea	Descripción	Habilidades requeridas

Cambie la configuración de transporte de registros conectándose a DGMGRL desde el nodo principal.	Cambie el modo de transporte de registros a `FastSync`, correspondiente a la configuración redo transport `SYNC +NOAFFIRM` . Para asegurarse de que tiene una configuración válida después del cambio de rol, cámbiela tanto para la base de datos principal como para la base de datos en espera.
	
	No CDB
	
	`DGMGRL>`
	`DGMGRL> edit database orcl_d set property logxptmode=fastsync;`
	`Property "logxptmode" updated`
	`DGMGRL> show database orcl_d LogXptMode;`
	`LogXptMode = 'fastsync'`
	`DGMGRL> edit database orcl_a set property logxptmode=fastsync;`
	`Property "logxptmode" updated`
	`DGMGRL> show database orcl_a logxptmode;`
	`LogXptMode = 'fastsync'`
	`DGMGRL>`
	
	CDB
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`DGMGRL> edit database rdscdb_b set property logxptmode=fastsync;DGMGRL> edit database rdscdb_b set property logxptmode=fastsync;Property "logxptmode" updated DGMGRL> show database rdscdb_b LogXptMode; LogXptMode = 'fastsync' DGMGRL> edit database rdscdb_a set property logxptmode=fastsync;Property "logxptmode" updated DGMGRL> show database rdscdb_a logxptmode; LogXptMode = 'fastsync' DGMGRL>`	

Tarea	Descripción	Habilidades requeridas

Cambie el modo de protección a MaxAvailability.	Cambie el modo de protección a `MaxAvailability` mediante una conexión a DGMGRL desde el nodo principal.
	
	No CDB
	
	`DGMGRL> edit configuration set protection mode as maxavailability;`
	`Succeeded.`
	`DGMGRL> show configuration;`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`orcl_a - Primary database`
	`orcl_d - Physical standby database`
	`Fast-Start Failover: Disabled`
	`Configuration Status:`
	`SUCCESS (status updated 38 seconds ago)`
	`DGMGRL>`
	
	CDB
	
	`DGMGRL> show configuration`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	rdscdb_a - Primary database rdscdb_b - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 57 seconds ago) DGMGRL>	

Cambie el estado de la réplica de montada a de solo lectura y habilite redo apply.

Tarea	Descripción	Habilidades requeridas
Detenga redo apply para la base de datos en espera.	La réplica de lectura se crea en modo MOUNT de forma predeterminada. Para abrirla en modo de solo lectura, primero debe desactivar redo apply conectándose a DGMGRL desde el nodo principal o en espera. No CDB DGMGRL> show database orcl_dDGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago)	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Average Apply Rate: 11.00 KByte/s Real Time Query: OFF Instance(s): ORCL Database Status: SUCCESS DGMGRL> edit database orcl_d set state=app ly-off; Succeeded. DGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY- OFF Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 42 seconds (computed 1 second ago) Average Apply Rate: (unknown) Real Time Query: OFF Instance(s): ORCL Database Status: SUCCESS DGMGRL> CDB DGMGRL> show configura tionDGMGRL> show configuration Configuration - rds_dg Protection Mode: MaxAvailability Members:	

Tarea	Descripción	Habilidades requeridas
	rdscdb_a - Primary database rdscdb_b - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 57 seconds ago) DGMGRL> show database rdscdb_b; Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 2.00 KByte/s Real Time Query: OFF Instance(s): RDSCDB Database Status: SUCCESS DGMGRL> edit database rdscdb_b set state=apply-off; Succeeded. DGMGRL> show database rdscdb_b; Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-OFF	

Tarea	Descripción	Habilidades requeridas

	<pre> Transport Lag:
	0 seconds (computed 1
	second ago)
	  Apply Lag:
	0 seconds (computed 1
	second ago)
	  Average Apply Rate:
	(unknown)
	  Real Time Query:
	OFF
	  Instance(s):
	    RDSCDB
	Database Status:
	SUCCESS</pre>	

Tarea	Descripción	Habilidades requeridas
Abra la instancia de réplica de lectura en modo de solo lectura.	Conéctese a la base de datos en espera mediante la entrada TNS y ábrala en modo de solo lectura conectándose a ella desde el nodo principal o en espera. No CDB `$ sqlplus RDS_DATAG UARD@RDS_CUSTOM_OR CL_D as sysdg -bash-4.2$ sqlplus RDS_DATAGUARD@RDS_ CUSTOM_ORCL_D as sysdg SQL*Plus: Release 19.0.0.0.0 - Productio n on Fri Sep 30 23:00:14 2022 Version 19.10.0.0.0 Copyright (c) 1982, 2020, Oracle. All rights reserved. Enter password: Last Successful login time: Fri Sep 30 2022 22:48:27 +00:00 Connected to: Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production Version 19.10.0.0.0 SQL> select open_mode from v$database; OPEN_MODE -------------------- MOUNTED SQL> alter database open read only;`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Database altered. SQL> select open_mode from v$database; OPEN_MODE -------------------- READ ONLY SQL> CDB -bash-4.2$ sqlplus C##RDS_DATAGUARD@R DS_CUSTOM_RDSCDB_B as sysdg SQL*Plus: Release 19.0.0.0.0 - Productio n on Wed Jan 11 21:14:07 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2022, Oracle. All rights reserved. Enter password: Last Successful login time: Wed Jan 11 2023 21:12:05 +00:00 Connected to: Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production Version 19.16.0.0.0 SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- --------- ----------- RDSCDB MOUNTED SQL> alter database open read only; Database altered.	

Tarea	Descripción	Habilidades requeridas
	SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- --------- ----------- RDSCDB READ ONLY SQL>	

Tarea	Descripción	Habilidades requeridas
Active redo apply en la instancia de réplica de lectura.	Active redo apply en la instancia de réplica de lectura mediante DGMGR L desde el nodo principal o en espera. No CDB `$ dgmgrl RDS_DATAG UARD@RDS_CUSTOM_OR CL_D DGMGRL for Linux: Release 19.0.0.0.0 - Production on Fri Sep 30 23:02:16 2022 Version 19.10.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for informati on. Password: Connected to "ORCL_D" Connected as SYSDG. DGMGRL> edit database orcl_d set state=apply-on; DGMGRL> edit database orcl_d set state=app ly-on; Succeeded. DGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY-ON`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Transport Lag: 0 seconds (computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Average Apply Rate: 496.00 KByte/s Real Time Query: ON Instance(s): ORCL Database Status: SUCCESS DGMGRL> CDB -bash-4.2$ dgmgrl C##RDS_DATAGUARD@RDS_CUSTOM_RDSCDB_B -bash-4.2$ dgmgrl C##RDS_DATAGUARD@RDS_CUSTOM_RDSCDB_B DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 11 21:21:11 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for information. Password: Connected to "RDSCDB_B" Connected as SYSDG.	

Tarea	Descripción	Habilidades requeridas
	DGMGRL> edit database rdscdb_b set state=apply-on; Succeeded. DGMGRL> show database rdscdb_b Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Average Apply Rate: 35.00 KByte/s Real Time Query: ON Instance(s): RDSCDB Database Status: SUCCESS DGMGRL> show database rdscdb_b Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 16.00 KByte/s Real Time Query: ON Instance(s): RDSCDB	

Tarea	Descripción	Habilidades requeridas

	`Database Status:`
	`SUCCESS`
	`DGMGRL>`	

Recursos relacionados

- Configuración de Amazon RDS como una PeopleSoft base de datos de Oracle (documento técnico de AWS)
- Guía de agente de Oracle Data Guard (documentación de referencia de Oracle)
- Oracle Data Guard Concepts and Administration(documentación de referencia de Oracle)

Información adicional

Seleccionar el modo de protección de su base de datos

Oracle Data Guard ofrece tres modos de protección para configurar su entorno de Data Guard en función de sus requisitos de disponibilidad, protección y rendimiento. Estos tres modos se resumen en la tabla siguiente:

Modo de protección	Configuración redo transport	Description (Descripción)
MÁXIMO RENDIMIENTO	ASYNC	En el caso de las transacciones que se realizan en la base de datos principal, los datos de redo se transmiten de forma asíncrona y se escriben en el redo log de la base de datos en espera. Por lo tanto, el impacto en el rendimiento es mínimo. `MaxPerformance` no puede proporcionar RPO=0 debido al envío asincrónico de registros.

MÁXIMA PROTECCIÓN	SYNC+AFFIRM	En el caso de las transacciones de la base de datos principal, los datos de redo se transmiten de forma sincrónica y se escriben en el disco de la base de datos en espera redo log antes de que se confirme la transacción. Si la base de datos en espera deja de estar disponible, la base de datos principal se cierra automáticamente para garantizar la protección de las transacciones.
MÁXIMA DISPONIBILIDAD	SYNC+AFFIRM	Es similar al modo `MaxProtection` , excepto cuando no se recibe ningún acuse de recibo de la base de datos en espera. En ese caso, funciona como si estuviera en modo `MaxPerformance` para preservar la disponibilidad de la base de datos principal hasta que pueda volver a escribir su redo stream en una base de datos en espera sincronizada.

SYNC+NOAFFIRM	En el caso de las transacciones de la base de datos principal, el redo se transmite de forma sincrónica a la base de datos en espera, y la principal solo espera una confirmación de acuse de recibo del redo en la base de datos en espera, no a que se haya escrito en el disco en espera. Este modo, también conocido como `FastSync`, puede proporcionar una ventaja en el rendimiento a costa de la posible exposición a la pérdida de datos en un caso especial de varios fallos simultáneos.

Las réplicas de lectura en RDS Custom para Oracle se crean con el modo de protección del máximo rendimiento, que también es el modo de protección predeterminado de Oracle Data Guard. El modo de rendimiento máximo proporciona el menor impacto en el rendimiento de la base de datos principal, lo que puede ayudarle a cumplir el requisito del objetivo de punto de recuperación (RPO) medido en segundos.

Para lograr el objetivo de cero pérdidas de datos (RPO=0), puede personalizar el modo de protección de Oracle Data Guard a `MaxAvailability` con la configuración `SYNC+NOAFFIRM` redo transport para mejorar el rendimiento. Como las confirmaciones en la base de datos principal solo se reconocen después de que los vectores redo correspondientes se hayan transmitido correctamente a la base de datos en espera, la latencia de la red entre la instancia principal y la réplica puede ser crucial para las cargas de trabajo sensibles a las confirmaciones. Recomendamos realizar pruebas de carga de la carga de trabajo para evaluar el impacto en el rendimiento cuando la réplica de lectura esté personalizada para ejecutarse en modo `MaxAvailability`.

La implementación de la réplica de lectura en la misma zona de disponibilidad que la base de datos principal proporciona una latencia de red más baja en comparación con la implementación de la

réplica de lectura en una zona de disponibilidad diferente. Sin embargo, es posible que implementar las réplicas principal y de lectura en la misma zona de disponibilidad no cumpla con los requisitos de alta disponibilidad porque, en el improbable caso de que la zona de disponibilidad no esté disponible, tanto la instancia principal como la instancia de réplica de lectura se ven afectadas.

Análisis de las dependencias de los objetos para realizar migraciones parciales de bases de datos de Oracle a PostgreSQL

anuradha chintha, Amazon Web Services

Resumen

Este patrón describe la importancia de identificar y administrar de forma sistemática las dependencias del sistema al migrar una base de datos de Oracle a Amazon Relational Database Service (Amazon RDS) o Amazon Aurora PostgreSQL. En una migración parcial, solo se migra un subconjunto de objetos de base de datos y datos de la base de datos original, mientras que la base de datos de origen sigue funcionando y sirviendo a aplicaciones que dependen de componentes no migrados

Debe identificar y analizar el alcance de la migración cuando gestione bases de datos a gran escala que tengan aplicaciones con acoplamiento ajustado con dependencias en las fases anteriores y posteriores. Para iniciar una migración parcial, identifique los objetos que están en el alcance, incluidas las tablas, los desencadenadores, las vistas, los procedimientos almacenados, las funciones y los paquetes. El proceso de identificación del alcance sigue un enfoque integral:

- Los objetos que están en el alcance de primer nivel se identifican mediante referencias directas en el código de la aplicación y en los trabajos críticos específicos de los módulos.
- Los objetos de segundo nivel se obtienen mediante un análisis de dependencia exhaustivo.

Cuando comprenda cómo interactúan las diferentes partes del sistema, podrá planificar mejor el orden correcto para mover los componentes de la base de datos y reducir el riesgo de que se produzcan errores en la migración. En la siguiente tabla se enumeran los distintos tipos de análisis de las dependencias.

Tipo de análisis	Áreas de interés	Finalidad
Dependencias de objetos	• Tablas • Vistas • Procedimientos almacenados • Funciones	Identifica las relaciones entre los objetos de la base de datos y sus estructuras jerárquicas

	• Desencadenadores	
Dependencias de segmentos	• Relaciones de claves externas • Relaciones de claves principales • Referencias entre esquemas	Mapea las relaciones de los datos y mantiene la integridad de las referencias
Dependencias de seguridad	• Permisos de usuario • Jerarquías de roles • Privilegios de objeto	Garantiza el control de acceso, la migración y el mantenimiento de la seguridad adecuados
Patrones de acceso	• Operaciones de lectura • Operaciones de escritura	Determina los patrones de interacción de las bases de datos

Para mantener la coherencia entre los sistemas de origen y destino, establezca mecanismos de sincronización de datos durante el periodo de transición. También debe modificar el código y las funciones de la aplicación para gestionar la distribución de datos en las bases de datos de Oracle de origen y las bases de datos de PostgreSQL de destino.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Una base de datos de Oracle (origen)
- Una base de datos de Amazon RDS o Amazon Aurora PostgreSQL (destino)

Versiones de producto

- Oracle 19c o posterior
- PostgreSQL 16 o posterior

Arquitectura

Pila de tecnología de origen

- Oracle 19c o posterior

Pila de tecnología de destino

- Amazon RDS o Amazon Aurora PostgreSQL

Arquitectura de destino

En el siguiente diagrama se muestra el proceso de migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle, que incluye lo siguiente:

- Identificación de las dependencias de la base de datos
- Migración del código y los objetos de la base de datos mediante AWS Schema Conversion Tool ()AWS SCT
- Migración de datos mediante AWS Database Migration Service ()AWS DMS
- Replicar los cambios en curso mediante la captura de datos sobre cambios (CDC) mediante AWS DMS

Para obtener más información, consulte Integración AWS Database Migration Service con AWS Schema Conversion Tool en la AWS documentación.

Tools (Herramientas)

Servicios de AWS

- Amazon Relational Database Service (Amazon RDS) para Oracle lo ayuda a configurar, utilizar y escalar una base de datos relacional de Oracle en la Nube de AWS.
- Amazon Aurora es un motor de base de datos relacional completamente administrado diseñado para la nube y compatible con MySQL y PostgreSQL.
- AWS Schema Conversion Tool (AWS SCT) admite migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayoría del código personalizado a un formato compatible con la base de datos de destino.

- AWS Database Migration Service (AWS DMS) le ayuda a migrar los almacenes de datos a una combinación de configuraciones locales y en la nube Nube de AWS o entre ellas.

Otros servicios

- Oracle SQL Developer es un entorno de desarrollo integrado que simplifica el desarrollo y la administración de bases de datos de Oracle, tanto en implementaciones tradicionales como en implementaciones basadas en la nube. Para este patrón, puede usar SQL*Plus.

Prácticas recomendadas

Para ver prácticas recomendadas sobre el aprovisionamiento y migración de bases de datos de Oracle, consulte Best practices for migrating to Amazon RDS for Oracle.

Epics

Identificación de las dependencias de objetos

Tarea	Descripción	Habilidades requeridas
Cree una tabla de objetos.	Identifique los objetos que son esenciales para la funcionalidad de la aplicación y cree una tabla con el nombre `DEPENDENT_ANALYSIS_BASELINE`. Agregue registros para cada objeto a la tabla. Para obtener ejemplos, consulte la sección Información adicional.	Ingeniero de datos, Administrador de base de datos
Cree un procedimiento de la base de datos	Cree un procedimiento almacenado llamado `sp_object_dependency_analysis` para analizar las dependencias de los objetos en ambas direcciones (hacia adelante	Ingeniero de datos, Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	y hacia atrás) mediante los datos de la tabla `DBA_DEPENDENCIES` . Para obtener ejemplos, consulte la sección Información adicional.	
Ejecute el procedimiento.	Ejecute los scripts en cada nivel sucesivo hasta que no se encuentren nuevas dependencias entre objetos. Todas las dependencias y niveles se almacenan en la tabla `DEPENDENT_ANALYSIS_BASELINE` .	Administrador de base de datos, ingeniero de datos

Creación de un procedimiento para las dependencias a nivel de segmento

Tarea	Descripción	Habilidades requeridas
Cree una tabla de dependencias.	Cree una tabla de dependencias a nivel de segmento denominada `REFERENTIAL_ANALYSIS_BASELINE` . Cuando se detecten todas las dependencias a nivel de objeto, compruebe las tablas principales de `DEPENDENT_ANALYSIS_BASELINE` consultando la tabla `DBA_CONSTRAINT` . Excluya las dependencias en las que otras tablas hacen referencia a las tablas de referencia. La reposición	Ingeniero de datos, Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	gestiona estas relaciones. A continuación se muestra un ejemplo de script: `CREATE TABLE REFERENTIAL_ANALYSIS_BASELINE (CHILD_OWNER VARCHAR2(50 BYTE), CHILD_NAME VARCHAR2(100 BYTE), PARENT_OWNER VARCHAR2(50 BYTE), PARENT_NAME VARCHAR2(50 BYTE), REFERENCE_PATH VARCHAR2(1000 BYTE));`	
Cree un procedimiento de la base de datos	Cree un procedimiento denominado `SP_OBJECT_REFERENTIAL_ANALYSIS` y genere un análisis referencial para todos los objetos identificados. Para obtener ejemplos, consulte la sección Información adicional.	Ingeniero de datos, Administrador de base de datos
Ejecute el procedimiento.	Ejecute el procedimiento para obtener las dependencias referenciales. Genere detalles del objeto de análisis referencial en `REFERENTIAL_ANALYSIS_BASELINE`.	Ingeniero de datos, Administrador de base de datos

Identificación de objetos que leen y escriben

Tarea	Descripción	Habilidades requeridas

Cree tablas para los objetos de lectura y escritura.	Utilice el siguiente script para crear una tabla de objetos de lectura denominada `TABLE_READ_OBJECT_DETAILS` y una tabla de objetos de escritura denominada `TABLE_WRITE_OBJECT_DETAILS` :
	
	`CREATE TABLE TABLE_READ_OBJECT_DETAILS (OWNER VARCHAR2(50 BYTE), TAB_NAME VARCHAR2(50 BYTE), READER_OWNER VARCHAR2(50 BYTE), READER_NAME VARCHAR2(50 BYTE), READER_TYPE VARCHAR2(50 BYTE));`
	
	`CREATE TABLE TABLE_WRITE_OBJECT_DETAILS (TABLE_NAME VARCHAR2(100 BYTE), WRITEOBJ_OWNER VARCHAR2(100 BYTE), WRITEOBJ_NAME VARCHAR2(100 BYTE), WRITEOBJ_TYPE VARCHAR2(100 BYTE), LINE VARCHAR2(100 BYTE), TEXT VARCHAR2(4000 BYTE),`
		Ingeniero de datos, Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`OWNER VARCHAR2(50 BYTE));`	
Cree un procedimiento para el análisis.	Cree los procedimientos `SP_READER_OBJECTS_ANALYSIS` y `SP_WRITER_OBJECTS_ANALYSIS` para analizar los objetos de lectura y escritura, respectivamente. Estos procedimientos utilizan la coincidencia de patrones para buscar objetos relacionados. Para ver un ejemplo, consulte la sección Información adicional.	Ingeniero de datos, Administrador de base de datos
Ejecute los procedimientos.	Ejecute estos procedimientos para identificar los objetos dependientes.	Administrador de base de datos, ingeniero de datos

Revisión de privilegios de base de datos

Tarea	Descripción	Habilidades requeridas
Cree una tabla para revisar los privilegios.	Cree una tabla para analizar los privilegios denominada `OBJECT_PRIVS_ANALYSIS` . Para capturar de forma recursiva los privilegios de los objetos de la tabla `DEPENDENT_ANALYSIS_BASELINE` , utilice el siguiente script:	Ingeniero de datos, Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`CREATE TABLE OBJECT_PRIVS_ANALYSIS (OWNER VARCHAR2(50 BYTE), OBJECT_NAME VARCHAR2(50 BYTE), USER_NAME VARCHAR2(50 BYTE), PRIVS VARCHAR2(50 BYTE));`	
Cree un procedimiento para revisar los privilegios.	Cree un procedimiento denominado `SP_OBJECT_PRIVS_ANALYSIS` . Genere un análisis de privilegios para los objetos identificados. Para obtener ejemplos, consulte la sección Información adicional.	Administrador de base de datos, ingeniero de datos
Ejecute el procedimiento.	Ejecute el procedimiento para capturarlos en la tabla `OBJECT_PRIVS_ANALYSIS` .	Administrador de base de datos, ingeniero de datos

Resolución de problemas

Problema	Solución
No se puede acceder a las tablas del diccionario	Asegúrese de que el usuario que creó los objetos de análisis pueda acceder a las tablas de DBA.

Recursos relacionados

Documentación de AWS

- Documentación de Amazon RDS y Aurora
- Oracle database 19c to Amazon Aurora PostgreSQL migration playbook
- ¿Qué es? AWS Database Migration Service
- What is the AWS Schema Conversion Tool?

Otra documentación

- Oracle database objects

Información adicional

Script para **DEPENDENT_ANALYSIS_BASELINE**

```
CREATE TABLE DEPENDENT_ANALYSIS_BASELINE
(OWNER VARCHAR2(128 BYTE) NOT NULL ENABLE,
OBJECT_NAME VARCHAR2(128 BYTE) NOT NULL ENABLE,
OBJECT_TYPE VARCHAR2(20 BYTE),
DEPEDNCY_LEVEL NUMBER,
PROJECT_NEED VARCHAR2(20 BYTE),
CATAGORY VARCHAR2(4000 BYTE),
COMMENTS VARCHAR2(4000 BYTE),
CATAGORY1 CLOB,
COMMENTS1 CLOB,
CUSTOMER_COMMENTS VARCHAR2(1000 BYTE),
BACKFILL_TO_GUS VARCHAR2(1000 BYTE),
BACKFILL_NEAR_REAL_TIME_OR_BATCH VARCHAR2(1000 BYTE),
PK_EXISTS VARCHAR2(3 BYTE),
UI_EXISTS VARCHAR2(3 BYTE),
LOB_EXISTS VARCHAR2(3 BYTE),
MASTER_LINK VARCHAR2(100 BYTE),
CONSTRAINT PK_DEPENDENT_ANALYSIS_BASELINE PRIMARY KEY (OWNER,OBJECT_NAME,OBJECT_TYPE));
```

Procedimientos para **SP_WRITER_OBJECTS_ANALYSIS**

```
CREATE OR REPLACE PROCEDURE SP_WRITER_OBJECTS_ANALYSIS IS
BEGIN
```

```
  EXECUTE IMMEDIATE 'TRUNCATE TABLE TABLE_WRITE_OBJECT_DETAILS';
  FOR I IN (SELECT OWNER, OBJECT_NAME FROM DEPENDENT_ANALYSIS_BASELINE WHERE
 OBJECT_TYPE = 'TABLE')
  LOOP
    INSERT INTO TABLE_WRITE_OBJECT_DETAILS(OWNER, TABLE_NAME, WRITEOBJ_OWNER,
 WRITEOBJ_NAME, WRITEOBJ_TYPE, LINE, TEXT)
    SELECT DISTINCT I.OWNER, I.OBJECT_NAME, OWNER WRITEOBJ_OWNER, NAME, TYPE, LINE,
 TRIM(TEXT)
    FROM DBA_SOURCE
    WHERE UPPER(TEXT) LIKE '%' || I.OBJECT_NAME || '%'
      AND (UPPER(TEXT) LIKE '%INSERT%' || I.OBJECT_NAME || '%'
        OR UPPER(TEXT) LIKE '%UPDATE%' || I.OBJECT_NAME || '%'
        OR UPPER(TEXT) LIKE '%DELETE%' || I.OBJECT_NAME || '%'
        OR UPPER(TEXT) LIKE '%UPSERT%' || I.OBJECT_NAME || '%'
        OR UPPER(TEXT) LIKE '%MERGE%' || I.OBJECT_NAME || '%')
      AND UPPER(TEXT) NOT LIKE '%PROCEDURE%'
      AND UPPER(TEXT) NOT LIKE 'PROCEDURE%'
      AND UPPER(TEXT) NOT LIKE '%FUNCTION%'
      AND UPPER(TEXT) NOT LIKE 'FUNCTION%'
      AND UPPER(TEXT) NOT LIKE '%TRIGGER%'
      AND UPPER(TEXT) NOT LIKE 'TRIGGER%'
      AND UPPER(TRIM(TEXT)) NOT LIKE '%AFTER UPDATE%'
      AND UPPER(TRIM(TEXT)) NOT LIKE 'BEFORE UPDATE%'
      AND UPPER(TRIM(TEXT)) NOT LIKE 'BEFORE INSERT%'
      AND UPPER(TRIM(TEXT)) NOT LIKE 'AFTER INSERT%'
      AND UPPER(TRIM(TEXT)) NOT LIKE 'BEFORE DELETE%'
      AND UPPER(TRIM(TEXT)) NOT LIKE 'AFTER DELETE%'
      AND UPPER(TRIM(TEXT)) NOT LIKE '%GGLOGADM.GG_LOG_ERROR%'
      AND (TRIM(TEXT) NOT LIKE '/*%' AND TRIM(TEXT) NOT LIKE '--%' )
      AND (OWNER, NAME, TYPE) IN (SELECT OWNER, NAME, TYPE FROM DBA_DEPENDENCIES WHERE
 REFERENCED_NAME = I.OBJECT_NAME);
  END LOOP;
END;
```

Script para **SP_READER_OBJECTS_ANALYSIS**

```
CREATE OR REPLACE PROCEDURE SP_READER_OBJECTS_ANALYSIS IS
BEGIN
  EXECUTE IMMEDIATE 'TRUNCATE TABLE TABLE_READ_OBJECT_DETAILS';
  FOR I IN (SELECT OWNER, OBJECT_NAME FROM DEPENDENT_ANALYSIS_BASELINE WHERE
 OBJECT_TYPE = 'TABLE')
  LOOP
    INSERT INTO TABLE_READ_OBJECT_DETAILS
```

```
    SELECT DISTINCT i.owner, i.object_name, owner, name, type
    FROM dba_dependencies
    WHERE referenced_name = I.OBJECT_NAME
    AND referenced_type = 'TABLE'
    AND type NOT IN ('SYNONYM', 'MATERIALIZED VIEW', 'VIEW')
    AND (owner, name, type) NOT IN (
      SELECT DISTINCT owner, trigger_name, 'TRIGGER'
      FROM dba_triggers
      WHERE table_name = I.OBJECT_NAME
      AND table_owner = i.owner
      UNION ALL
      SELECT DISTINCT owner, name, type
      FROM dba_source
      WHERE upper(text) LIKE '%' || I.OBJECT_NAME || '%'
      AND (upper(text) LIKE '%INSERT %' || I.OBJECT_NAME || '%'
        OR upper(text) LIKE '%UPDATE% ' || I.OBJECT_NAME || '%'
        OR upper(text) LIKE '%DELETE %' || I.OBJECT_NAME || '%'
        OR upper(text) LIKE '%UPSERT %' || I.OBJECT_NAME || '%'
        OR upper(text) LIKE '%MERGE %' || I.OBJECT_NAME || '%')
      AND upper(text) NOT LIKE '%PROCEDURE %'
      AND upper(text) NOT LIKE 'PROCEDURE %'
      AND upper(text) NOT LIKE '%FUNCTION %'
      AND upper(text) NOT LIKE 'FUNCTION %'
      AND upper(text) NOT LIKE '%TRIGGER %'
      AND upper(text) NOT LIKE 'TRIGGER %'
      AND upper(trim(text)) NOT LIKE 'BEFORE INSERT %'
      AND upper(trim(text)) NOT LIKE 'BEFORE UPDATE %'
      AND upper(trim(text)) NOT LIKE 'BEFORE DELETE %'
      AND upper(trim(text)) NOT LIKE 'AFTER INSERT %'
      AND upper(trim(text)) NOT LIKE 'AFTER UPDATE %'
      AND upper(trim(text)) NOT LIKE 'AFTER DELETE %'
      AND (trim(text) NOT LIKE '/*%' AND trim(text) NOT LIKE '--%'));
  END LOOP;
END;
```

Script para **SP_OBJECT_REFERENTIAL_ANALYSIS**

```
CREATE OR REPLACE PROCEDURE SP_OBJECT_REFERENTIAL_ANALYSIS IS
BEGIN
  EXECUTE IMMEDIATE 'TRUNCATE TABLE REFERENTIAL_ANALYSIS_BASELINE';
  INSERT INTO REFERENTIAL_ANALYSIS_BASELINE
  WITH rel AS (
    SELECT DISTINCT c.owner, c.table_name, c.r_owner r_owner,
```

```
      (SELECT table_name FROM dba_constraints
       WHERE constraint_name = c.r_constraint_name
       AND owner = c.r_owner) r_table_name
    FROM dba_constraints c
    WHERE constraint_type = 'R'
    AND c.owner NOT IN (SELECT username FROM dba_users WHERE oracle_maintained = 'Y')
    AND c.r_owner NOT IN (SELECT username FROM dba_users WHERE oracle_maintained =
 'Y')),
  tab_list AS (
    SELECT OWNER, object_name
    FROM DEPENDENT_ANALYSIS_BASELINE
    WHERE UPPER(OBJECT_TYPE) = 'TABLE')
  SELECT DISTINCT owner child_owner, table_name child, r_owner parent_owner,
    r_table_name parent, SYS_CONNECT_BY_PATH(r_table_name, ' -> ') || ' -> ' ||
 table_name PATH
  FROM rel
  START WITH (r_owner, r_table_name) IN (SELECT * FROM tab_list)
  CONNECT BY NOCYCLE (r_owner, r_table_name) = ((PRIOR owner, PRIOR table_name))
  UNION
  SELECT DISTINCT owner child_owner, table_name child, r_owner parent_owner,
    r_table_name parent, SYS_CONNECT_BY_PATH(table_name, ' -> ') || ' -> ' ||
 r_table_name PATH
  FROM rel
  START WITH (owner, table_name) IN (SELECT * FROM tab_list)
  CONNECT BY NOCYCLE (owner, table_name) = ((PRIOR r_owner, PRIOR r_table_name));
END;
```

Script para **SP_OBJECT_PRIVS_ANALYSIS**

```
CREATE OR REPLACE PROCEDURE SP_OBJECT_PRIVS_ANALYSIS IS
  V_SQL VARCHAR2(4000);
  V_CNT NUMBER;
BEGIN
  V_SQL := 'TRUNCATE TABLE OBJECT_PRIVS_ANALYSIS';
  EXECUTE IMMEDIATE V_SQL;
  FOR I IN (SELECT OWNER, OBJECT_NAME FROM DEPENDENT_ANALYSIS_BASELINE WHERE
 OBJECT_TYPE = 'TABLE')
  LOOP
    INSERT INTO OBJECT_PRIVS_ANALYSIS(OWNER, OBJECT_NAME, USER_NAME, PRIVS)
    WITH obj_to_role AS (
      SELECT DISTINCT GRANTEE role_name,
        DECODE(privilege, 'SELECT', 'READ', 'REFERENCE', 'READ', 'INSERT', 'WRITE',
               'UPDATE', 'WRITE', 'DELETE', 'WRITE', privilege) privs
```

```
      FROM DBA_TAB_PRIVS t, DBA_ROLES r
      WHERE OWNER = I.OWNER
      AND TYPE = 'TABLE'
      AND TABLE_NAME = I.OBJECT_NAME
      AND t.GRANTEE = r.ROLE
      AND r.ROLE IN (SELECT ROLE FROM DBA_ROLES WHERE ORACLE_MAINTAINED = 'N')
    )
    SELECT I.OWNER, I.OBJECT_NAME, grantee, privs
    FROM (
      -- Recursively Role to User mapping with privilege
      SELECT DISTINCT grantee, privs
      FROM (SELECT rp.granted_role, rp.grantee, privs,
        (SELECT DECODE(COUNT(*), 0, 'ROLE', 'USER')
         FROM (SELECT 'User' FROM DBA_users WHERE username = rp.GRANTEE)) grantee_type
        FROM DBA_role_privs rp, obj_to_role r
        WHERE rp.granted_role = r.role_name
        AND grantee IN ((SELECT USERNAME FROM DBA_USERS WHERE ORACLE_MAINTAINED = 'N')
                        UNION (SELECT ROLE FROM DBA_ROLES WHERE ORACLE_MAINTAINED =
 'N'))
        AND granted_role IN (SELECT ROLE FROM DBA_ROLES WHERE ORACLE_MAINTAINED = 'N')
        START WITH granted_role IN (SELECT DISTINCT role_name FROM obj_to_role)
        CONNECT BY granted_role = PRIOR grantee)
      WHERE grantee_type = 'USER'
    )
    UNION
    (
      -- Direct Object grants to User
      SELECT I.OWNER, I.OBJECT_NAME, GRANTEE,
        DECODE(privilege, 'SELECT', 'READ', 'REFERENCE', 'READ', 'INSERT', 'WRITE',
               'UPDATE', 'WRITE', 'DELETE', 'WRITE', privilege) privs
      FROM DBA_TAB_PRIVS, DBA_USERS
      WHERE GRANTEE = USERNAME
      AND OWNER = I.OWNER
      AND TYPE = 'TABLE'
      AND TABLE_NAME = I.OBJECT_NAME
    )
    ORDER BY 2 DESC;
  END LOOP;
END;
```

Procedimientos para **SP_OBJECT_DEPENDENCY_ANALYSIS**

```
CREATE OR REPLACE PROCEDURE SP_OBJECT_DEPENDENCY_ANALYSIS (v_level NUMBER) IS
```

```
  TYPE typ IS RECORD (
    schema VARCHAR2(100),
    obj_type VARCHAR2(100),
    obj_name VARCHAR2(100),
    path VARCHAR2(5000)
  );
  TYPE array IS TABLE OF typ;
  l_data array;
  c SYS_REFCURSOR;
  l_errors NUMBER;
  l_errno NUMBER;
  l_msg VARCHAR2(4000);
  l_idx NUMBER;
  l_level NUMBER;
BEGIN
  l_level := v_level + 1;
  OPEN c FOR
    WITH obj_list AS (
      SELECT owner schema_name, object_type, object_name
      FROM DEPENDENT_ANALYSIS_BASELINE
      WHERE depedncy_level = v_level
    ),
    fw_dep_objects AS (
      SELECT level lvl, owner, name, type, referenced_owner, referenced_name,
        referenced_type, SYS_CONNECT_BY_PATH(name, ' -> ') || ' -> ' || referenced_name
 PATH
      FROM dba_dependencies
      START WITH (owner, CASE WHEN type = 'PACKAGE BODY' THEN 'PACKAGE' ELSE type END,
 name)
        IN (SELECT schema_name, object_type, object_name FROM obj_list)
      CONNECT BY NOCYCLE (owner, type, name) =
        ((PRIOR referenced_owner, PRIOR referenced_type, PRIOR referenced_name))
    ),
    bw_dep_objects AS (
      SELECT level lvl, owner, name, type, referenced_owner, referenced_name,
        referenced_type, SYS_CONNECT_BY_PATH(name, ' <- ') || ' <- ' || referenced_name
 PATH
      FROM dba_dependencies
      START WITH (referenced_owner, CASE WHEN referenced_type = 'PACKAGE BODY' THEN
 'PACKAGE'
        ELSE referenced_type END, referenced_name) IN (SELECT schema_name, object_type,
 object_name FROM obj_list)
      CONNECT BY NOCYCLE (referenced_owner, referenced_type, referenced_name) =
        ((PRIOR owner, PRIOR type, PRIOR name))
```

```
    )
    SELECT * FROM (
      (SELECT DISTINCT referenced_owner schema, referenced_type obj_type,
        referenced_name obj_name, path FROM fw_dep_objects)
      UNION
      (SELECT DISTINCT owner schema, type obj_type, name obj_name, path
       FROM bw_dep_objects)
    )
    WHERE schema IN (SELECT username FROM all_users WHERE oracle_maintained = 'N')
    ORDER BY obj_type;

  LOOP
    FETCH c BULK COLLECT INTO l_data LIMIT 100;
    BEGIN
      FORALL i IN 1..l_data.count SAVE EXCEPTIONS
        INSERT INTO DEPENDENT_ANALYSIS_BASELINE (
          owner, object_name, object_type, catagory, depedncy_level, project_need,
comments
        )
        VALUES (
          l_data(i).schema,
          l_data(i).obj_name,
          CASE WHEN l_data(i).obj_type = 'PACKAGE BODY' THEN 'PACKAGE' ELSE
l_data(i).obj_type END,
          'level ' || l_level || ' dependency',
          l_level,
          '',
          'from dependency proc' || l_data(i).path
        );
    EXCEPTION
      WHEN OTHERS THEN
        l_errors := sql%bulk_exceptions.count;
        FOR i IN 1..l_errors LOOP
          l_errno := sql%bulk_exceptions(i).error_code;
          l_msg := SQLERRM(-l_errno);
          l_idx := sql%bulk_exceptions(i).error_index;
          UPDATE DEPENDENT_ANALYSIS_BASELINE
          SET catagory1 = catagory1 || ', found in level' || l_level || ' dependent of
' || l_data(l_idx).path,
              comments1 = comments1 || ', from dependency proc exception ' ||
l_data(i).path
          WHERE owner = l_data(l_idx).schema
          AND object_name = l_data(l_idx).obj_name
          AND object_type = l_data(l_idx).obj_type;
```

```
        END LOOP;
    END;
    EXIT WHEN c%NOTFOUND;
  END LOOP;
  CLOSE c;
END;
```

Evaluar el rendimiento de las consultas para migrar bases de datos de SQL Server a MongoDB Atlas en AWS

Battulga Purevragchaa, Amazon Web Services

Krishnakumar Sathyanarayana PeerIslands , US Inc

Babu Srinivasan, MongoDB

Resumen

Este patrón proporciona una guía para cargar MongoDB con datos casi reales y evaluar el rendimiento de las consultas de MongoDB que sea lo más parecido posible al escenario de producción. La evaluación proporciona información para ayudar a planificar la migración a MongoDB desde una base de datos relacional. El patrón utiliza el generador de datos de prueba y el analizador PeerIslands de rendimiento para probar el rendimiento de las consultas.

Este patrón es particularmente útil para la migración de Microsoft SQL Server a MongoDB, ya que realizar transformaciones de esquemas y cargar datos de las instancias actuales de SQL Server a MongoDB puede resultar muy complejo. En lugar de esto, puede cargar datos prácticamente reales en MongoDB, conocer el rendimiento de MongoDB y ajustar el diseño del esquema antes de iniciar la migración propiamente dicha.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Familiaridad con MongoDB Atlas
- Esquema de MongoDB de destino
- Patrones típicos de consulta

Limitaciones

- Los tiempos de carga de datos y el rendimiento estarán limitados por el tamaño de la instancia del clúster de MongoDB. Se recomienda seleccionar instancias que estén recomendadas para uso en producción a fin de comprender el rendimiento en el mundo real.

- PeerIslands Actualmente, Test Data Generator y Performance Analyzer solo admiten consultas y cargas de datos en línea. Aún no se admite el procesamiento por lotes sin conexión (por ejemplo, cargar datos en MongoDB mediante conectores Spark).
- PeerIslands El generador de datos de prueba y el analizador de rendimiento admiten las relaciones de campo dentro de una colección. No admite relaciones entre colecciones.

Ediciones de producto

- Este patrón es compatible con MongoDB Atlas y MongoDB Enterprise Advanced.

Arquitectura

Pila de tecnología de destino

- MongoDB Atlas o MongoDB Enterprise Advanced

Arquitectura

PeerIslands El generador de datos de prueba y el analizador de rendimiento se crean con Java y Angular, y almacenan los datos generados en Amazon Elastic Block Store (Amazon EBS). La herramienta consta de dos flujos de trabajo: la generación de datos de prueba y las pruebas de rendimiento.

- En la generación de datos de prueba, se crea una plantilla, que es la representación en JSON del modelo de datos que se debe generar. Después de crear la plantilla, se pueden generar los datos en una colección de destino, tal y como se define en la configuración de generación de carga.
- En las pruebas de rendimiento, se crea un perfil. Un perfil es un escenario de prueba en varias etapas en el que se pueden configurar las operaciones de creación, lectura, actualización y eliminación (CRUD), los procesos de agregación, la ponderación de cada operación y la duración de cada etapa. Tras crear el perfil, puede realizar pruebas de rendimiento en la base de datos de destino, en función de la configuración.

PeerIslands El generador de datos de prueba y el analizador de rendimiento almacenan sus datos en Amazon EBS, por lo que puede conectar Amazon EBS a MongoDB mediante cualquier mecanismo de conexión compatible con MongoDB, incluidos el emparejamiento, las listas de permisos y los puntos de enlace privados. De forma predeterminada, la herramienta no incluye componentes

operativos; sin embargo, se puede configurar con Amazon Managed Service for Prometheus, Amazon Managed Grafana CloudWatch, Amazon y AWS Secrets Manager si es necesario.

Tools (Herramientas)

- PeerIslands El generador de datos de prueba y el analizador de rendimiento incluyen dos componentes. El componente generador de datos de prueba ayuda a generar datos del mundo real altamente específicos del cliente, basados en el esquema de MongoDB. La herramienta está totalmente basada en la interfaz de usuario, con una rica biblioteca de datos, y se puede utilizar para generar rápidamente miles de millones de registros en MongoDB. La herramienta también proporciona capacidades para implementar relaciones entre campos en el esquema de MongoDB. El componente analizador del rendimiento ayuda a generar consultas y agregaciones altamente específicas para el cliente y a realizar pruebas de rendimiento realistas en MongoDB. Se puede usar el analizador de rendimiento para probar el rendimiento de MongoDB con perfiles de carga enriquecidos y consultas parametrizadas para un caso de uso específico.

Prácticas recomendadas

Consulte los siguientes recursos:

- MongoDB Schema Design Best Practices (Prácticas recomendadas de diseño de esquemas de MongoDB) (sitio web para desarrolladores de MongoDB)
- Best Practices of Deploying MongoDB Atlas on AWS (Prácticas recomendadas para implementar MongoDB Atlas en AWS) (sitio web de MongoDB)
- Conexión segura de aplicaciones a un plano de datos de MongoDB Atlas con AWS PrivateLink (entrada del blog de AWS)
- Best Practices Guide for MongoDB Performance (Guía de prácticas recomendadas para el rendimiento de MongoDB) (sitio web de MongoDB)

Epics

Comprender los datos de origen

Tarea	Descripción	Habilidades requeridas
Conozca el tamaño de la base de datos de origen actual de SQL Server.	Conozca su huella actual de SQL Server. Para este fin, se pueden ejecutar consultas en el esquema `INFORMATION_SCHEMA` de la base de datos. Determine el número de tablas y el tamaño de cada tabla. Analice el índice asociado a cada tabla. Para obtener más información sobre el análisis de SQL, consulte la entrada del blog SQL2Mongo: Data Migration Journey en el sitio web. PeerIslands	Administrador de base de datos
Comprenda el esquema de origen.	Determine el esquema de la tabla y la representación empresarial de los datos (por ejemplo, códigos postales, nombres y moneda). Utilice el diagrama de relaciones entre entidades (ER) existente o genere el diagrama ER a partir de la base de datos existente. Para obtener más información, consulte la entrada del blog SQL2Mongo: Data Migration Journey en el PeerIslands sitio web.	Administrador de base de datos
Comprenda los patrones de consulta.	Documente las 10 consultas SQL principales que utiliza.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Puede utilizar las tablas performance_schema .events_statements _summary_by_digest, disponibles en la base de datos, para comprender las consultas principales. Para obtener más información, consulte la entrada del blog SQL2Mongo: Data Migration Journey en el PeerIslands sitio web.	
Comprenda los compromisos de SLA.	Documente los acuerdos de nivel de servicio (SLAs) previstos para las operacion es de bases de datos. Las medidas habituales incluyen la latencia de las consultas y las consultas por segundo. Las medidas y sus objetivos suelen estar disponibles en los documentos de requisitos no funcionales (NFR).	Administrador de base de datos

Definir el esquema de MongoDB

Tarea	Descripción	Habilidades requeridas
Defina el esquema de origen.	Defina varias opciones para el esquema de MongoDB de destino. Para obtener más información, consulte Schemas (Esquemas) en la documentación de MongoDB	Ingeniero de MongoDB

Tarea	Descripción	Habilidades requeridas
	Atlas. Tenga en cuenta las prácticas recomendables y los patrones de diseño basados en las relaciones de las tablas.	
Defina los patrones de consulta de destino.	Defina las consultas de MongoDB y las canalizaciones de agregación. Estas consultas equivalen a las consultas principales que capturó para su carga de trabajo de SQL Server. Para saber cómo construir canalizaciones de agregación de MongoDB, consulte la documentación de MongoDB.	Ingeniero de MongoDB
Defina el tipo de instancia de MongoDB.	Determine el tamaño de la instancia que planea utilizar para las pruebas. Para obtener orientación, consulte la documentación de MongoDB.	Ingeniero de MongoDB

Prepare la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Configure el clúster de MongoDB Atlas.	Para configurar un clúster de MongoDB en AWS, siga las instrucciones de la documentación de MongoDB.	Ingeniero de MongoDB
Cree usuarios en la base de datos de destino.	Configure el clúster de MongoDB Atlas para el	Ingeniero de MongoDB

Tarea	Descripción	Habilidades requeridas
	acceso y la seguridad de la red siguiendo las instrucciones de la documentación de MongoDB.	
Cree los roles adecuados en AWS y configure el control de acceso basado en roles para Atlas.	Si es necesario, configure usuarios adicionales siguiendo las instrucciones de la documentación de MongoDB. Configure la autenticación y la autorización mediante los roles de AWS.	Ingeniero de MongoDB
Configure Compass para el acceso a MongoDB Atlas.	Configure el programa de utilidad GUI MongoDB Compass para facilitar la navegación y el acceso.	Ingeniero de MongoDB

Configurar la carga base mediante el generador de datos de prueba

Tarea	Descripción	Habilidades requeridas
Instale el generador de datos de prueba.	Instale PeerIsland Test Data Generator en su entorno.	Ingeniero de MongoDB
Configure el generador de datos de prueba para generar los datos adecuados.	Cree una plantilla mediante la biblioteca de datos para generar datos específicos para cada campo del esquema de MongoDB. Para obtener más información, consulte MongoDB Data Generator & Perf. Video del analizador.	Ingeniero de MongoDB

Tarea	Descripción	Habilidades requeridas
Generador de datos de prueba con escala horizontal para generar la carga requerida.	Utilice la plantilla que creó para iniciar la generación de cargas con respecto a la colección de destino; para ello, configure el paralelismo requerido. Determine los plazos y la escala para generar los datos necesarios.	Ingeniero de MongoDB
Valide la carga en MongoDB Atlas.	Compruebe los datos cargados en MongoDB Atlas.	Ingeniero de MongoDB
Genere los índices necesarios en MongoDB.	Defina los índices según sea necesario, en función de los patrones de consulta. Para conocer las prácticas recomendadas, consulte la documentación de MongoDB.	Ingeniero de MongoDB

Llevar a cabo pruebas de rendimiento

Tarea	Descripción	Habilidades requeridas
Configure los perfiles de carga en Performance Analyzer.	Cree un perfil de pruebas de rendimiento en Performance Analyzer; para ello, configure consultas específicas y sus correspondientes ponderación, duración de la prueba y etapas. Para obtener más información, consulte MongoDB Data Generator & Perf. Video del analizador.	Ingeniero de MongoDB

Tarea	Descripción	Habilidades requeridas
Ejecute las pruebas de rendimiento.	Utilice el perfil de prueba de rendimiento que creó para iniciar la prueba con respecto a la colección de destino; para ello, configure el paralelismo requerido. Escale horizontalmente la herramien ta de prueba de rendimiento para ejecutar consultas en MongoDB Atlas.	Ingeniero de MongoDB
Registre los resultados de la prueba.	Registre la latencia P95 y P99 para las consultas.	Ingeniero de MongoDB
Ajuste su esquema y sus patrones de consulta.	Modifique los índices y los patrones de consulta para solucionar cualquier problema de rendimiento.	Ingeniero de MongoDB

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporale s de AWS.	Elimine todos los recursos temporales que utilizó para el generador de datos de prueba y el analizador de rendimiento.	Administrador de AWS
Actualice los resultados de las pruebas de rendimiento.	Comprenda el rendimiento de las consultas de MongoDB y compárelo con el suyo. SLAs Si es necesario, ajuste el esquema de MongoDB y vuelva a ejecutar el proceso.	Ingeniero de MongoDB

Tarea	Descripción	Habilidades requeridas
Finalice el proyecto.	Cerrar el proyecto y enviar comentarios.	Ingeniero de MongoDB

Recursos relacionados

- GitHub repositorio: S3toAtlas
- Esquema: MongoDB Schema design (Diseño de esquema de MongoDB)
- Canalizaciones de agregación: MongoDB aggregation pipelines (Canalizaciones de agregación de MongoDB)
- Dimensionamiento de MongoDB Atlas: Sizing tier selection (Selección de capa de dimensionamiento)
- Video: MongoDB Data Generator & Perf. Analizador
- Referencias: documentación de MongoDB
- Tutorialws: MongoDB developer guide, MongoDB Jumpstart
- AWS Marketplace: MongoDB Atlas en AWS Marketplace
- Soluciones de socios de AWS: MongoDB Atlas on AWS Reference Deployment (Implementación de referencia de MongoDB Atlas en AWS)

Recursos adicionales:

- Análisis de SQL
- MongoDB Developer Community forums (Foros de la comunidad de desarrolladores de MongoDB)
- MongoDB Performance Tuning Questions (Preguntas sobre el ajuste del rendimiento de MongoDB)
- Operational Analytics with Atlas and Redshift (Análisis operativo con Atlas y Redshift)
- Application modernization with MongoDB Atlas and AWS Elastic Beanstalk (Modernización de aplicaciones con MongoDB Atlas y AWS Elastic Beanstalk)

Automatice blue/green las implementaciones de las bases de datos globales de Amazon Aurora mediante los principios de la IaC

Ishwar Chauthaiwale, ANKIT JAIN y Ramu Jagini, Amazon Web Services

Resumen

La administración de las actualizaciones de bases de datos, las migraciones o los esfuerzos de escalado puede resultar difícil para las organizaciones que ejecutan cargas de trabajo críticas en bases de datos globales de Amazon Aurora. Garantizar que estas operaciones se lleven a cabo de forma fluida y sin tiempo de inactividad es esencial para mantener la disponibilidad del servicio y evitar interrupciones para los usuarios.

Una estrategia de blue/green implementación ofrece una solución a este desafío, ya que le permite ejecutar dos entornos idénticos de forma simultánea: azul (el entorno actual) y verde (el nuevo entorno). Una blue/green estrategia le permite implementar cambios, realizar pruebas y cambiar el tráfico entre entornos con un riesgo y un tiempo de inactividad mínimos.

Este patrón le ayuda a automatizar el proceso de blue/green implementación de las bases de datos globales de Aurora mediante el uso de los principios de la infraestructura como código (IaC). Utiliza AWS CloudFormationAmazon Route 53 y Amazon Route 53 para simplificar blue/green las implementaciones. AWS Lambda Para mejorar la confiabilidad, utiliza identificadores de transacciones globales (GTIDs) para la replicación. La replicación basada en GTID proporciona una mejor coherencia de datos y funcionalidades de conmutación por error entre entornos en comparación con la replicación de registros binarios (binlog).

> **Note**
>
> Este patrón presupone que usa un clúster de base de datos global de la edición de Aurora compatible con MySQL. Si en su lugar utiliza una edición de Aurora compatible con PostgreSQL, utilice los equivalentes en PostgreSQL de los comandos de MySQL.

Si sigue los pasos que se describen en este patrón, puede hacer lo siguiente:

- Aprovisionar una base de datos global de Aurora verde: mediante CloudFormation plantillas, se crea un entorno verde que refleja el entorno azul existente.
- Configurar la replicación basada en GTID: configure la replicación de GTID para mantener sincronizados los entornos azul y verde.

- Cambie el tráfico sin problemas: utilice Route 53 y Lambda para cambiar automáticamente el tráfico del entorno azul al verde tras completar la sincronización.
- Finalice la implementación: valide que el entorno ecológico esté en pleno funcionamiento como base de datos principal y, a continuación, detenga la replicación y elimine los recursos temporales.

El enfoque de este patrón proporciona las siguientes ventajas:

- Reduce el tiempo de inactividad durante las actualizaciones o migraciones críticas de las bases de datos: la automatización garantiza una transición fluida entre entornos con una interrupción mínima del servicio.
- Permite reversiones rápidas: si surge un problema después de cambiar el tráfico al entorno verde, puede volver rápidamente al entorno azul y mantener la continuidad del servicio.
- Mejora las pruebas y la verificación: el entorno verde se puede probar por completo sin afectar al entorno azul activo, lo que reduce la probabilidad de que surjan errores en producción.
- Garantiza la coherencia de datos: la replicación basada en GTID mantiene sincronizados los entornos azul y verde, lo que evita la pérdida de datos o las incoherencias durante la migración.
- Mantiene la continuidad empresarial: la automatización de blue/green las implementaciones ayuda a evitar interrupciones prolongadas y pérdidas financieras al mantener sus servicios disponibles durante las actualizaciones o las migraciones.

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- Un clúster de base de datos global de Aurora compatible con MySQL de origen (entorno azul). Las bases de datos globales proporcionan una configuración multirregional para tener alta disponibilidad y recuperación ante desastres. Para obtener instrucciones sobre cómo configurar un clúster de base de datos global, consulte la documentación de Aurora.
- Replicación basada en GTID habilitada en el clúster de origen.

Limitaciones

- Algunos Servicios de AWS no están disponibles en todos Regiones de AWS. Para conocer la disponibilidad de las regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- Versión 8.0 o posterior de Aurora compatible con MySQL

Arquitectura

En el siguiente diagrama se ilustra lo siguiente:

- Configuración de la base de datos global: un clúster de base de datos global Aurora se implementa estratégicamente en dos Regiones de AWS. Esta configuración permite la distribución geográfica y la redundancia regional para mejorar las capacidades de recuperación ante desastres.
- Replicación de la región principal a la región secundaria: el mecanismo de replicación lógica garantiza una sincronización perfecta de los datos de la región principal a la secundaria. Esta replicación conserva la coherencia de datos con una latencia mínima en todas las distancias geográficas.
- Replicación entre clústeres basada en GTID: la replicación basada en GTID mantiene la coherencia de las transacciones y el orden del flujo de datos entre el clúster principal azul y el clúster principal verde, y garantiza una sincronización de datos fiable.
- Replicación del clúster azul principal al secundario: la replicación lógica establece una canalización de datos sólida entre el clúster principal azul y el clúster secundario. Esta replicación permite una sincronización continua de los datos y una alta disponibilidad.
- Configuración de DNS de Route 53: los registros de zonas alojadas de Route 53 administran la resolución de DNS de todos los puntos de conexión de las bases de datos de clústeres azules y verdes. Esta configuración proporciona una asignación perfecta de los puntos de conexión y permite un enrutamiento eficiente del tráfico durante los escenarios de conmutación por error.

Tools (Herramientas)

Servicios de AWS

- Amazon Aurora es un motor de base de datos relacional completamente administrado diseñado para la nube y compatible con MySQL y PostgreSQL.
- CloudFormationle ayuda a modelar y configurar sus AWS recursos para que pueda dedicar menos tiempo a administrarlos y más tiempo a centrarse en las aplicaciones en las que se ejecutan AWS. Crea una plantilla que describe todos los AWS recursos que desea y CloudFormation se encarga de aprovisionar y configurar esos recursos por usted.
- AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.

Prácticas recomendadas

Le recomendamos que revise detenidamente la AWS documentación para comprender mejor la estrategia de implementación económica y ecológica, la replicación basada en GTID y las políticas de enrutamiento ponderado de Route 53. Este conocimiento es crucial para implementar y administrar eficazmente las migraciones de bases de datos, garantizar la coherencia de datos y optimizar el enrutamiento del tráfico. Al obtener una comprensión completa de estas AWS funciones y prácticas recomendadas, estará mejor preparado para gestionar futuras actualizaciones, minimizar el tiempo de inactividad y mantener un entorno de base de datos seguro y resistente.

Para ver las pautas de Servicios de AWS uso de este patrón, consulte la siguiente AWS documentación:

- Prácticas recomendadas con Amazon Aurora MySQL
- prácticas recomendadas de CloudFormation
- Prácticas recomendadas para trabajar con AWS Lambda funciones
- Prácticas recomendadas para Amazon Route 53

Epics

Creación de un entorno verde

Tarea	Descripción	Habilidades requeridas
Cree una copia de seguridad de la instantánea a partir del clúster azul.	En una blue/green implement ación, el entorno verde representa una versión nueva e idéntica del entorno de base de datos actual (azul). Utilice el entorno verde para probar las actualizaciones de forma segura, validar los cambios y garantizar la estabilidad antes de cambiar el tráfico de producción. Actúa como espacio de pruebas para implementar cambios en las bases de datos con una interrupción mínima del entorno activo. Para crear un entorno verde, primero debe crear una instantánea del clúster principal (azul) en la base de datos global de Aurora compatible con MySQL. Esta instantánea sirve de base para crear el entorno verde. Para crear una instantánea: 1. Inicie sesión en la consola de Amazon Relational Database Service (Amazon	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	RDS) Consola de administración de AWS y ábrala. 2. Seleccione su clúster principal (azul). 3. Seleccione Acciones, Tomar una instantánea. 4. Proporcione un nombre para la instantánea, como `blue-green-demo` , e inicie el proceso de copia de seguridad. Como alternativa, puede usar AWS Command Line Interface (AWS CLI) para crear la instantánea: `aws rds create-db-cluster-snapshot --db-cluster-snapshot-identifier blue-green-demo --db-cluster-identifier ex-global-cluster --region eu-west-1` Asegúrese de que la instantánea se complete correctamente antes de pasar al siguiente paso.	

Tarea	Descripción	Habilidades requeridas
Genere la CloudFormation plantilla para su base de datos global y sus recursos.	El generador CloudForm ation IaC le ayuda a generar CloudFormation plantillas a partir de AWS los recursos existentes. Utilice esta función para crear una CloudForm ation plantilla para su base de datos global compatible con Aurora MySQL existente y sus recursos asociados. Esta plantilla configura grupos de subred, grupos de seguridad, grupos de parámetros y otros ajustes. 1. Siga las instrucciones de la CloudFormation documenta ción para navegar hasta la herramienta y conectarla a su entorno. AWS 2. Seleccione la base de datos global de Aurora y los recursos asociados para generar la plantilla.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Modifique la CloudFormation plantilla para el entorno ecológico.	Personalice la CloudFormation plantilla para que refleje la configuración del entorno verde. Esto implica actualizar los nombres e identificadores de los recursos para garantizar que el entorno verde funcione de forma independiente del clúster azul. 1. Actualice las propiedades `DBClusterIdentifier` y `DBInstanceIdentifier` para representar el entorno verde. 2. Modifique los nombres de otros recursos (por ejemplo, los grupos de subredes y los grupos de seguridad) para evitar conflictos con el entorno azul existente. 3. Habilite la replicación basada en GTID en la plantilla configurando los parámetros correctos, tal y como se describe en la documentación de Aurora. 4. Cambie la `SnapshotIdentifier` propiedad para especificar el Región de AWS ID de su cuenta y el nombre de la instantánea del paso anterior:	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`SnapshotIdentifier: arn:aws:rds:<region>:<account-id>:snapshot:<snapshot-name>` **Note** Si utiliza la propiedad `SnapshotIdentifier` para restaurar un clúster de base de datos, evite especificar propiedades como `GlobalClusterIdentifier`, `MasterUsername` o `MasterUserPassword`.	

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation pila para crear recursos para un entorno ecológico.	En este paso, implementará la CloudFormation plantilla personalizada para crear los recursos para el entorno ecológico. Para implementar la CloudFormation pila: 1. Abra la consola de AWS CloudFormation. 2. Seleccione Crear pila, Con nuevos recursos (estándar). 3. Carga la CloudFormation plantilla modificada o especifica la URL de la plantilla. Elija Siguiente. 4. Introduzca un nombre de pila como `GreenClusterStack` y proporcione los parámetros necesarios (por ejemplo, `GreenClusterIdentifier`). Elija Siguiente. 5. Configura opciones de pila adicionales según sea necesario y marca la casilla para confirmar que CloudFormation podrían crearse recursos AWS Identity and Access Management (IAM). Elija Siguiente.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	6. Revise los detalles de la pila. 7. Elija Enviar. CloudFormation inicia el proceso de creación de los recursos del entorno ecológico. Este proceso puede tardar varios minutos en completarse.	

Tarea	Descripción	Habilidades requeridas
Valide la CloudFormation pila y los recursos.	Cuando se complete el despliegue de la CloudFormation pila, tendrás que comprobar que el entorno ecológico se ha creado correctamente: 1. En la sección Resultados de la CloudFormation pila, compruebe los puntos finales del clúster de base de datos y de la instancia de la base de datos para comprobar que la configuración es correcta. 2. Abra la consola de Amazon RDS y confirme que el nuevo clúster de base de datos de Aurora (entorno verde) esté disponible. 3. Asegúrese de que todos los recursos asociados, como las subredes y los grupos de seguridad, se hayan creado y vinculado al entorno verde. Tras la verificación, el entorno verde estará listo para seguirlo configurando, así como para replicarlo desde el entorno azul.	Administrador de base de datos

Configuración de la replicación basada en GTID

Tarea	Descripción	Habilidades requeridas
Compruebe la configuración de GTID en el clúster azul.	GTIDs proporcionan un método altamente confiable para replicar datos entre sus entornos azul y verde. La replicación basada en GTID ofrece un enfoque flexible y simplificado al asignar un identificador único a cada transacción en el entorno azul. Este método garantiza que la sincronización de datos entre los entornos sea fluida, coherente y más fácil de administrar que la replicación binlog tradicional. Antes de configurar la replicación, debe asegurarse de que la replicación basada en GTID esté habilitada correctamente en el clúster azul. Este paso garantiza que cada transacción del entorno azul tenga un seguimiento exclusivo y se pueda replicar en el entorno verde. Para confirmar que los GTID están habilitados, siga estos pasos: 1. En la consola de Amazon RDS, revise el grupo de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	parámetros asignado al clúster azul. 2. Compruebe que estén configurados los siguientes parámetros: • `gtid-mode = ON` • `enforce_gtid_consistency = ON` Esta configuración permite hacer un seguimiento de los GTID para todas las transacciones futuras en el entorno azul. Después de confirmar esta configuración, puede comenzar a configurar la replicación.	

Tarea	Descripción	Habilidades requeridas
Cree un usuario de replicación	Para replicar datos del entorno azul al entorno verde, tiene que crear un usuario de replicación específico en el clúster azul. Este usuario será responsable de administrar el proceso de replicación. Para configurar el usuario de replicación, siga estos pasos: 1. Conéctese al clúster azul con un cliente MySQL. 2. Ejecute los siguientes comandos para crear el usuario de replicación: `CREATE USER 'repl_use r'@'%' IDENTIFIED BY 'repl_password'; GRANT REPLICATI ON SLAVE ON . TO 'repl_user'@'%'; FLUSH PRIVILEGES;` Este usuario ahora tiene los permisos necesarios para replicar datos entre los dos entornos.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Configure la replicación basada en GTID en el clúster verde.	El siguiente paso es configurar el clúster verde para la replicación basada en GTID. Esta configuración garantiza que en el entorno verde se reflejen continuamente todas las transacciones que se realicen en el entorno azul. Para configurar el clúster verde, siga estos pasos: 1. Conéctese al clúster verde con un cliente MySQL. 2. Ejecute el siguiente comando para configurar la replicación. `CHANGE MASTER TO MASTER_HOST='blue-cluster-endpoint', MASTER_USER='repl_user', MASTER_PASSWORD='repl_password', MASTER_AUTO_POSITION=1;` donde: • Sustituya `blue-cluster-endpoint` por el punto de conexión del clúster azul. • El parámetro `MASTER_AUTO_POSITION=1` le indica a MySQL que use la replicación basada en	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	GTID. Coloca automáticamente el clúster verde para replicar las transacciones del clúster azul sin tener que hacer un seguimiento de los registros y las posiciones manualmente.	
Inicie la replicación en el clúster verde.	Ya puede empezar el proceso de replicación: En el clúster verde, ejecute este comando: `START SLAVE;` Este comando permite que el entorno verde comience a sincronizar los datos y a recibir y aplicar transacciones del entorno azul.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Verifique el proceso de replicación.	Para comprobar que el entorno verde está replicando con precisión los datos del clúster azul, siga estos pasos: 1. Ejecute el siguiente comando en el clúster verde para comprobar el estado de la replicación: `SHOW SLAVE STATUS\G;` 2. Revise la salida para comprobar lo siguiente: • `Slave_IO_Running = Yes` • `Slave_SQL_Running = Yes` • Los `Executed_Gtid_Set` valores `Retrieved_Gtid_Set` up-to-date y están sincronizados con el clúster azul. • No hay errores de replicación en el campo `Last_Error` . Si todos los indicadores son correctos, la replicación basada en GTID funciona sin problemas y el entorno verde está completamente sincronizado con el entorno azul.	Administrador de base de datos

Cambio del tráfico del clúster azul al verde

Tarea	Descripción	Habilidades requeridas
Configure las políticas de enrutamiento ponderado de Route 53.	Después de verificar la coherencia de datos entre los entornos azul y verde, puede cambiar el tráfico del clúster azul al clúster verde. Esta transición debe ser fluida y minimizar el tiempo de inactividad y garantizar la integridad de la base de datos de la aplicación. Para cumplir con estos requisito s, puede usar Route 53 para el enrutamiento de DNS y Lambda para automatizar el cambio de tráfico. Además, un plan de reversión bien definido garantiza que pueda volver al clúster azul en caso de que surja algún problema. El primer paso es configura r el enrutamiento ponderado en Route 53. El enrutamiento ponderado le permite controlar la distribución del tráfico entre los clústeres azul y verde y desplazar gradualmente el tráfico de un entorno a otro. Para configurar el enrutamie nto ponderado, siga estos pasos:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	1. Abra la consola de Route 53 y seleccione la zona alojada. 2. Cree dos registros DNS (CNAMEs) para la base de datos: un registro para el clúster azul y otro para el clúster verde. 3. Asigne las ponderaciones iniciales: • Establezca una ponderación inicial baja (por ejemplo, un 5 %) para que el clúster verde envíe una pequeña parte del tráfico para realizar pruebas. • Establezca una ponderación mayor (por ejemplo, un 95 %) para el clúster azul, de modo que retenga la mayor parte del tráfico. Esta configuración le permite realizar una transición gradual que reduce el riesgo y permite realizar pruebas en tiempo real antes de hacer el cambio completo. Para obtener más información sobre las políticas de	

Tarea	Descripción	Habilidades requeridas
	enrutamiento ponderado, consulte la documentación de Route 53.	

Tarea	Descripción	Habilidades requeridas

Implemente una función de Lambda para supervisar el retraso de la replicación.	Para garantizar que el entorno verde se sincronice completamente con el entorno azul, implemente una función de Lambda que supervise el retraso de la replicación entre los clústeres. Esta función puede comprobar el estado de la replicación (específicamente, la métrica Seconds_Behind_Master) para determinar si el clúster verde está preparado para gestionar todo el tráfico.
	
	A continuación, se muestra un ejemplo de función de Lambda que puede utilizar:
	
	`import boto3`
	
	`def check_replication_lag(event, context):`
	`client = boto3.client('rds')`
	`response = client.describe_db_instances(DBInstanceIdentifier='green-cluster-instance')`
	`replication_status = response['DBInstances'][0]['ReadReplicaDBInstanceIdentifiers']`
	`if replication_status:`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	<pre>lag = replicati
	on_status[0]['Repl
	icationLag']
	return lag
	return -1</pre>
	Esta función comprueba el retraso de la replicación y devuelve el valor. Si el retraso es cero, el clúster verde está totalmente sincronizado con el clúster azul.	

Tarea	Descripción	Habilidades requeridas

Automatice el ajuste de ponderaciones de DNS mediante Lambda.	Cuando el retraso de la replicación llegue a cero, ya podrá cambiar todo el tráfico al clúster verde. Puede automatizar esta transició n mediante otra función de Lambda que ajuste las ponderaciones de DNS en Route 53 para dirigir el 100 % del tráfico al clúster verde.
	
	A continuación, se muestra un ejemplo de una función de Lambda que automatiza el cambio de tráfico:
	
	`import boto3`
	
	`def switch_traffic(eve nt, context):`
	`route53 = boto3.cli ent('route53')`
	`lag = check_rep lication_lag(event, context)`
	`if lag == 0:`
	`response = route53.change_res ource_record_sets(`
	`HostedZon eId='YOUR_HOSTED_Z ONE_ID',`
	`ChangeBat ch={`
	`'Changes': [`
	`{`
	`'Action': 'UPSERT',`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	'ResourceRecordSet': {
	'Name': 'db.example.com',
	'Type': 'CNAME',
	'SetIdentifier': 'GreenCluster',
	'Weight': 100,
	'TTL': 60,
	'ResourceRecords': [{'Value': 'green-cluster-endpoint'}]
	}
	},
	{
	'Action': 'UPSERT',
	'ResourceRecordSet': {
	'Name': 'db.example.com',
	'Type': 'CNAME',
	'SetIdentifier': 'BlueCluster',
	'Weight': 0,
	'TTL': 60,
	'ResourceRecords':	

Tarea	Descripción	Habilidades requeridas

	<pre>[{'Value': 'blue-clu
	ster-endpoint'}]
	
	}
	}
	]
	}
	)
	return response</pre>
	Esta función comprueba el retraso de la replicación y actualiza las ponderaciones de DNS de Route 53 cuando el retraso es cero para transferir completamente el tráfico al clúster verde.
	
	Note
	Durante el proceso de transición, si el clúster azul experimenta un tráfico de escritura intenso, considere la posibilidad de pausar temporalmente las operaciones de escritura durante la transición. Esto garantiza que la replicación se recupere del retraso y evita incoherencias	

Tarea	Descripción	Habilidades requeridas
	en los datos entre los clústeres azul y verde.	

Tarea	Descripción	Habilidades requeridas
Verifique el cambio de tráfico.	Una vez que la función de Lambda ajuste las ponedraciones de DNS, debe comprobar que todo el tráfico se dirige al clúster verde y que el cambio se ha realizado correctamente. Para verificarlo, siga estos pasos: 1. Supervise los registros de DNS de Route 53 para confirmar que el tráfico se dirija al clúster verde. Para obtener más información, consulte la documentación de Route 53. 2. Confirme que se atienda a los usuarios desde el entorno verde para comprobar el rendimiento de las aplicaciones. 3. Compruebe las conexione s de la base de datos para confirmar que el clúster verde gestione todas las solicitudes de la base de datos. 4. Supervisa CloudWatch las métricas de Amazon para detectar cualquier signo de latencia, retraso en la replicación o degradaci	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	ón del rendimiento. Para obtener más información, consulte la documentación de Aurora. Si todo funciona según lo esperado, el cambio de tráfico se ha completado.	

Tarea	Descripción	Habilidades requeridas
Si encuentra algún problema, revierta los cambios.	Tener un plan de reversión es esencial en caso de que surja algún problema después del cambio de tráfico. A continuación, le explicamos cómo revertir rápidamente al clúster azul si es necesario: 1. Para revertir las ponderaciones de DNS en Route 53, utilice la misma función de Lambda o ajuste manualmente las ponderaciones de DNS de Route 53 para volver a dirigir el 100 % del tráfico al clúster azul. 2. Supervise el rendimiento de las aplicaciones: supervise inmediatamente los registros, CloudWatch las métricas y el rendimiento de las bases de datos de las aplicaciones para confirmar que el cambio al entorno azul ha resuelto los problemas. 3. Identifique y resuelva los problemas: investigue y solucione cualquier problema relacionado con el clúster verde antes de intentar realizar otro cambio de tráfico.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Al implementar este plan de reversión, puede garantizar una interrupción mínima para sus usuarios en caso de que surjan problemas inesperados.	

Validación y detención de la replicación basada en GTID

Tarea	Descripción	Habilidades requeridas
Detenga la replicación basada en GTID en el clúster verde.	Después de cambiar el tráfico del entorno azul al entorno verde, debe validar que la transición se haya completado correctamente y asegurarse de que el clúster verde funcione según lo esperado. Además, debe detener la replicación basada en GTID entre los clústeres azul y verde, ya que el entorno verde ahora sirve como base de datos principal. Realizar estas tareas garantiza que su entorno sea seguro, ágil y optimizado para las operaciones continuas. Para detener la replicación, siga estos pasos: 1. Utilice un cliente MySQL para conectarse al clúster verde.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	2. Ejecute el siguiente comando SQL para detener el proceso de replicación en el clúster verde:
	`STOP SLAVE;`
	3. (Opcional) Si lo desea, puede restablecer la configuración de replicación para borrar cualquier configuración de replicación residual:
	`RESET SLAVE ALL;`
	Cuando detiene la replicación, el clúster verde pasa a ser completamente independiente y funciona como el entorno de base de datos principal para las cargas de trabajo.	

Tarea	Descripción	Habilidades requeridas
Eliminación de recursos.	Al limpiar los recursos temporales o no usados que se crearon durante la migración del clúster azul al verde, se asegura de que el entorno siga siendo optimizado, seguro y rentable. Durante la limpieza, de ajustar la configuración de seguridad, realizar las copias de seguridad finales y retirar los recursos innecesarios. Para limpiar los recursos, siga estos pasos: 1. Actualice los grupos de seguridad: configure los grupos de seguridad asociados a los clústeres azul y verde para que reflejen el nuevo entorno principal (verde). Restrinja el acceso al entorno azul si ya no es necesario y compruebe que la configura ción de seguridad del clúster verde siga las prácticas recomendadas. 2. Realice una copia de seguridad final del clúster verde: una vez finalizad a la migración, tome una última instantánea del clúster verde para que	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	sirva de copia de seguridad . Si es necesario, puede utilizar esta instantánea para restaurar el entorno en el futuro.
	
	`aws rds create-db-snapshot --db-instance-identifier green-cluster-instance --db-snapshot-identifier green-cluster-final-snapshot`
	
	3. Revise y elimine los recursos temporales: revise los recursos temporales que se crearon durante la migración, como los grupos de seguridad temporales, las instantáneas u otras configuraciones. Elimine los recursos que ya no sean necesarios para evitar costos innecesarios. Por ejemplo, elimine el clúster azul si ya no es necesario:
	
	`aws rds delete-db-cluster --db-cluster-identifier blue-cluster-identifier --skip-final-snapshot`
	
	La limpieza de los recursos ayuda a mantener un entorno	

Tarea	Descripción	Habilidades requeridas
	seguro y optimizado, reduce los costos y garantiza que solo quede la infraestructura necesaria.	

Recursos relacionados

CloudFormation:

- CloudFormation Guía del usuario
- prácticas recomendadas de CloudFormation
- Generar plantillas de los recursos existentes con el generador IaC
- Importe aplicaciones enteras a CloudFormation (AWS entrada de blog)

Amazon Aurora:

- Guía del usuario de Amazon Aurora
- Administración de un clúster de base de datos Amazon Aurora

Estrategia de implementación azul/verde:

- Descripción general de las Blue/Green implementaciones de Amazon Aurora

Replicación basada en GTID:

- Uso de la replicación basada en GTID (documentación de Amazon RDS)

AWS Lambda:

- AWS Lambda Guía para desarrolladores
- Prácticas recomendadas para trabajar con funciones AWS Lambda

Amazon Route 53:

- Guía para desarrolladores de Amazon Route 53
- Enrutamiento ponderado

Herramientas del cliente MySQL:

- PyMySQL

Automatice la replicación de las instancias de Amazon RDS en Cuentas de AWS

Parag Nagwekar y Arun Chandapillai, Amazon Web Services

Resumen

Este patrón le muestra cómo automatizar el proceso de replicación, seguimiento y reversión de sus instancias de base de datos de Amazon Relational Database Service (Amazon RDS) en Cuentas de AWS diferentes instancias mediante el uso de y. AWS Step Functions AWS Lambda Puede utilizar esta automatización para realizar una replicación a gran escala de instancias de base de datos de RDS sin que ello afecte al rendimiento ni a los gastos operativos adicionales, independientemente del tamaño de su organización. También puede utilizar este patrón para ayudar a su organización a cumplir con las estrategias de gobierno de datos obligatorias o los requisitos de conformidad que exigen que sus datos se repliquen y sean redundantes en diferentes y diferentes. Cuentas de AWS Regiones de AWS La replicación entre cuentas de los datos de Amazon RDS a escala es un proceso manual ineficiente y propenso a errores que puede resultar costoso y llevar mucho tiempo, pero la automatización de este patrón puede ayudarle a conseguir la replicación entre cuentas de forma segura, eficaz y eficiente.

Requisitos previos y limitaciones

Requisitos previos

- Dos Cuentas de AWS
- Una instancia de base de datos de RDS, activa y en ejecución en la fuente Cuenta de AWS
- Un grupo de subredes para la instancia de base de datos de RDS en el destino Cuenta de AWS
- Una clave AWS Key Management Service (AWS KMS) creada en el origen Cuenta de AWS y compartida con la cuenta de destino (para obtener más información sobre los detalles de la política, consulte la sección de información adicional de este patrón).
- Una AWS KMS key en el destino Cuenta de AWS para cifrar la base de datos de la cuenta de destino

Limitaciones

- Algunas Servicios de AWS no están disponibles en todas Regiones de AWS. Para conocer la disponibilidad de las regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- Python 3.9 (usando AWS Lambda)
- PostgreSQL 11.3, 13.x y 14.x

Arquitectura

Pila de tecnología

- Amazon Relational Database Service (Amazon RDS)
- Amazon Simple Notification Service (Amazon SNS)
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- AWS Secrets Manager
- AWS Step Functions

Arquitectura de destino

El siguiente diagrama muestra una arquitectura para usar Step Functions para orquestar la replicación programada y bajo demanda de instancias de base de datos de RDS desde una cuenta de origen (cuenta A) a una cuenta de destino (cuenta B).

En la cuenta de origen (cuenta A en el diagrama), la máquina de estados Step Functions realiza lo siguiente:

1. Crea una instantánea de la instancia de base de datos de RDS en la cuenta A.
2. Copia y cifra la instantánea con una AWS KMS key de la cuenta A. Para garantizar el cifrado en tránsito, la instantánea se cifra independientemente de que la instancia de base de datos esté cifrada o no.
3. Comparte la instantánea de base de datos con la cuenta B al permitir que la cuenta B acceda a la instantánea.

4. Envía una notificación al tema de SNS y, a continuación, el tema de SNS invoca la función de Lambda en la cuenta B.

En la cuenta de destino (cuenta B en el diagrama), la función de Lambda ejecuta la máquina de estados Step Functions para orquestar lo siguiente:

1. Copia la instantánea compartida de la cuenta A a la cuenta B y utiliza la AWS KMS key de la cuenta A para descifrar primero los datos y, a continuación, los cifra mediante la AWS KMS key cuenta B.
2. Leer el secreto de Secrets Manager para capturar el nombre de la instancia de base de datos actual.
3. Restaura la instancia de base de datos de la instantánea con un nombre nuevo y predeterminado AWS KMS key para Amazon RDS.
4. Leer el punto de conexión de la nueva base de datos y actualizar el secreto de Secrets Manager con el nuevo punto de conexión de la base de datos y, a continuación, etiquetar la instancia de base de datos anterior para poder eliminarla más adelante.
5. Conservar las N instancias más recientes de las bases de datos y eliminar todas las demás instancias.

Tools (Herramientas)

Servicios de AWS

- Amazon Relational Database Service (Amazon RDS) lo ayuda a configurar, utilizar y escalar una base de datos relacional en la Nube de AWS.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todo el territorio Cuentas de AWS y Regiones de AWS.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la

capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

- AWS SDK para Python (Boto3)es un kit de desarrollo de software que le ayuda a integrar su aplicación, biblioteca o script de Python con Servicios de AWS.
- AWS Secrets Manager lo ayuda a reemplazar las credenciales codificadas en su código, incluidas contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- AWS Step Functionses un servicio de organización sin servidor que le ayuda a combinar funciones de Lambda y otras Servicios de AWS para crear aplicaciones críticas para la empresa.

Repositorio de código

El código de este patrón está disponible en el repositorio RDS Replication de Crossaccount. GitHub

Epics

Automatice la replicación de todas las instancias de base de datos de RDS Cuentas de AWS con un solo clic

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation pila en la cuenta de origen.	1. Inicie sesión en la cuenta Consola de administración de AWS de origen (cuenta A) y abra la CloudFormation consola. 2. En el panel de navegación, seleccione Stacks (Pilas). 3. Elija Create stack (Crear pila) y, a continuación, seleccione With existing resources (import resources) (Con recursos existentes (importar recursos)).	Administrador de la nube, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	4. En la página Identific ar recursos, seleccione Siguiente. 5. En la página Specify Template (Especificar plantilla), seleccione Upload a template (Subir una plantilla). 6. Seleccione Elegir archivo, seleccione el **`Cloudform ation-SourceAccoun tRDS.yaml`** archivo del repositorio de GitHub Crossaccount RDS Replication y, a continuac ión, elija Siguiente. 7. En Stack name (Nombre de pila), escriba un nombre para su pila. 8. En la sección Parameter s (Parámetros), especifiq ue los parámetros que se definen en la plantilla de la pila: • Para DestinationAccount Number, introduzca el número de cuenta de la instancia de base de datos de RDS de destino. • Para KeyName, introduzc a su. AWS KMS key • Para ScheduleE xpression, introduzca	

Tarea	Descripción	Habilidades requeridas
	una expresión cron (el valor predeterminado es a las 12:00 de la mañana todos los días). • DBIdentifierEn Fuente, introduzca el nombre de la base de datos de origen. • En DBSnapshotNombre de origen, introduzca el nombre de la instantán ea o acepte el nombre predeterminado. 9. Elija Siguiente. 10. En la página Configure stack options (Configur ar opciones de la pila), mantenga las opciones predeterminadas y elija Next (Siguiente). 11. Revise la configuración de la pila y seleccione Submit (Enviar). 12. Seleccione la pestaña Resources (Recursos) para su pila y, a continuación, anote el Nombre de recurso de Amazon (ARN) del tema de SNS.	

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation pila en la cuenta de destino.	1. Inicie sesión en la cuenta Consola de administración de AWS de destino (cuenta B) y abra la CloudFormation consola. 2. En el panel de navegación, seleccione Stacks (Pilas). 3. Elija Create stack (Crear pila) y, a continuación, seleccione With existing resources (import resources) (Con recursos existentes (importar recursos)). 4. En la página Identific ar recursos, seleccione Siguiente. 5. En la página Specify Template (Especificar plantilla), seleccione Upload a template (Subir una plantilla). 6. Elija un archivo, selección elo del **`Cloudform ation-DestinationA ccountRDS.yaml`** repositorio de GitHub Crossaccount RDS Replication y, a continuac ión, elija Siguiente. 7. En Stack name (Nombre de pila), escriba un nombre para su pila.	Arquitecto de nube, DevOps ingeniero y administrador de nube

Tarea	Descripción	Habilidades requeridas
	8. En la sección Parameters (Parámetros), especifique los parámetros que se definen en la plantilla de la pila: • Para DatabaseName, introduzca un nombre para la base de datos. • En Engine (Motor), introduzca el tipo de motor de base de datos que coincida con la base de datos fuente. • En DBInstanceClass, introduzca el tipo de instancia de base de datos preferido o acepte el predeterminado. • En Subnetgrups (Grupos de subredes), introduzca el grupo de subredes de VPC existente. Para obtener instrucciones sobre cómo crear un grupo de subredes, consulte el paso 2: Creación de un grupo de subredes de base de datos en la documentación de Amazon RDS. • Para SecretName, introduzca la ruta y el nombre secreto, o acepte el valor predeterminado.	

Tarea	Descripción	Habilidades requeridas
	• Para SGID, introduzca el ID del grupo de seguridad del clúster de destino. • Para KMSKey, introduzc a el ARN de la clave KMS en su cuenta de destino. • Para NoOfOlderInstances ello, introduzca el número de copias antiguas de las instancias de base de datos de RDS que desea conservar para la reversión. 9. Elija Siguiente. 10. En la página Configure stack options (Configur ar opciones de la pila), mantenga las opciones predeterminadas y elija Next (Siguiente). 11. Revise la configuración de la pila y seleccione Submit (Enviar). 12. Elija la pestaña Resources (Recursos) para su pila y, a continuación, anote el ID físico y el ARN de `InvokeStepFunction` .	

Tarea	Descripción	Habilidades requeridas
Compruebe la creación de la instancia de base de datos de RDS en la cuenta de destino.	1. Inicie sesión en la consola de Amazon RDS Consola de administración de AWS y ábrala. 2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, compruebe que la nueva instancia de base de datos de RDS aparece en el nuevo clúster.	Administrador de nube, arquitecto de nube, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas

Suscriba la función de Lambda al tema de SNS.	Debe ejecutar los siguiente s comandos AWS Command Line Interface (AWS CLI) para suscribir la función Lambda de la cuenta de destino (cuenta B) al tema de SNS de la cuenta de origen (cuenta A).
	
	En la cuenta A, ejecute el siguiente comando:
	
	`aws sns add-permission \ --label lambda-access --aws-account-id <DestinationAccount> \ --topic-arn <Arn of SNSTopic > \ --action-name Subscribe ListSubscriptionsB yTopic`
	
	En la cuenta B, ejecute el siguiente comando:
	
	`aws lambda add-permi ssion \ --function-name <Name of InvokeStepFunction > \ --source-arn <Arn of SNSTopic > \ --statement-id function-with-sns \ --action lambda:In vokeFunction \`
		Administrador de la nube, arquitecto de la nube y administrador de bases de datos

Tarea	Descripción	Habilidades requeridas

	`--principal sns.amazonaws.com`
	
	En la cuenta B, ejecute el siguiente comando:
	
	`aws sns subscribe \ --protocol "lambda" \ --topic-arn <Arn of SNSTopic> \ --notification-endpoint <Arn of InvokeStepFunction>`	

Tarea	Descripción	Habilidades requeridas
Sincronice la instancia de base de datos de RDS de la cuenta de origen con la cuenta de destino.	Inicie la replicación de la base de datos bajo demanda iniciando la máquina de estados Step Functions en la cuenta de origen. 1. Abra la consola Step Functions. 2. En el panel de navegación, elija State machines (Máquinas de estado). 3. Elija su máquina de estado. 4. En la pestaña Executions (Ejecuciones), seleccione la función y, a continuación, elija Start execution (Iniciar ejecución) para iniciar el flujo de trabajo. **Note** Hay un programador para ayudarlo a ejecutar la replicación automáticamente según lo programador, pero el programador está desactivado de forma predeterminada. Puedes encontrar el nombre de la CloudWatch regla de Amazon para el programador en la	Arquitecto de nube, DevOps ingeniero y administrador de nube

Tarea	Descripción	Habilidades requeridas
	pestaña Recursos de la CloudFormation pila de la cuenta de destino. Para obtener instrucciones sobre cómo modificar la regla de CloudWatch eventos, consulte Eliminar o deshabilitar una regla de CloudWatch eventos en la CloudWatch documentación.	

Tarea	Descripción	Habilidades requeridas
Restaure su base de datos a cualquiera de las copias anteriores cuando sea necesario.	1. Abra la consola de Secrets Manager. 2. De la lista de secretos, elige el secreto que creaste con la CloudFormation plantilla anterior. Su aplicación usa el secreto para acceder a la base de datos del clúster de destino. 3. Para actualizar el valor secreto desde la página de detalles, en la sección Secret value (Valor del secreto), elija Retrieve secret value (Recupera r valor del secreto) y, a continuación, Edit (Editar). 4. Introduzca los detalles del punto de conexión de la base de datos.	Administrador de la nube, administrador de bases de datos, ingeniero DevOps

Recursos relacionados

- Réplicas de lectura de para diferentes regiones (documentación de Amazon RDS)
- Implementaciones azul/verdes (documentación de Amazon RDS)

Información adicional

Puedes usar el siguiente ejemplo de política para compartir tu información AWS KMS key . Cuentas de AWS

```
{
    "Version": "2012-10-17",
    "Id": "cross-account-rds-kms-key",
```

```
    "Statement": [
        {
            "Sid": "Enable user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<SourceAccount>:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow administration of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<DestinationAccount>:root"
            },
            "Action": [
                "kms:Create*",
                "kms:Describe*",
                "kms:Enable*",
                "kms:List*",
                "kms:Put*",
                "kms:Update*",
                "kms:Revoke*",
                "kms:Disable*",
                "kms:Get*",
                "kms:Delete*",
                "kms:ScheduleKeyDeletion",
                "kms:CancelKeyDeletion"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::<DestinationAccount>:root",
                    "arn:aws:iam::<SourceAccount>:root"
                ]
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
```

```
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey",
                "kms:CreateGrant"
            ],
            "Resource": "*"
        }
    ]
}
```

Automatice las tareas de bases de datos en SQL Server Express en Amazon EC2 mediante un programador AWS Lambda de tareas

Subhani Shaik, Amazon Web Services

Resumen

Este patrón muestra cómo programar y administrar las tareas de la base de datos en SQL Server Express Edition, que es la versión gratuita de SQL Server. Sin embargo, SQL Server Express Edition carece del servicio de agentes de SQL Server, que normalmente gestiona las operaciones automatizadas de las bases de datos. Este patrón explica cómo puede utilizar el Programador de tareas y AWS Lambda como alternativa para automatizar las tareas de bases de datos en la edición SQL Server Express que se ejecuta en una instancia de Amazon Elastic Compute Cloud (Amazon EC2).

El Programador de tareas es una utilidad integrada en el sistema Windows que facilita la ejecución automática de tareas rutinarias. Proporciona un mecanismo para programar y administrar las operaciones automatizadas, eliminando la necesidad de intervención manual en los procesos repetititvos. AWS Lambda es un servicio de computación sin servidor que ejecuta código automáticamente en respuesta a los eventos, sin necesidad de administrar la infraestructura subyacente.

Requisitos previos y limitaciones

Requisitos previos

- Una activa Cuenta de AWS
- Una nube privada virtual (VPC) creada con Amazon Virtual Private Cloud (Amazon VPC)
- Una instancia de Amazon EC2 con Windows Server
- Volúmenes de Amazon Elastic Block Store (Amazon EBS) adjuntos a una instancia de Amazon EC2 con Windows Server
- Elementos binarios de SQL Server Express Edition

Limitaciones

- Para obtener información sobre las limitaciones de las características de SQL Server Express Edition, consulte el sitio web de Microsoft.

- Algunos Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- SQL Server 2016 o posterior con SQL Server Express Edition

Arquitectura

En el siguiente diagrama se muestra una instancia de Amazon EC2 que se ejecuta con SQL Server Express Edition. Se puede acceder a la instancia a través del cliente de protocolo de escritorio remoto (RDP) o desde AWS Systems Manager Session Manager. AWS Key Management Service (AWS KMS) gestiona el cifrado de datos de los volúmenes de Amazon EBS para garantizar la data-at-rest seguridad. La infraestructura también incluye AWS Identity and Access Management (IAM), que proporciona control de acceso y administra los permisos para la ejecución de las funciones de Lambda. Amazon Simple Storage Service (Amazon S3) guarda las funciones de Lambda.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento de nivel de bloque para su uso con instancias de Amazon EC2.
- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Systems Manager Session Manageres una AWS Systems Manager herramienta totalmente gestionada. Con Session Manager, puede gestionar sus instancias de Amazon EC2, dispositivos perimetrales, servidores locales y máquinas virtuales (). VMs
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Otras herramientas

- Microsoft SQL Server Management Studio (SSMS) es una herramienta para administrar SQL Server, que incluye el acceso, la configuración y la administración de los componentes de SQL Server.
- Python es un lenguaje de programación informático de uso general. Puede usar esta herramienta para crear aplicaciones, automatizar tareas y desarrollar servicios en Nube de AWS.
- El Programador de tareas es una herramienta de Microsoft que puede usar para programar tareas rutinarias en su equipo automáticamente.

Prácticas recomendadas

- Prácticas recomendadas para Amazon EC2
- Prácticas recomendadas para trabajar con funciones AWS Lambda
- Security best practices in IAM (Prácticas recomendadas de seguridad en IAM)

Epics

Creación de una instancia de Amazon EC2 e instalación de SQL Server Express Edition

Tarea	Descripción	Habilidades requeridas
Implemente una instancia de Amazon EC2.	Para crear una instancia de Amazon EC2, abra la consola Amazon EC2 https://console.aws.amazon.com/ec2/en y	ADMINISTRADOR DE BASES DE DATOS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	seleccione una imagen de máquina de Amazon (AMI) de la lista de instancias disponibl es para Windows Server. Para obtener más información, consulte Lanzar una instancia de Amazon EC2 en la AWS documentación.	

Tarea	Descripción	Habilidades requeridas
Instale SQL Server Express Edition.	Para instalar SQL Server Express Edition, siga los pasos que se indican a continuación: 1. Para conectarse a su instancia de Amazon EC2, elija una opción: • Opción A: uso del protocolo de escritori o remoto (RDP). Para obtener instrucciones, consulte Conectarse a la instancia de Windows mediante un cliente RDP en la AWS documenta ción. • Opción B: utilice la consola Amazon EC2 y. AWS Systems Manager Session Manager Para obtener instrucciones, consulte Conectarse a su instancia de Amazon EC2 mediante Session Manager en la AWS documentación. 2. Para descargar la instancia de SQL Server Express Edition necesaria, vaya a Descargas de SQL Server en el sitio web de Microsoft. 3. Para instalar SQL Server Express Edition, siga las	ADMINISTRADOR DE BASES DE DATOS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	instrucciones de Planificación de una instalación de SQL Server en el sitio web de Microsoft.	

Creación de tareas automatizadas de mantenimiento de bases de datos

Tarea	Descripción	Habilidades requeridas
Identifique las tareas rutinarias.	Identifique las tareas rutinarias que desea automatizar. Por ejemplo, las siguientes tareas pueden automatizarse: • Copias de seguridad de bases de datos (registro completo, diferencial y de transacciones) • Mantenimiento y reorganización de índices • Actualizaciones de estadísticas • Operaciones específicas para cada aplicación • Limpieza o archivado de datos	Administrador de base de datos
Preparación de scripts de SQL	Para preparar scripts de SQL, siga los pasos que se detallan a continuación: 1. Cree consultas de SQL para cada tarea de mantenimiento. A continuac	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	ión, tiene un ejemplo de consulta de T-SQL para realizar una copia de seguridad de una base de datos específica: `Backup Database <Database_Name> To Disk='C:\Backups\Database_Name.bak'` 2. Guarde el archivo de script como `<File Name>.sql`. A continuación, guarde los scripts en una ubicación accesible de la unidad local del servidor, en la instancia de Amazon EC2 o en un recurso compartido de archivos de red.	

Tarea	Descripción	Habilidades requeridas
Configuración de permisos de acceso	Para configurar permisos de acceso, haga lo siguiente: 1. Configure los permisos adecuados del sistema de archivos. Para obtener instrucciones, consulte Configuración de los permisos del sistema de archivos para el acceso al motor de la base de datos en el sitio web de Microsoft. 2. Compruebe que la cuenta de servicio de SQL Server tenga el acceso necesario. Para obtener instrucciones, consulte Configuración de cuentas de servicio y permisos de Windows en el sitio web de Microsoft. 3. Compruebe la conectividad de red de los recursos compartidos remotos. Para obtener más información, consulte Acceder a los datos mediante recursos compartidos de archivos en la AWS documentación.	Administrador de base de datos

Automatización de las tareas con el Programador de tareas

Tarea	Descripción	Habilidades requeridas

Cree archivos por lotes.	• Para crear un archivo por lotes, utilice un editor de texto para escribir el siguiente comando. Sustituya los parámetros `username` y `password` por sus propios valores. A continuación, guarde el archivo como `<Name>.bat` .
	
	`sqlcmd -S servername -U username -P password -i <T-SQL query path.sql>`
	
	• Para crear un archivo por lotes para tareas de SQL, utilice un editor de texto y escriba los siguientes comandos. Sustituya los parámetros `ServerName` , `DatabaseName` , `username` y `password` por sus propios valores. A continuación, guarde el archivo como `<Name>.bat` .
	
	`@echo off`
	`sqlcmd -S [ServerName] -d [Database`
		AWS DevOps, DBA

Tarea	Descripción	Habilidades requeridas
	`Name] -U username -P password -i "PathToSQLScript\Script.sql" -o "PathToOutput\Output.txt"`	

Tarea	Descripción	Habilidades requeridas
Cree tareas en el Programad or de tareas.	Para crear una tarea en el Programador de tareas, siga estos pasos: 1. Para abrir el Programador de tareas, escriba taskschd. msc en la búsqueda de Windows. 2. Seleccione el menú de acción y, a continuación, seleccione Crear tarea básica. 3. En Nombre, proporcione un nombre para la tarea y, a continuación, elija Siguiente . 4. En Desencadenador, seleccione la opción según la cual quiere que comience la tarea y, a continuación, elija Siguiente. 5. Proporcione la informaci ón de inicio u repetición de la tarea y, a continuación, seleccione Siguiente. 6. En la sección Acción, seleccione Iniciar un programa y, a continuación, seleccione Siguiente. 7. En Programa/script, especifique la ruta del archivo por lotes que creó en la tarea anterior y, a	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	continuación, elija Siguiente . 8. Seleccione Finalizar. Para ejecutar la tarea manualmente, haga clic con el botón derecho en la tarea recién creada y, a continuac ión, seleccione Ejecutar.	
Consulte el estado de la tarea.	Para ver el estado de una tarea en el Programador de tareas, siga estos pasos: 1. En el programador de tareas, vaya a la biblioteca del Programador de tareas, que muestra todas las tareas. 2. Para ver el estado de la tarea que creó anteriorm ente, selecciónela y, a continuación, vaya a la pestaña Historial.	ADMINISTRADOR DE BASES DE DATOS, AWS DevOps

Automatice las tareas con AWS Lambda

Tarea	Descripción	Habilidades requeridas
Implemente la solución.	Para implementar la solución de este patrón, siga los pasos que se describen a continuac ión:	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	1. Creación de una función de Lambda. Para obtener instrucciones, consulte Crear su primera función Lambda en la AWS documentación. 2. Programación de la función de Lambda. Para obtener instrucciones, consulte Invocar una función Lambda según un cronograma en AWS la documentación. 3. Ejecute consultas de T-SQL. Para obtener más información, consulte el tutorial: Uso de una función Lambda para acceder a una base de datos de Amazon RDS en la documentación. AWS El tutorial explica cómo conectar bases de datos de Amazon RDS desde funciones de Lambda para ejecutar consultas de SQL.	

Resolución de problemas

Problema	Solución
Problemas con Lambda	Para obtener ayuda con los errores y problemas que pueda encontrar al usar Lambda AWS Lambda, consulte Solución de

Problema	Solución
	problemas en Lambda en la AWS documentación.

Recursos relacionados

- Tipos de instancias de Amazon EC2
- AWS Lambda documentación
- AWS Lambda precios
- Programador de tareas para desarrolladores (sitio web de Microsoft)

Automatización de la conmutación por error y la conmutación por recuperación entre regiones mediante DR Orchestrator Framework

Jitendra Kumar, Pavithra Balasubramanian y Oliver Francis, Amazon Web Services

Resumen

Este patrón describe cómo utilizar DR Orchestrator Framework para orquestar y automatizar los pasos manuales que san propensos a errores, para realizar la recuperación ante desastres en todas las regiones de Amazon Web Services (AWS). El patrón cubre las siguientes bases de datos:

- Amazon Relational Database Service (Amazon RDS) para MySQL, Amazon RDS para PostgreSQL o Amazon RDS para MariaDB
- Edición compatible de Amazon Aurora MySQL o de Amazon Aurora PostgreSQL (mediante un archivo centralizado)
- Amazon ElastiCache (Redis OSS)

Para demostrar la funcionalidad de DR Orchestrator Framework, debe crear dos instancias o clústeres de bases de datos. El principal está en y Región de AWS `us-east-1` el secundario está dentro. `us-west-2` Para crear estos recursos, utilice las AWS CloudFormation plantillas de la `App-Stack` carpeta del GitHub repositorio aws-cross-region-dr-databases.

Requisitos previos y limitaciones

Requisitos previos generales

- El marco DR Orchestrator se implementó tanto en el sistema primario como en el secundario Regiones de AWS
- Dos buckets de Amazon Simple Storage Service
- Una nube privada virtual (VPC) con dos subredes y un grupo de seguridad AWS

Requisitos previos específicos del motor

- Amazon Aurora: debe haber al menos una base de datos global de Aurora disponible en dos Regiones de AWS. Puede utilizar `us-east-1` como región principal y `us-west-2` como región secundaria.

- Amazon ElastiCache (Redis OSS): un almacén de datos ElastiCache global debe estar disponible en dos. Regiones de AWS Puede usar `use us-east-1` como región principal y `us-west-2` como región secundaria.

Limitaciones de Amazon RDS

- DR Orchestrator Framework no comprueba el retraso de la replicación antes de realizar una conmutación por error o una conmutación por recuperación. El retraso de la replicación debe comprobarse manualmente.
- Esta solución se probó con una instancia de base de datos principal con una réplica de lectura. Si desea utilizar más de una réplica de lectura, pruebe la solución minuciosamente antes de implementarla en un entorno de producción.

Limitaciones de Aurora

- La disponibilidad de las características varía según las versiones específicas de cada motor de base de datos y entre Regiones de AWS. Para más información sobre la disponibilidad en características y regiones de la replicación entre regiones, consulte Réplicas de lectura entre regiones.
- Las bases de datos globales de Aurora tienen requisitos de configuración específicos para las clases de instancias de base de datos Aurora compatibles y el número máximo de Regiones de AWS. Para más información, consulte Requisitos de configuración de una base de datos global de Amazon Aurora.
- Esta solución se probó con una instancia de base de datos principal con una réplica de lectura. Si desea utilizar más de una réplica de lectura, pruebe la solución minuciosamente antes de implementarla en un entorno de producción.

ElastiCache Limitaciones

- Para obtener información sobre la disponibilidad regional del almacén de datos global y los requisitos de ElastiCache configuración, consulte los requisitos previos y las limitaciones en la documentación. ElastiCache

Versiones de productos de Amazon RDS

Amazon RDS es compatible con las siguientes versiones de motor:

- MySQL: Amazon RDS admite instancias de base de datos que ejecutan las siguientes versiones de MySQL: MySQL 8.0 y MySQL 5.7.
- PostgreSQL: para obtener información sobre las versiones compatibles de Amazon RDS para PostgreSQL, consulte Versiones de bases de datos disponibles de PostgreSQL.
- MariaDB: Amazon RDS admite instancias de base de datos que ejecutan las siguientes versiones de MariaDB:
  - MariaDB 10.11
  - MariaDB 10.6
  - MariaDB 10.5

Versiones de productos de Aurora

- La transición de base de datos global de Amazon Aurora requiere una instancia de Aurora MySQL que sea compatible con MySQL 5.7 o la versión 2.09.1 y superior.

  Para más información, consulte Limitaciones de bases de datos globales de Amazon Aurora.

ElastiCache Versiones de productos (Redis OSS)

Amazon ElastiCache (Redis OSS) es compatible con las siguientes versiones de Redis:

- Redis 7.1 (mejorada)
- Redis 7.0 (mejorada)
- Redis 6.2 (mejorada)
- Redis 6.0 (mejorada)
- Redis 5.0.6 (mejorada)

Para obtener más información, consulte Versiones compatibles ElastiCache (Redis OSS).

Arquitectura

Arquitectura de Amazon RDS

La arquitectura de Amazon RDS incluye los siguientes recursos:

- La instancia de base de datos de Amazon RDS principal creada en la región principal (`us-east-1`) con read/write acceso para los clientes

- Una réplica de lectura de Amazon RDS creada en la región secundaria (`us-west-2`) con acceso de solo lectura para los clientes
- DR Orchestrator Framework se implementó tanto en la región principal como en la secundaria

En el diagrama se muestra lo siguiente:

1. Replicación asíncrona entre la instancia principal y la instancia secundaria
2. Acceso de lectura y escritura para los clientes de la región principal
3. Acceso de solo lectura para los clientes de la región secundaria

Arquitectura de Aurora

La arquitectura de Amazon Aurora incluye los siguientes recursos:

- El clúster de base de datos principal de Aurora creado en la región principal (`us-east-1`) con un punto de conexión de escritura activo
- Un clúster de base de datos de Aurora creado en la región secundaria (`us-west-2`) con un punto de conexión de escritura inactivo
- DR Orchestrator Framework se implementó tanto en la región principal como en la secundaria

En el diagrama se muestra lo siguiente:

1. Replicación asíncrona entre el clúster principal y el clúster secundario
2. El clúster de base de datos principal con un punto de conexión de escritura activo
3. El clúster de base de datos secundario con un punto de conexión de escritura inactivo

ElastiCache Arquitectura (Redis OSS)

La arquitectura Amazon ElastiCache (Redis OSS) incluye los siguientes recursos:

- Un almacén de datos global ElastiCache (Redis OSS) creado con dos clústeres:
  1. El clúster principal de la región principal (`us-east-1`)

2. El clúster secundario de la región secundaria (`us-west-2`)

- Un enlace entre regiones de Amazon con encriptado TLS 1.2 entre los dos clústeres
- DR Orchestrator Framework se implementó tanto en la región principal como en la secundaria

Automatización y escala

DR Orchestrator Framework es escalable y admite la conmutación por error o la conmutación por recuperación de más de una base de datos AWS en paralelo.

Puede utilizar el siguiente código de carga útil para realizar la conmutación por error de varias AWS bases de datos de su cuenta. En este ejemplo, tres AWS bases de datos (dos bases de datos globales, como Aurora MySQL o Aurora PostgreSQL, y una instancia de Amazon RDS for MySQL) se conmutan por error a la región DR:

```
{
  "StatePayload": [
    {
      "layer": 1,
      "resources": [
        {
          "resourceType": "PlannedFailoverAurora",
          "resourceName": "Switchover (planned failover) of Amazon Aurora global
 databases (MySQL)",
          "parameters": {
            "GlobalClusterIdentifier": "!Import dr-globaldb-cluster-mysql-global-
identifier",
            "DBClusterIdentifier": "!Import dr-globaldb-cluster-mysql-cluster-
identifier"
          }
        },
        {
          "resourceType": "PlannedFailoverAurora",
          "resourceName": "Switchover (planned failover) of Amazon Aurora global
 databases (PostgreSQL)",
          "parameters": {
            "GlobalClusterIdentifier": "!Import dr-globaldb-cluster-postgres-global-
identifier",
            "DBClusterIdentifier": "!Import dr-globaldb-cluster-postgres-cluster-
identifier"
```

```
          }
        },
        {
          "resourceType": "PromoteRDSReadReplica",
          "resourceName": "Promote RDS for MySQL Read Replica",
          "parameters": {
            "RDSInstanceIdentifier": "!Import rds-mysql-instance-identifier",
            "TargetClusterIdentifier": "!Import rds-mysql-instance-global-arn"
          }
        }
      ]
    }
  ]
}
```

Tools (Herramientas)

AWS servicios

- Amazon Aurora es un motor de base de datos relacional completamente administrado diseñado para la nube y compatible con MySQL y PostgreSQL.
- Amazon le ElastiCache ayuda a configurar, gestionar y escalar los entornos de caché en memoria distribuidos en. Nube de AWS Este patrón usa Amazon ElastiCache (Redis OSS).
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice. En este patrón, las funciones Lambda se utilizan AWS Step Functions para realizar los pasos.
- Amazon Relational Database Service (Amazon RDS) lo ayuda a configurar, utilizar y escalar una base de datos relacional en la Nube de AWS. Este patrón admite Amazon RDS para MySQL, Amazon RDS para PostgreSQL y Amazon RDS para MariaDB.
- AWS SDK para Python (Boto3)le ayuda a integrar su aplicación, biblioteca o script de Python con Servicios de AWS. En este patrón, los Boto3 APIs se utilizan para comunicarse con las instancias de la base de datos o las bases de datos globales.
- AWS Step Functionses un servicio de organización sin servidor que le ayuda a combinar AWS Lambda funciones y otras Servicios de AWS para crear aplicaciones críticas para la empresa. En este patrón, las máquinas de estado Step Functions se utilizan para organizar y ejecutar la

conmutación por error y la conmutación por recuperación entre regiones de las instancias de bases de datos o las bases de datos globales.

Repositorio de código

El código de este patrón está disponible en el repositorio -databases deaws-cross-region-dr. GitHub

Epics

Instalación de DR Orchestrator Framework

Tarea	Descripción	Habilidades requeridas
Clona el GitHub repositorio.	Para clonar el repositorio, ejecute el siguiente comando: `git clone https://github.com/aws-samples/aws-cross-region-dr-databases.git`	AWS DevOps, administrador de AWS

Comprima el código de las funciones de Lambda en un archivo .zip.	Cree los archivos de almacenamiento de las funciones de Lambda para incluir las dependencias de DR Orchestrator Framework:
	`cd <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts`
	
	`bash scripts/deploy-orchestrator-sh.sh`
		Administrador de AWS

Cree los buckets de S3.	Los buckets de S3 son necesarios para almacenar DR Orchestrator Framework junto con la configuración más reciente. Cree dos buckets de	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	S3, uno en la región principal (`us-east-1`) y otro en la región secundaria (`us-west-2`): • `dr-orchestrator-xxxxxx-us-east-1` • `dr-orchestrator-xxxxxx-us-west-2` Sustituya `xxxxxx` por un valor aleatorio para que los nombres de los buckets sean únicos.	
Cree subredes y grupos de seguridad.	Tanto en la región principal (`us-east-1`) como en la región secundaria (`us-west-2`), cree dos subredes y un grupo de seguridad para la implementación de la función de Lambda en la VPC: • `subnet-XXXXXXX` • `subnet-YYYYYYY` • `sg-XXXXXXXXXXX`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Actualice los archivos de parámetros de DR Orchestrator.	En la carpeta <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts/cloudformation , actualice los siguientes archivos de parámetros de DR Orchestrator: • Orchestrator-Deployer-parameters-us-east-1.json • Orchestrator-Deployer-parameters-us-west-2.json Utilice los siguientes valores de parámetros, sustituyendo x y y por los nombres de sus recursos: [{ "ParameterKey": "TemplateStoreS3BucketName", "ParameterValue": "dr-orchestrator-xxxxxx-us-east-1" }, { "ParameterKey": "TemplateVPCId", "ParameterValue": "vpc-xxxxxx" }, {	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	"ParameterKey": "TemplateLambdaSubnetID1", "ParameterValue": "subnet-xxxxx" }, { "ParameterKey": "TemplateLambdaSubnetID2", "ParameterValue": "subnet-yyyyy" }, { "ParameterKey": "TemplateLambdaSecurityGroupID", "ParameterValue": "sg-xxxxxxxxxx" }]	

Tarea	Descripción	Habilidades requeridas
Cargue el código de DR Orchestrator Framework en el bucket de S3.	El código estará más seguro en un bucket de S3 que en el directorio local. Cargue el directorio `DR-Orchestration-artifacts`, incluidos todos los archivos y subcarpetas, en los buckets de S3. Para cargar el código, haga lo siguiente: 1. Inicie sesión en Consola de administración de AWS. 2. Vaya a la consola de Amazon S3. 3. Seleccione la `dr-orchestrator-xxxxxx-us-east-1 bucket`. 4. Elija la carpeta Upload (Cargar) y Add folder (Añadir carpeta). 5. Seleccione la carpeta `DR-Orchestration-artifacts`. 6. Seleccione Cargar. 7. Seleccione el bucket `dr-orchestrator-xxxxxx-us-west-2`. 8. Repita los pasos 4 a 7.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

Implemente DR Orchestrator Framework en la región principal.	Para implementar DR Orchestrator Framework en la región principal (`us-east-1`), ejecute los siguientes comandos:
	`cd <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts/cloudformation`
	
	`aws cloudformation deploy \`
	`--region us-east-1 \`
	`--stack-name dr-orchestrator \`
	`--template-file Orchestrator-Deployer.yaml \`
	`--parameter-overrides file://Orchestrator-Deployer-parameters-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
		Administrador de AWS

Tarea	Descripción	Habilidades requeridas

Implemente DR Orchestrator Framework en la región secundaria.	En la región secundaria (`us-west-2`), ejecute los siguientes comandos:
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts/cloudformation`
	
	`aws cloudformation deploy \`
	`--region us-west-2 \`
	`--stack-name dr-orchestrator \`
	`--template-file Orchestrator-Deployer.yaml \`
	`--parameter-overrides file://Orchestrator-Deployer-parameters-us-west-2.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
		Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Comprobar la implementación.	Si el CloudFormation comando se ejecuta correctamente, devuelve el siguiente resultado: `Successfully created/updated stack - dr-orchestrator` Como alternativa, puede ir a la CloudFormation consola y verificar el estado de la `dr-orchestrator` pila.	Administrador de AWS

Creación de instancias o clústeres de bases de datos

Tarea	Descripción	Habilidades requeridas
Cree las subredes y los grupos de seguridad de base de datos.	En su VPC, cree dos subredes y un grupo de seguridad para la instancia de base de datos o la base de datos global en las regiones principal (`us-east-1`) y secundaria (`us-west-2`): • `subnet-XXXXXX` • `subnet-XXXXXX` • `sg-XXXXXXXXXX`	Administrador de AWS
Actualice el archivo de parámetros de la instancia o el clúster de la base de datos principal.	En la carpeta `<YOUR LOCAL GIT FOLDER>/App-Stack`, actualice el archivo	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	de parámetros de la región principal. Amazon RDS En el archivo `RDS-MySQL-parameter-us-east-1.json`, actualice `SubnetIds` y `DBSecurityGroup` con los nombres de los recursos que creó: `{ "Parameters": { "SubnetIds": "subnet-xxxxxx,subnet-xxxxxx", "DBSecurityGroup": "sg-xxxxxxxxxx", "MySqlGlobalIdentifier":"rds-mysql-instance", "InitialDatabaseName": "mysqldb", "DBPortNumber": "3789", "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2", "KMSKeyAliasName": "rds/rds-mysql-instance-KmsKeyId" } }` Amazon Aurora	

Tarea	Descripción	Habilidades requeridas

	En el archivo `Aurora-MySQL-parameter-us-east-1.json` , actualice `SubnetIds` y `DBSecurityGroup` con los nombres de los recursos que creó:
	
	`{`
	`  "Parameters": {`
	`  "SubnetIds": "subnet1-xxxxxx,subnet2-xxxxxx",`
	`  "DBSecurityGroup": "sg-xxxxxxxxxx",`
	`  "GlobalClusterIdentifier":"dr-globaldb-cluster-mysql",`
	`  "DBClusterName":"dbcluster-01",`
	`  "SourceDBClusterName":"dbcluster-02",`
	`  "DBPortNumber": "3787",`
	`  "DBInstanceClass": "db.r5.large",`
	`  "InitialDatabaseName": "sampledb",`
	`  "PrimaryRegion": "us-east-1",`
	`  "SecondaryRegion": "us-west-2",`
	`  "KMSKeyAliasName": "rds/dr-globaldb-cluster-mysql-KmsKeyId"`
	`  }`
	`}`
	
	Amazon ElastiCache (Redis OSS)	

Tarea	Descripción	Habilidades requeridas
	En el archivo `ElastiCache-parameter-us-east-1.json`, actualice `SubnetIds` y `DBSecurityGroup` con los nombres de los recursos que creó. `{ "Parameters": { "CacheNodeType": "cache.m5.large", "DBSecurityGroup": "sg-xxxxxxxxxx", "SubnetIds": "subnet-xxxxxx,subnet-xxxxxx", "EngineVersion": "5.0.6", "GlobalReplicationGroupIdSuffix": "demo-redis-global-datastore", "NumReplicas": "1", "NumShards": "1", "ReplicationGroupId": "demo-redis-cluster", "DBPortNumber": "3788", "TransitEncryption": "true", "KMSKeyAliasName": "elasticache/demo-redis-global-datastore-KmsKeyId", "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2" }`	

Tarea	Descripción	Habilidades requeridas
	}	

Tarea	Descripción	Habilidades requeridas

Implemente su instancia o clúster de base de datos en la región principal.	Para implementar la instancia o el clúster en la región principal (`us-east-1`), ejecute los siguientes comandos en función del motor de base de datos.
	
	Amazon RDS
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-east-1 \`
	`--stack-name rds-mysql-app-stack \`
	`--template-file RDS-MySQL-Primary.yaml \`
	`--parameter-overrides file://RDS-MySQL-parameter-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
	
	Amazon Aurora
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-east-1 \`
		Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	`--stack-name aurora-mysql-app-stack \`
	`--template-file Aurora-MySQL-Primary.yaml \`
	`--parameter-overrides file://Aurora-MySQL-parameter-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
	
	Amazon ElastiCache (Redis OSS)
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-east-1 --stack-name elasticache-ds-app-stack \`
	`--template-file ElastiCache-Primary.yaml \`
	`--parameter-overrides file://ElastiCache-parameter-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`	

Tarea	Descripción	Habilidades requeridas
	Compruebe que los CloudFormation recursos se han desplegado correctam ente.	

Tarea	Descripción	Habilidades requeridas
Actualice el archivo de parámetros de la instancia o el clúster de la base de datos secundaria.	En la carpeta `<YOUR LOCAL GIT FOLDER>/App-Stack`, actualice el archivo de parámetros de la región secundaria. Amazon RDS En el archivo `RDS-MySQL-parameter-us-west-2.json` , actualice `SubnetIDs` y `DBSecurityGroup` con los nombres de los recursos que creó. Actualice el valor `PrimaryRegionKMSKeyArn` con el valor `MySQLKmsKeyId` obtenido de la sección de resultados de la CloudFormation pila de la instancia de base de datos principal: `{ "Parameters": { "SubnetIds": "subnet-aaaaaaaaa, subnet-bbbbbbbbb", "DBSecurityGroup": "sg-ccccccccc", "MySqlGlobalIdentifier":"rds-mysql-instance", "InitialDatabaseName": "mysqldb", "DBPortNumber": "3789", "PrimaryRegion": "us-east-1",`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	"SecondaryRegion": "us-west-2", "KMSKeyAliasName": "rds/rds-mysql-instance-KmsKeyId", "PrimaryRegionKMSKeyArn":"arn:aws:kms:us-east-1:xxxxxxxxx:key/mrk-xxxxxxxxxxxxxxxxx" } } Amazon Aurora En el archivo `Aurora-MySQL-parameter-us-west-2.json`, actualice `SubnetIDs` y `DBSecurityGroup` con los nombres de los recursos que creó. Actualice el valor `PrimaryRegionKMSKeyArn` con el valor `AuroraKmsKeyId` tomado de la sección de salidas de la CloudFormation pila de la instancia de base de datos principal: { "Parameters": { "SubnetIds": "subnet1-aaaaaaaaa,subnet2-bbbbbbbbb", "DBSecurityGroup": "sg-ccccccccc", "GlobalClusterIdentifier":"dr-globaldb-cluster-mysql",	

Tarea	Descripción	Habilidades requeridas

	<pre>"DBClusterName":"dbcluster-01",
	"SourceDBClusterName":"dbcluster-02",
	"DBPortNumber": "3787",
	"DBInstanceClass": "db.r5.large",
	"InitialDatabaseName": "sampledb",
	"PrimaryRegion": "us-east-1",
	"SecondaryRegion": "us-west-2",
	"KMSKeyAliasName": "rds/dr-globaldb-cluster-mysql-KmsKeyId"
	}
	}</pre>
	Amazon ElastiCache (Redis OSS)
	
	En el archivo `ElastiCache-parameter-us-west-2.json`, actualice `SubnetIDs` y `DBSecurityGroup` con los nombres de los recursos que creó. Actualice el valor `PrimaryRegionKMSKeyArn` con el valor `ElastiCacheKmsKeyId` obtenido de la sección de resultados de la CloudFormation pila de la instancia de base de datos principal:	

Tarea	Descripción	Habilidades requeridas

	{
	  "Parameters": {
	  "CacheNodeType": "cache.m5.large",
	  "DBSecurityGroup": "sg-ccccccccc",
	  "SubnetIds": "subnet-aaaaaaaaa, subnet-bbbbbbbbb",
	  "EngineVersion": "5.0.6",
	  "GlobalReplicationGroupIdSuffix": "demo-redis-global-datastore",
	  "NumReplicas": "1",
	  "NumShards": "1",
	  "ReplicationGroupId": "demo-redis-cluster",
	  "DBPortNumber": "3788",
	  "TransitEncryption": "true",
	  "KMSKeyAliasName": "elasticache/demo-redis-global-datastore-KmsKeyId",
	  "PrimaryRegion": "us-east-1",
	  "SecondaryRegion": "us-west-2"
	  }
	}	

Tarea	Descripción	Habilidades requeridas

Implemente su instancia o clúster de base de datos en la región secundaria.	Ejecute los siguientes comandos, en función del motor de base de datos.
	
	Amazon RDS
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-west-2 \`
	`--stack-name rds-mysql-app-stack \`
	`--template-file RDS-MySQL-DR.yaml \`
	`--parameter-overrides file://RDS-MySQL-parameter-us-west-2.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
	
	Amazon Aurora
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-west-2 \`
	`--stack-name aurora-mysql-app-stack \`
	`--template-file Aurora-MySQL-DR.yaml \`
		Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	`--parameter-overrides file://Aurora-MySQL-parameter-us-west-2.json \ --capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \ --disable-rollback`
	
	Amazon ElastiCache (Redis OSS)
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \ --region us-west-2 \ --stack-name elasticache-ds-app-stack \ --template-file ElastiCache-DR.yaml \ --parameter-overrides file://ElastiCache-parameter-us-west-2.json \ --capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \ --disable-rollback`
	
	Compruebe que los CloudFormation recursos se han desplegado correctamente.	

Recursos relacionados

- Estrategia de recuperación ante desastres para bases de datos en AWS vigor (estrategia de orientación AWS prescriptiva)
- Automatice su solución de recuperación ante desastres para bases de datos relacionales en AWS(guía de orientación AWS prescriptiva)
- Uso de bases de datos globales de Amazon Aurora
- Replicación Regiones de AWS mediante el uso de almacenes de datos globales
- Automatice su solución de recuperación ante desastres para bases de datos relacionales en AWS(guía de orientación AWS prescriptiva)

Realice copias de seguridad automáticas de las bases de datos de SAP HANA mediante Systems Manager y EventBridge

Ambarish Satarkar y Gaurav Rath, Amazon Web Services

Resumen

Este patrón describe cómo automatizar las copias de seguridad de bases de datos de SAP HANA mediante AWS Systems Manager EventBridge, Amazon, Amazon Simple Storage Service (Amazon S3) y AWS Backint Agent para SAP HANA.

Este patrón proporciona un enfoque basado en script de intérprete de comandos utilizando el comando `BACKUP DATA` y elimina la necesidad de mantener scripts y configuraciones de trabajo para cada instancia de sistema operativo (OS) a través de numerosos sistemas.

Nota: En abril de 2023, AWS Backup anunció la compatibilidad con las bases de datos de SAP HANA en Amazon Elastic Compute Cloud (Amazon EC2). Para obtener más información, consulte la copia de seguridad de bases de datos de SAP HANA en EC2 instancias de Amazon.

Según las necesidades de su organización, puede utilizar el servicio AWS Backup para hacer copias de seguridad automáticas de sus bases de datos de SAP HANA o puede utilizar este patrón.

Requisitos previos y limitaciones

Requisitos previos

- Una instancia de SAP HANA existente con una versión compatible en estado de ejecución en una instancia gestionada de Amazon Elastic Compute Cloud (Amazon EC2) configurada para Systems Manager
- Debe contar con la versión 2.3.274.0 de Systems Manager Agent (Agente de SSM) instalada o una posterior
- Un bucket de S3 que no tiene habilitado el acceso público
- Una clave `hdbuserstore` llamada `SYSTEM`
- Un rol de IAM de AWS Identity and Access Management para que el manual de procedimientos se ejecute según lo programado

- Las políticas `AmazonSSMManagedInstanceCore` y `ssm:StartAutomationExecution` están asociadas al rol de servicio de automatización de Systems Manager.

Limitaciones

- AWS Backint Agent para SAP HANA no admite la deduplicación.
- AWS Backint Agent para SAP HANA no admite la compresión de datos.

Versiones de producto

AWS Backint Agent es compatible con los siguientes sistemas operativos:

- SUSE Linux Enterprise Server
- SUSE Linux Enterprise Server para SAP
- Red Hat Enterprise Linux para SAP

AWS Backint Agent es compatible con las siguientes bases de datos:

- SAP HANA 1.0 SP12 (nodo único y varios nodos)
- SAP HANA 2.0 y versiones posteriores (nodo único y varios nodos)

Arquitectura

Pila de tecnología de destino

- AWS Backint Agent
- Amazon S3
- AWS Systems Manager
- Amazon EventBridge
- SAP HANA

Arquitectura de destino

En el siguiente diagrama se muestran los scripts de instalación que instalan AWS Backint Agent, el bucket S3 y Systems Manager EventBridge, y que utilizan un documento de comandos para programar copias de seguridad periódicas.

Automatización y escala

- Se pueden instalar varios AWS Backint Agents mediante un manual de procedimientos de Systems Manager Automation.
- Cada ejecución del manual de procedimientos de Systems Manager puede escalarse hasta un número n de instancias de SAP HANA, en función de la selección de objetivos.
- EventBridge puede automatizar las copias de seguridad de SAP HANA.

Tools (Herramientas)

- AWS Backint Agent para SAP HANA es una aplicación independiente que se integra con sus flujos de trabajo existentes para hacer copias de seguridad de la base de datos de SAP HANA en un bucket de S3 que especifique en el archivo de configuración. AWS Backint Agent admite copias de seguridad completas, incrementales y diferenciales de bases de datos de SAP HANA. Se ejecuta en un servidor de bases de datos SAP HANA, donde las copias de seguridad y los catálogos se transfieren de la base de datos de SAP HANA a AWS Backint Agent.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que puede utilizar para conectar sus aplicaciones con datos de diversas fuentes. EventBridge ofrece un flujo de datos en tiempo real desde sus aplicaciones, aplicaciones de software como servicio (SaaS) y servicios de AWS a objetivos como las funciones de AWS Lambda, los puntos de enlace de invocación HTTP que utilizan destinos de API o los buses de eventos de otras cuentas.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web.
- AWS Systems Manager le ayuda a ver y controlar la infraestructura en AWS. Mediante la consola de Systems Manager, puede ver los datos operativos de varios servicios de AWS y automatizar las tareas operativas en sus recursos de AWS.

Código

El código de este patrón está disponible en el repositorio. aws-backint-automated-backup GitHub

Epics

Cree un SISTEMA de claves hdbuserstore

Tarea	Descripción	Habilidades requeridas

Cree una clave hdbuserstore.	1. Vaya a `/usr/sap/<SID>/HDB<Inst No>/exe`.
	2. Ejecute el siguiente comando, con XX como número instancia de la base de datos SAP HANA.
	`hdbuserstore -i set SYSTEM <hostname>:3XX13@SYSTEMDB SYSTEM`
	Por ejemplo, para un host de SAP HANA `saphanadb` con número de instancia `00`, ejecute el siguiente comando.
	`hdbuserstore -i set SYSTEM saphanadb:30013@SYSTEMDB SYSTEM`
		Administrador de AWS, administrador de SAP HANA

Instalación de AWS Backint Agent

Tarea	Descripción	Habilidades requeridas
Instalación de AWS Backint Agent.	Siga las instrucciones de Instalación y configuración de AWS Backint Agent para SAP	Administrador de AWS, administrador de SAP HANA

Tarea	Descripción	Habilidades requeridas
	HANA en la documentación de AWS Backint Agent.	

Cree un documento de comandos de Systems Manager

Tarea	Descripción	Habilidades requeridas
Cree un documento de comandos de Systems Manager.	1. Inicie sesión en la consola de administración de AWS y abra la consola de AWS Systems Manager. 2. Seleccione Documents (Documentos) y seleccione Owned by me (De mi propiedad). 3. Confirme que se encuentra en la misma región de AWS que su base de datos de SAP HANA. 4. Seleccione Create document (Crear documento), Command or session (Comando o sesión) para crear su documento. 5. Utilice un nombre único y descriptivo, sin espacios (por ejemplo, SAP HANA-Backup). 6. Asegúrese de que el Document type (Tipo de documento) esté configurado como Command	Administrador de AWS, administrador de SAP HANA

Tarea	Descripción	Habilidades requeridas
	document (Documento de comando). 7. En el encabezado de Content (Contenido), hay un código de ejemplo. Asegúrese de elegir el tipo de código JSON y sustituya el código por el código del `HDB_Backup_SSM_Document.json` archivo del GitHub repositorio. 8. Elija Create document (Crear documento). 9. Consulte su documento en la sección De mi propiedad.	

Programe las copias de seguridad con una frecuencia periódica

Tarea	Descripción	Habilidades requeridas
Programa copias de seguridad periódicas con Amazon EventBridge.	1. Abre la EventBridge consola de Amazon, selecciona Rules y selecciona Create rule. 2. En la pantalla Define rule detail (Definir detalles de la regla), introduzca un nombre y una descripción únicos para la regla y utilice el bus de eventos predeterminado. 3. En Rule type (Tipo de regla), seleccione Schedule	Administrador de AWS, administrador de SAP HANA

Tarea	Descripción	Habilidades requeridas
	(Programar) y, a continuación, Next (Siguiente). 4. En la pantalla Define schedule (Definir programación), elija el patrón de programación apropiado y la expresión cron o expresión de frecuencia en función de la frecuencia requerida. 5. En la pantalla Select targets (Seleccionar destinos), en Target type (Tipo de destino), elija AWS service (Servicio de AWS). En Select a target (Seleccione un destino), elija Systems Manager Run Command. 6. Elija el documento que creó anteriormente. 7. En Target key (Clave de destino) y Target value (Valor objetivo), proporcione el ID de la instancia. Puede utilizar nombres y valores de etiquetas para agregar varias instancias. 8. En Configure automation parameters (Configurar los parámetros de automatización), seleccione Constant (Constante) para las copias de seguridad incrementales o diferenciales. Si desea	

Tarea	Descripción	Habilidades requeridas
	una copia de seguridad completa, seleccione No Parameters (Sin parámetros).	
	9. Elija si desea crear una nueva función o utilizar una función existente. Si utiliza un rol existente, asegúrese de que tenga las políticas necesarias para invocar el objetivo.	
	10. Conserve la configuración adicional predeterminada y seleccione Next (Siguiente).	
	11. La pantalla Configure tags (Configurar etiquetas) es opcional. Elija Next (Siguiente).	
	12. En la pantalla Review and create (Revisar y crear), revise la configuración de la regla y seleccione Create (Crear). La regla debe crearse correctamente.	
	Puede verificar el éxito de la copia de seguridad desde la ruta del bucket de S3. `s3:/<your_bucket_name>/<target folder>/<SID>/usr/sap/<SID>/SYS/global/hdb/backint/DB_<SID>/`	

Tarea	Descripción	Habilidades requeridas
	También puede verificar las copias de seguridad desde el catálogo de copias de seguridad de SAP HANA.	

Recursos relacionados

- AWS Backint Agent para SAP HANA
- Instalación y configuración de AWS Backint Agent para SAP HANA

Generación automática de un modelo de PynamoDB y funciones CRUD para Amazon DynamoDB mediante una aplicación de Python

Vijit Vashishtha, Dheeraj Alimchandani y Dhananjay Karanjkar, Amazon Web Services

Resumen

Es habitual que se requieran entidades y funciones de operaciones de creación, lectura, actualización y eliminación (CRUD) para realizar operaciones de base de datos de Amazon DynamoDB. PynamoDB es una interfaz basada en Python que admite Python 3. También ofrece características como la compatibilidad con las transacciones de Amazon DynamoDB, la serialización y deserialización automáticas de los valores de los atributos y la compatibilidad con los marcos de trabajo más comunes de Python, como Flask y Django. Este patrón permite a los desarrolladores trabajar con Python y DynamoDB, ya que proporciona una biblioteca que facilita la creación automática de modelos de PynamoDB y funciones de operación CRUD. Si bien genera funciones CRUD esenciales para las tablas de bases de datos, también puede aplicar ingeniería inversa a los modelos de PynamoDB y a las funciones CRUD de las tablas de Amazon DynamoDB. Este patrón está diseñado para simplificar las operaciones de la base de datos mediante una aplicación basada en Python.

Estas son algunas de las características principales de la solución:

- Esquema JSON a modelo PynamoDB: genere automáticamente modelos de PynamoDB en Python mediante la importación de un archivo de esquema JSON.
- Generación de funciones CRUD: genere automáticamente funciones para realizar operaciones CRUD en tablas de DynamoDB.
- Ingeniería inversa desde DynamoDB: utilice la asignación relacional de objetos (ORM) de PynamoDB para aplicar ingeniería inversa a los modelos de PynamoDB y a las funciones CRUD de las tablas de Amazon DynamoDB existentes.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- La versión 3.8 o posterior de Python descargada e instalada
- La versión 3.1.2 o posterior de Jinja2 descargada e instalada

- Tablas de Amazon DynamoDB para las que desea generar ORM
- AWS Command Line Interface (AWS CLI), instalado y configurado
- La versión 5.4.1 o posterior de PynamoDB instalada

Arquitectura

Pila de tecnología de destino

- script de JSON
- aplicación de Python
- modelo de PynamoDB
- instancia de base de datos de Amazon DynamoDB

Arquitectura de destino

1. Debe crear un archivo de esquema JSON de entrada. Este archivo de esquema JSON representa los atributos de las tablas de DynamoDB respectivas a partir de las que desea crear modelos de PyNamoDB y para las que desea crear funciones CRUD. Contiene estas tres claves importantes:
   - `name`: el nombre de la tabla de destino de DynamoDB.
   - `region`— El Región de AWS lugar donde está alojada la tabla
   - `attributes`: atributos que forman parte de la tabla de destino, como la clave de partición (también conocida como atributo hash), la clave de clasificación, los índices secundarios locales, los índices secundarios globales y cualquier atributo que no sea clave. Esta herramienta espera que el esquema de entrada solo proporcione atributos que no sean clave, ya que la aplicación los obtiene directamente de la tabla de destino. Para ver un ejemplo de cómo especificar atributos en el archivo de esquema JSON, consulte la sección Información adicional de este patrón.
2. Ejecute la aplicación Python y proporcione el archivo de esquema JSON como entrada.
3. La aplicación Python lee el archivo de esquema JSON.
4. La aplicación Python se conecta a las tablas de DynamoDB para derivar el esquema y los tipos de datos. La aplicación ejecuta la operación describe_table y obtiene los atributos clave y de índice de la tabla.

5. La aplicación Python combina los atributos del archivo de esquema JSON y la tabla de DynamoDB. Utiliza el motor de plantillas de Jinja para generar un modelo de PynamoDB y las funciones CRUD correspondientes.
6. Puede acceder al modelo de PynamoDB para realizar operaciones CRUD en la tabla de DynamoDB.

Tools (Herramientas)

Servicios de AWS

- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.

Otras herramientas

- Jinja es un motor de plantillas extensible que compila plantillas en código Python optimizado. Este patrón usa Jinja para generar contenido dinámico al incrustar marcadores de posición y lógica en las plantillas.
- PynamoDB es una interfaz basada en Python para Amazon DynamoDB.
- Python es un lenguaje de programación informático de uso general.

Repositorio de código

El código de este patrón está disponible en el repositorio de funciones CRUD y modelos de PynamoDB de GitHub generación automática. El repositorio está dividido en dos partes principales: el paquete de controladores y las plantillas.

Paquete de controladores

El paquete Python de controladores contiene la lógica de aplicación principal que ayuda a generar el modelo de PynamoDB y las funciones CRUD. Contiene lo siguiente:

- `input_json_validator.py`: este script de Python valida el archivo de esquema JSON de entrada y crea los objetos Python que contienen la lista de tablas de DynamoDB de destino y los atributos necesarios para cada uno.

- `dynamo_connection.py`: este script establece una conexión con la tabla de DynamoDB y utiliza la operación `describe_table` para extraer los atributos necesarios para crear el modelo de PynamoDB.
- `generate_model.py`: este script contiene una clase de Python `GenerateModel` que crea el modelo de PynamoDB en función del archivo de esquema JSON de entrada y de la operación `describe_table`.
- `generate_crud.py`: para las tablas de DynamoDB que se definen en el archivo de esquema JSON, este script utiliza la operación `GenerateCrud` para crear las clases de Python.

Plantillas

Este directorio de Python contiene las siguientes plantillas de Jinja:

- `model.jinja`: esta plantilla de Jinja contiene la expresión de plantilla para generar el script de modelo de PynamoDB.
- `crud.jinja`: esta plantilla de Jinja contiene la expresión de plantilla para generar el script de funciones CRUD.

Epics

Configuración del entorno

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Introduzca el comando siguiente para clonar el repositorio Generación automática de modelos de PynamoDB y funciones CRUD. `git clone https://github.com/aws-samples/amazon-reverse-engineer-dynamodb.git`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Configure el entorno de Python.	1. Vaya al directorio de nivel superior del repositorio clonado.
	`cd amazon-reverse-engineer-dynamodb`
	2. Para instalar las bibliotecas y los paquetes necesarios, introduzca el comando siguiente.
	`pip install -r requirements.txt`
		Desarrollador de aplicaciones

Generación del modelo de PynamoDB y las funciones CRUD

Tarea	Descripción	Habilidades requeridas
Modifique el archivo de esquema JSON.	1. Vaya al directorio de nivel superior del repositorio clonado. `cd amazon-reverse-engineer-dynamodb` 2. Abra el archivo `test.json` en el editor que desee. Puede usar este archivo como referencia para crear su propio archivo de esquema JSON o puede actualizar los valores del archivo para que coincidan con su entorno.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	3. Modifique los valores de nombre y atributos de las tablas de DynamoDB de destino. Región de AWS **Note** Si define una tabla que no existe en el archivo de esquema JSON, esta solución no genera modelos ni funciones CRUD para esa tabla. 4. Guarde y cierre el archivo `test.json` . Le recomendamos que guarde este archivo con un nuevo nombre.	
Ejecute la aplicación Python.	Introduzca el siguiente comando para generar los modelos de PynamoDB y las funciones CRUD, donde `<input_schema.json>` es el nombre del archivo de esquema JSON. `python main.py --file <input_schema.json>`	Desarrollador de aplicaciones

Verificación del modelo de PynamoDB y las funciones CRUD

Tarea	Descripción	Habilidades requeridas
Compruebe el modelo de PynamoDB generado.	1. En el directorio de nivel superior del repositorio clonado, introduzca el siguiente comando para ir al repositorio `models`. `cd models` 2. De forma predeterminada, esta solución asigna un nombre al archivo `demo_model.py` de modelo de PynamoDB. Compruebe que el archivo esté presente.	Desarrollador de aplicaciones
Verifique las funciones CRUD generadas.	1. En el directorio de nivel superior del repositorio clonado, introduzca el siguiente comando para ir al repositorio `crud`. `cd crud` 2. De forma predeterm inada, esta solución asigna un nombre al script `demo_crud.py` . Compruebe que el archivo esté presente. 3. Utilice las clases de Python del archivo `demo_crud .py` para realizar una operación CRUD en la tabla	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	de DynamoDB de destino. Confirme que la operación se completó correctamente.	

Recursos relacionados

- Componentes básicos de Amazon DynamoDB (documentación de DynamoDB)
- Mejora del acceso con índices secundarios (documentación de DynamoDB)

Información adicional

Ejemplos de atributos para el archivo de esquema JSON

```
[
{
"name": "test_table",
"region": "ap-south-1",
"attributes": [
{
"name": "id",
"type": "UnicodeAttribute"
},
{
"name": "name",
"type": "UnicodeAttribute"
},
{
"name": "age",
"type": "NumberAttribute"
}
]
}
]
```

Bloquee el acceso público a Amazon RDS mediante Cloud Custodian

abhay kumar y Dwarika Patra, Amazon Web Services

Resumen

Muchas organizaciones ejecutan sus cargas de trabajo y servicios en múltiples proveedores de nube. En estos entornos de nube híbrida, la infraestructura de nube necesita un gobierno estricto, además de la seguridad proporcionada por los proveedores de nube individuales. Una base de datos en la nube, como Amazon Relational Database Service (Amazon RDS), es un servicio importante que debe supervisarse para detectar cualquier vulnerabilidad de acceso y permisos. Si bien puede restringir el acceso a la base de datos de Amazon RDS configurando un grupo de seguridad, también puede añadir un segundo nivel de protección para prohibir acciones como el acceso público. Bloquear el acceso público lo ayudará a cumplir con el Reglamento General de Protección de Datos (RGPD), la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA), el Instituto Nacional de Estándares y Tecnología (NIST) y el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS).

Cloud Custodian es un motor de reglas de código abierto que puede usar para imponer restricciones de acceso a los recursos de Amazon Web Services (AWS), como Amazon RDS. Cloud Custodian le permite establecer reglas que validen el entorno según los estándares de seguridad y conformidad definidos. Puede usar Cloud Custodian para administrar sus entornos de nube y así garantizar el cumplimiento de las políticas de seguridad, las políticas de etiquetado, la recopilación de elementos no utilizados y la administración de costos. Con Cloud Custodian puede usar una única interfaz para implementar la gobernanza en su entorno de nube híbrida. Por ejemplo, puede usar la interfaz Cloud Custodian para interactuar con Microsoft Azure AWS y reducir el esfuerzo de trabajar con mecanismos como AWS Config los grupos de AWS seguridad y las políticas de Azure.

Este patrón proporciona instrucciones para usar Cloud Custodian AWS para imponer la restricción de la accesibilidad pública en las instancias de Amazon RDS.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Un par de claves
- AWS Lambda instalado

Arquitectura

En el siguiente diagrama AWS Lambda, se muestra a Cloud Custodian implementando la política AWS CloudTrail e iniciando el `CreateDBInstance` evento y configurando la función Lambda en `PubliclyAccessible` false en Amazon RDS.

Tools (Herramientas)

Servicios de AWS

- AWS CloudTraille ayuda a auditar la gobernanza, el cumplimiento y el riesgo operativo de su empresa. Cuenta de AWS
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar Servicios de AWS mediante comandos en su consola de línea de comandos.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Relational Database Service (Amazon RDS) lo ayuda a configurar, utilizar y escalar una base de datos relacional en la Nube de AWS.

Otras herramientas

- Cloud Custodian unifica las herramientas y scripts que emplean muchas organizaciones para administrar sus cuentas de nube pública en una sola herramienta de código abierto. Emplea un motor de reglas sin estado para la definición y aplicación de las políticas con métricas, resultados estructurados e informes detallados de la infraestructura de la nube. Se integra perfectamente con tiempos de ejecución sin servidor para proporcionar soluciones y respuestas en tiempo real con una baja sobrecarga operativa.

Epics

Configure el AWS CLI

Tarea	Descripción	Habilidades requeridas
Instale el AWS CLI.	Para instalar el AWS CLI, siga las instrucciones de la AWS documentación.	Administrador de AWS

Configure AWS las credencia les.	Configure los ajustes AWS CLI con los que interactuarán AWS, incluidos el Región de AWS formato de salida que desee utilizar.
	`$>aws configure`
	`AWS Access Key ID`
	`[None]: <your_acc`
	`ess_key_id>`
	`AWS Secret Access Key`
	`[None]: <your_sec`
	`ret_access_key>`
	`Default region name`
	`[None]:`
	`Default output format`
	`[None]:`
	Para obtener más información, consulte la Documentación de AWS.
		Administrador de AWS

Crear un rol de IAM.	Para crear un rol de IAM con el rol de ejecución de Lambda, ejecute el siguiente comando.
	`aws iam create-role`
	`--role-name lambda-`
	`ex --assume-role-poli`
	`cy-document '{"Versio`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`n": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principal": {"Service": "lambda.amazonaws.com"}, "Action": "sts:AssumeRole"}]}`	

Configure Cloud Custodian

Tarea	Descripción	Habilidades requeridas
Instale Cloud Custodian.	Para instalar Cloud Custodian en su sistema operativo y entorno, siga las instrucciones de la documentación de Cloud Custodian.	DevOps ingeniero
Consulte el esquema de Cloud Custodian.	Para ver una lista completa de los recursos de Amazon RDS con los que puede ejecutar políticas, introduzca el siguiente comando. `custodian schema aws.rds`	DevOps ingeniero
Cree la política de Cloud Custodian.	Guarda el código que se encuentra en el archivo de políticas de Cloud Custodian en la sección de Información adicional con una extensión YAML.	DevOps ingeniero
Defina las acciones de Cloud Custodian para cambiar el indicador de acceso público.	1. Localice el código de Custodian (por ejemplo, `/Users/abcd/custod`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`ian/lib/python3.9/site-packages/c7n/resources/rds.py`). 2. Localice la clase `RDSSetPublicAvailability` en `rds.py` y modifíquela introduciendo el código que se encuentra en el archivo rds.py de recursos de c7n, en la sección de Información adicional.	
Ejecute una prueba.	(Opcional) Para comprobar qué recursos identifica la política sin ejecutar ninguna acción en ellos, emplee el siguiente comando. `custodian run -dryrun <policy_name>.yaml -s <output_directory>`	DevOps ingeniero

Implemente la política

Tarea	Descripción	Habilidades requeridas
Implemente la política mediante Lambda.	Para crear la función de Lambda que ejecutará la política, introduzca el siguiente comando. `custodian run -s policy.yaml`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Luego, el AWS CloudTrail `CreateDBInstance` evento iniciará esta política. Como resultado, AWS Lambda configurará el indicador de acceso público `false` para las instancias que cumplan con los criterios.	

Recursos relacionados

- AWS Lambda sitio web
- Sitio web de Amazon RDS
- Documentación de Cloud Custodian

Información adicional

Archivo YAML de política de Cloud Custodian

```
policies:
  - name: "block-public-access"
    resource: rds
    description: |
      This Enforcement blocks public access for RDS instances.
    mode:
      type: cloudtrail
      events:
        - event: CreateDBInstance # Create RDS instance cloudtrail event
          source: rds.amazonaws.com
          ids: requestParameters.dBInstanceIdentifier
      role: arn:aws:iam::1234567890:role/Custodian-compliance-role
    filters:
      - type: event
        key: 'detail.requestParameters.publiclyAccessible'
        value: true
    actions:
```

```
      - type: set-public-access
        state: false
```

Archivo rds.py de recursos de c7n

```
@actions.register('set-public-access')
 class RDSSetPublicAvailability(BaseAction):

     schema = type_schema(
         "set-public-access",
         state={'type': 'boolean'})
     permissions = ('rds:ModifyDBInstance',)

     def set_accessibility(self, r):
         client = local_session(self.manager.session_factory).client('rds')
         waiter = client.get_waiter('db_instance_available')
         waiter.wait(DBInstanceIdentifier=r['DBInstanceIdentifier'])
         client.modify_db_instance(
             DBInstanceIdentifier=r['DBInstanceIdentifier'],
             PubliclyAccessible=self.data.get('state', False))


     def process(self, rds):
         with self.executor_factory(max_workers=2) as w:
             futures = {w.submit(self.set_accessibility, r): r for r in rds}
             for f in as_completed(futures):
                 if f.exception():
                     self.log.error(
                         "Exception setting public access on %s  \n %s",
                         futures[f]['DBInstanceIdentifier'], f.exception())
         return rds
```

Integración de Security Hub CSPM

Cloud Custodian se puede integrar con AWS Security Hub CSPM para enviar resultados de seguridad y tratar de adoptar medidas correctivas. Para obtener más información, consulte Anuncio de la integración de Cloud Custodian con. AWS Security Hub CSPM

Configure la autenticación de Windows para Amazon RDS for Microsoft SQL Server mediante AWS Managed Microsoft AD

Ramesh Babu Donti, Amazon Web Services

Resumen

Este patrón muestra cómo configurar la autenticación de Windows para un Amazon Relational Database Service (Amazon RDS) para instancias de SQL Server AWS Directory Service for Microsoft Active Directory mediante AWS Managed Microsoft AD(). La autenticación de Windows permite a los usuarios conectarse a la instancia de RDS mediante sus credenciales de dominio en lugar de tener que usar nombres de usuario y contraseñas específicos de la base de datos.

Puede habilitar la autenticación de Windows al crear una nueva base de datos de SQL Server de RDS o al agregarla a una instancia de base de datos existente. La instancia de base de datos se integra AWS Managed Microsoft AD para proporcionar autenticación y autorización centralizadas a los usuarios del dominio que acceden a la base de datos de SQL Server.

Esta configuración mejora la seguridad, ya que aprovecha la infraestructura de Active Directory existente y elimina la necesidad de administrar credenciales de bases de datos independientes para los usuarios del dominio.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS con los permisos adecuados
- Cree una nube privada virtual (VPC) con lo siguiente:
  - Tablas de enrutamiento y puertas de enlace de Internet configuradas
  - Puertas de enlace NAT en subredes públicas (si las instancias requieren acceso a Internet)
- AWS Identity and Access Management Funciones (IAM):
  - Un rol de dominio con las siguientes políticas AWS administradas:
    - `AmazonSSMManagedInstanceCore`para habilitar AWS Systems Manager
    - `AmazonSSMDirectoryServiceAccess` para proporcionar permisos para unir instancias a directorios
  - Un rol de supervisión mejorado de RDS (si la supervisión mejorada está habilitada)
- Grupos de seguridad:

  - grupo de seguridad del servicio de directorio para permitir los puertos de comunicación de Active Directory
  - Un grupo de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) para permitir las comunicaciones RDP `3389` y de dominio
  - Un grupo de seguridad de RDS para permitir la portabilidad `1433` de SQL Server desde orígenes autorizados
- Conectividad de red:
  - Resolución de DNS y conectividad de red adecuadas entre subredes

Limitaciones

- Para obtener información sobre Regiones de AWS ese soporte AWS Managed Microsoft AD con RDS para SQL Server, consulte Disponibilidad regional y de versiones.
- Algunas Servicios de AWS no están disponibles en todos Regiones de AWS. Para conocer la disponibilidad de las regiones, consulte Servicios de AWS by Region. Para los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

Pila de tecnología de origen

- Un Active Directory local o AWS Managed Microsoft AD

Pila de tecnología de destino

- Amazon EC2
- Amazon RDS for Microsoft SQL Server
- AWS Managed Microsoft AD

Arquitectura de destino

La arquitectura incluye lo siguiente:

- Un rol de IAM que une la EC2 instancia de Amazon al AWS Managed Microsoft AD dominio.

- Una instancia de Amazon EC2 Windows para la administración y las pruebas de bases de datos.
- Una instancia de Amazon VPC con una subred privada para alojar la instancia de Amazon RDS y los recursos internos en todas las zonas de disponibilidad.
- Grupos de seguridad para el control del acceso a la red:
  - Un grupo de seguridad de Amazon RDS para controlar el acceso entrante al puerto `1433` de SQL Server desde orígenes autorizados.
  - Un grupo EC2 de seguridad de Amazon para gestionar el acceso RDP a través de los puertos de comunicación de puertos `3389` y dominios.
  - Un grupo de seguridad del servicio de directorio para las comunicaciones de Active Directory a través de los puertos `53`, `88`, `389` y `445`.
- AWS Managed Microsoft AD para proporcionar servicios centralizados de autenticación y autorización para los recursos de Windows.
- Una instancia de base de datos de Amazon RDS para SQL Server en la subred privada con la autenticación de Windows habilitada.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática escalable en el Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Relational Database Service (Amazon RDS) lo ayuda a configurar, utilizar y escalar una base de datos relacional en la Nube de AWS.
- AWS Directory Serviceproporciona varias formas de utilizar Microsoft Active Directory (AD) con otras, Servicios de AWS como Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS) para SQL Server y FSx Amazon para Windows File Server.
- AWS Directory Service for Microsoft Active Directorypermite que sus cargas de trabajo y AWS recursos compatibles con directorios utilicen Microsoft Active Directory en. Nube de AWS
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.

Otros servicios

- Microsoft SQL Server Management Studio (SSMS) es una herramienta para administrar SQL Server, que incluye el acceso, la configuración y la administración de los componentes de SQL Server.

Prácticas recomendadas

- Para obtener información sobre las prácticas recomendadas generales, consulte Prácticas recomendadas para Amazon RDS.

Epics

Configuración AWS Managed Microsoft AD

Tarea	Descripción	Habilidades requeridas
Configure el tipo de directorio.	1. Desde el Consola de administración de AWS, navegue hasta. AWS Directory Service 2. Elija Configurar directorio. 3. Seleccione AWS Managed Microsoft AD para el tipo de directorio. 4. Selecciona Crear un nuevo dominio de AD AWS administrado y, a continuación, selecciona Siguiente.	DBA, ingeniero DevOps
Configure la información del directorio.	En la sección de información del directorio, introduzca la información necesaria y conserve los valores opcionales:	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	1. En Edición, seleccione una edición que se adapte a sus necesidades. 2. En Nombre DNS del directorio, introduzca un nombre de dominio completo (FQDN). 3. En Contraseña de administrador, establezca una contraseña para la cuenta de administrador y, a continuación, seleccione Siguiente.	
Configure la VPC y las subredes.	1. En Redes, seleccione una VPC de destino (como mínimo, debe configurar dos subredes separadas). Zonas de disponibilidad de AWS 2. En Tipo de red, selecciona Solo. IPv4 3. En Subredes, seleccione dos subredes privadas separadas y Zonas de disponibilidad de AWS, a continuación, elija Siguiente.	DBA, ingeniero DevOps
Revise y cree el directorio.	1. Revise los valores de configuración y luego elija Crear directorio. 2. Espere a que el estado del directorio cambie a Activo.	DBA, ingeniero DevOps

Crear y configurar una EC2 instancia de Amazon

Tarea	Descripción	Habilidades requeridas
Configure una AMI para Windows.	1. Desde Consola de administración de AWS, navegue hasta EC2. 2. Seleccione Iniciar instancia. 3. En Nombre y etiquetas, introduzca un nombre y cualquier etiqueta aplicable. 4. Elija una Imagen de máquina de Amazon (AMI) para Windows Server que cumpla con sus requisitos. 5. En Tipo de instancia, seleccione un tipo de tamaño adecuado. 6. En Par de claves (inicio de sesión), seleccione un par de claves existente o cree uno nuevo.	DBA, ingeniero DevOps
Configure los valores de red.	1. En Configuración de red, selecciona la misma VPC que se utiliza en AWS Directory Service. 2. Elija una subred privada. 3. En Firewall (grupos de seguridad), cree un grupo que permita las comunicaciones entre el puerto 3389 y dominios de RDP.	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
Configure el almacenamiento	Configure los volúmenes de Amazon EBS según sea necesario.	DBA, ingeniero DevOps
Configure los detalles avanzados y lance la instancia .	1. Amplíe la sección Detalles avanzados. 2. En el directorio de unión a dominios, seleccione el creado AWS Managed Microsoft AD anteriormente. 3. En el perfil de instancia de IAM, seleccione un rol con las políticas `AmazonSSMManagedInstanceCore` y `AmazonSSMDirectoryServiceAccess` . 4. Revise todos los valores de configuración y, luego, seleccione Iniciar instancia.	DBA, ingeniero DevOps

Creación y configuración de RDS para SQL Server con la autenticación de Windows

Tarea	Descripción	Habilidades requeridas
Cree una base de datos y configure las opciones del motor.	1. Vaya a la consola de Aurora y RDS y elija Crear una base de datos. 2. En Opciones del motor, elija Microsoft SQL Server. 3. En Tipo de administración de base de datos, elija Amazon RDS Custom.	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	4. En Edición, elija una instancia de SQL Server que cumpla con sus requisitos. 5. En Versión del motor, elija la última versión compatibl e.	
Elija una plantilla.	Elija una plantilla de muestra que se adapte a sus necesidades.	DBA, ingeniero DevOps
Configure los ajustes de base de datos.	1. En la sección Configura ción, introduzca un nombre único para el identificador de instancias de bases de datos. 2. En Nombre de usuario principal, configure las credenciales de administr ador. 3. En Administración de credenciales, elija Administr adas en AWS Secrets Manager o Autoadmin istradas.	DBA, ingeniero DevOps
Configurar la instancia	En la sección Configuración de instancias, en Clase de instancia de base de datos, seleccione un tamaño de instancia que cumpla sus requisitos.	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
Configure el almacenamiento	1. En la sección Almacenamiento, en Tipo de almacenamiento, elija un tipo que cumpla sus requisitos. Recomendamos que use gp3, io1 o io2. 2. Establezca los valores iniciales necesarios para el almacenamiento asignado, las IOPS aprovisionadas y el rendimiento del almacenamiento. 3. (Opcional) Amplíe la sección de configuración de almacenamiento adicional y seleccione Habilitar el escalado automático del almacenamiento.	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
Configure la conectividad.	1. En la sección Conectividad, decida si desea establecer una conexión a un recurso informático para la base de datos. 2. Para la VPC, elija la misma VPC que tiene. AWS Directory Service 3. En el grupo de subredes de base de datos, elija un grupo que abarque varias zonas de disponibilidad. 4. En el acceso público, elija No. 5. En el grupo de seguridad de VPC (firewall), elija un grupo existente o cree uno nuevo que permita el acceso a través del puerto 1433 de SQL Server. 6. Seleccione la zona de disponibilidad que prefiera. 7. Amplíe la sección Configuración adicional y decida si desea utilizar un puerto de base de datos personalizado.	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
Configure la autenticación de Windows.	1. En la sección de autenticación de Windows de Microsoft SQL Server, active la casilla Habilitar la autenticación de Windows de Microsoft SQL Server. 2. En el tipo de autenticación de Windows, elija AWS Managed Microsoft AD. 3. En Directorio, elija Examinar directorio y seleccione AWS Managed Microsoft AD.	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
Configure la supervisión	1. En la sección Supervisión, elija información de base de datos estándar o avanzada. 2. En Información de rendimiento, active la casilla Habilitar la información de rendimiento. 3. Seleccione un período de retención y una AWS KMS clave. 4. En Configuración de supervisión adicional , seleccione la casilla Supervisión mejorada. 5. (Opcional) En Exportaciones de registros, seleccione la casilla Registro de errores. Nota: Las métricas son útiles cuando desea ver cómo diferentes procesos o subprocesos usan la CPU. También puedes exportar los registros de errores a Amazon CloudWatch si el registro de errores está activado.	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
Configure los ajustes adicionales.	1. Amplíe la sección Configuración adicional. 2. En el grupo de parámetros de base de datos y el grupo de opciones de base de datos, elija valores predeterminados o personalizados. 3. Establezca la zona horaria que prefiera. 4. En Intercalación, establezca un valor. El valor predeterminado es `SQL_Latin1_General_CP1_CI_AS` . 5. En Copia de seguridad: • Seleccione la casilla Habilitar copias de seguridad automatizadas. Esto crea una instantánea de la base de datos. • En el período de retención de copias de seguridad, elija el número de días requerido. • En la ventana de copias de seguridad, seleccione un valor. • (Opcional) En la replicación de copias de seguridad, elija Habilitar replicación en otra Región de AWS.	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	• Seleccione la casilla de verificación Habilitar el cifrado para cifrar las instancias mediante. AWS KMS 6. En la ventana de mantenimiento, seleccione la casilla de verificación Elegir una ventana y establezca una hora preferida. 7. Seleccione la casilla Habilitar la protección contra borrado.	
Revise los costos y cree una base de datos.	Revise la sección de costos mensuales estimados y, a continuación, elija Crear base de datos.	DBA, ingeniero DevOps

Configuración del acceso a la base de datos y prueba de las conexiones

Tarea	Descripción	Habilidades requeridas
Conéctese a la máquina de Windows.	Conéctese a su máquina de Windows e inicie SQL Server Management Studio. 1. Utilice RDP para conectarse a su máquina Windows mediante credenciales AWS Managed Microsoft AD 2. Para iniciar SSMS, introduzca SSMS en el	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	menú Inicio y seleccione SQL Server Management Studio.	
Configure la conexión SSMS.	Configure la conexión a la base de datos mediante la autenticación de Windows. 1. Cuando aparezca el cuadro de diálogo Conectar al servidor (o al ir a Explorador de objetos, Conectar o Motor de base de datos), defina el tipo de servidor como Motor de base de datos. 2. Introduzca el punto de conexión de RDS SQL Server (por ejemplo, `your-rds-instance.region.rds.amazonaws.com`). 3. Seleccione Autenticación de Windows.	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
Configurar configuración de seguridad.	Establezca los parámetros de seguridad necesarios para la versión 20 o posterior de SSMS. 1. En la pestaña Propiedades de la conexión, establezca el cifrado como Obligatorio. 2. Seleccione la casilla de verificación Certificado de servidor de confianza. 3. Deje en blanco el campo Nombre de host en el certificado. 4. (Opcional) Establezca el nombre de la base de datos y ajuste el tiempo de espera de la conexión según sea necesario.	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas

Cree un inicio de sesión de Windows.	1. Configure y pruebe la autenticación de Windows para los usuarios del dominio.
	2. Para establecer una conexión inicial, elija Conectar.
	3. En la ventana de consulta, ejecute lo siguiente:
	`CREATE LOGIN [<domainName>\<user_name>] FROM WINDOWS;`
	`GO`
		DBA, ingeniero DevOps

Pruebe la autenticación de Windows	1. Cierra sesión en la EC2 instancia de Amazon. 2. Vuelva a iniciar sesión en la EC2 instancia con las credenciales de su dominio. 3. Inicie SSMS. 4. Conéctese mediante la autenticación de Windows. 5. Compruebe que la conexión se realizó correctamente.	DBA, ingeniero DevOps

Recursos relacionados

- Creando tu AWS Managed Microsoft AD
- Unir una instancia de Amazon EC2 Windows a su AWS Managed Microsoft AD
- Regiones y motores de base de datos compatibles para la autenticación Kerberos en Amazon RDS
- Qué es SQL Server Management Studio (SSMS)?

Configurar el acceso entre cuentas a Amazon DynamoDB

Shashi Dalmia, Imhoertha Ojior y Esteban Serna Parra, Amazon Web Services

Resumen

Este patrón explica los pasos para configurar el acceso entre cuentas a Amazon DynamoDB mediante políticas basadas en recursos. En el caso de las cargas de trabajo que utilizan DynamoDB, cada vez es más común utilizar estrategias de aislamiento de cargas de trabajo para minimizar las amenazas a la seguridad y cumplir con los requisitos de conformidad. La implementación de estrategias de aislamiento de la carga de trabajo a menudo requiere el acceso entre cuentas y regiones a los recursos de DynamoDB mediante AWS Identity and Access Management políticas basadas en la identidad (IAM). Esto implica establecer los permisos de IAM y establecer una relación de confianza entre. Cuentas de AWS

Las políticas basadas en recursos para DynamoDB simplifican en gran medida la postura de seguridad de las cargas de trabajo entre cuentas. Este patrón proporciona pasos y código de ejemplo para demostrar cómo se pueden configurar AWS Lambda las funciones en una sola cuenta Cuenta de AWS para escribir datos en una tabla de base de datos de DynamoDB en una cuenta diferente.

Requisitos previos y limitaciones

Requisitos previos

- Dos activas. Cuentas de AWS Este patrón hace referencia a estas cuentas como Cuenta A y Cuenta B.
- AWS Command Line Interface (AWS CLI) instalado y configurado para acceder a la cuenta A y crear la tabla de DynamoDB. Los demás pasos de este patrón proporcionan instrucciones para usar las consolas IAM, DynamoDB y Lambda. Si piensa utilizarla AWS CLI en su lugar, configúrela para acceder a ambas cuentas.

Limitaciones

- Algunas Servicios de AWS no están disponibles en todas Regiones de AWS. Para conocer la disponibilidad de las regiones, consulte Servicios de AWS by Region. Para los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

El siguiente diagrama muestra una arquitectura de cuenta única. AWS Lambda, Amazon Elastic Compute Cloud (Amazon EC2) y DynamoDB están todos en la misma cuenta. En este escenario, las funciones de Lambda y las EC2 instancias de Amazon pueden acceder a DynamoDB. Para conceder acceso a la tabla de DynamoDB, puede crear una política basada en identidades en IAM o una política basada en recursos en DynamoDB.

En el siguiente diagrama se muestra una arquitectura de varias cuentas. Si los recursos de una de ellas Cuenta de AWS requieren acceso a una tabla de DynamoDB de una cuenta diferente, debe configurar una política basada en recursos en DynamoDB para conceder el acceso necesario. Por ejemplo, en el siguiente diagrama, el acceso a la tabla de DynamoDB de la cuenta A se concede a una función de Lambda de la cuenta B mediante una política basada en recursos.

En este patrón se describe el acceso entre cuentas entre Lambda y DynamoDB. Puede seguir estos pasos con otros pasos Servicios de AWS si se configuran los permisos adecuados en ambas cuentas. Por ejemplo, si desea proporcionar a una función de Lambda acceso a un bucket de Amazon Simple Storage Service (Amazon S3) en la cuenta A, puede crear una política basada en recursos en Amazon S3 y añadir los permisos al rol de ejecución de Lambda en la cuenta B.

Tools (Herramientas)

Servicios de AWS

- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus recursos de AWS al controlar quién está autenticado y autorizado a usarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

Código

Este patrón incluye código de muestra en la sección de Información adicional para ilustrar cómo se puede configurar una función de Lambda en la cuenta B para escribir en la tabla de DynamoDB

de la cuenta A. El código se proporciona únicamente con fines ilustrativos y de prueba. Si va a implementar este patrón en un entorno de producción, utilice el código como referencia y personalícelo para su propio entorno.

Prácticas recomendadas

- Siga las prácticas recomendadas para las políticas basadas en recursos de la documentación de DynamoDB.
- Cumpla con el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Creación de una política y rol de IAM para la función de Lambda en la cuenta B

Tarea	Descripción	Habilidades requeridas
Cree una política en la cuenta B.	Esta política de IAM permite la PutItemacción para una tabla de DynamoDB en la cuenta A. 1. Inicie sesión en la cuenta B en. Consola de administración de AWS 2. Abra la consola de IAM. 3. En el panel de navegación, seleccione Políticas y, a continuación, Crear política. 4. En la página Especificar permisos del editor de políticas, seleccione JSON. 5. Escriba la siguiente política. `{ "Version": "2012-10-17",`	AWS general

Tarea	Descripción	Habilidades requeridas

	<pre>{
	  "Statement": [
	    {
	      "Sid": "Statemen
	t1",
	      "Effect":
	 "Allow",
	      "Action":
	 "dynamodb:PutItem",
	      "Resource":
	 "arn:aws:dynamodb:
	<Region>:<Account-
	A-ID>:table/Table-
	Account-A"
	    }
	  ]
	}</pre>
	6. Sustituya <Region> y <Account-A-ID> por sus valores y, a continuación, seleccione Siguiente.
	7. En Nombre de la política, especifique un nombre único para la política; por ejemplo DynamoDB-PutItem-Policy .
	8. (Opcional) Añada una descripción de la política.
	9. Elija Crear política.	

Tarea	Descripción	Habilidades requeridas
Cree un rol en la cuenta B.	La función de Lambda de la cuenta B utiliza este rol de IAM para acceder a la tabla de DynamoDB de la cuenta A. 1. Abra la consola de IAM. 2. En el panel de navegación, seleccione Roles y luego seleccione Crear rol. 3. En Select trusted entity (Seleccionar entidad de confianza), elija Servicio de AWS. 4. En la sección Caso de uso, elija Lambda. 5. Elija Next: Permissions (Siguiente: Permisos). 6. En el cuadro Filter policies (Políticas de filtro), escriba DynamoDB. 7. En la lista de políticas de DynamoDB, elija `DynamoDB-PutItem-Policy` . 8. Desactive la casilla Filtrar políticas y, a continuación, escriba Lambda. 9. En la lista de políticas Lambda, elija AWSLambda Ejecutar. 10. Seleccione Siguiente: asigne un nombre, revise y cree.	AWS general

Tarea	Descripción	Habilidades requeridas
	11. En Nombre del rol, ingrese un nombre único para su rol, por ejemplo, `DynamoDB-PutItemAccess` . 12. (Opcional) Añada una descripción del rol. 13. De manera opcional, agregue metadatos al rol al asociar etiquetas como pares de clave-valor. 14. Seleccione Crear rol. Para obtener más información sobre los usuarios de IAM, consulte la documentación de IAM.	
Apunte el ARN del rol .	1. Abra la consola de IAM. 2. Seleccione Roles en el panel de navegación. 3. En el cuadro de búsqueda, introduzca `DynamoDB-PutItemAccess` y, a continuación, seleccione el rol. 4. En la página de resumen del rol, copie el nombre de recurso de Amazon (ARN). El ARN se usa al configurar la función de Lambda.	AWS general

Crear una tabla en DynamoDB en la cuenta A

Tarea	Descripción	Habilidades requeridas

Crear una tabla de DynamoDB.	Utilice el siguiente AWS CLI comando para crear una tabla de DynamoDB.
	
	`aws dynamodb create-table \`
	`--table-name Table-Account-A \`
	`--attribute-definitions \`
	`Attribute Name=category,AttributeType=S \`
	`Attribute Name=item,AttributeType=S \`
	`--key-schema \`
	`Attribute Name=category,KeyType=HASH \`
	`Attribute Name=item,KeyType=RANGE \`
	`--provisioned-throughput \`
	`ReadCapacityUnits=5,WriteCapacityUnits=5 \`
	`--resource-policy \`
	`'{`
	`"Version": "2012-10-17",`
	`"Statement": [`
	`{`
	`"Sid": "Statement1",`
		AWS general

Tarea	Descripción	Habilidades requeridas
	"Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::<Account-B-ID>:role/<Role-Name>" }, "Action": "dynamodb:PutItem", "Resource": "arn:aws:dynamodb:<Region>:<Account-A-ID>:table/Table-Account-A" }] }' Sustituya lo siguiente en el código de muestra: • `<Account-B-ID>` es el ID de la cuenta B. • `<Role-Name>` es el nombre del rol de IAM que ha creado, como `DynamoDB-PutItemAccess`. • `<Region>`es Región de AWS donde se va a crear la tabla de DynamoDB. • `<Account-A-ID>` es el ID de la cuenta A.	

Tarea	Descripción	Habilidades requeridas
	Note Para especificar la configuración de la política basada en los recursos en la declaración `create-table` , utilice el indicador `--resource-policy` . Esta política hace referencia al ARN de la tabla de DynamoDB de la cuenta A. Para obtener más información acerca de la creación de tablas, consulte la documentación de DynamoDB.	

Creación de una función de Lambda en la cuenta B

Tarea	Descripción	Habilidades requeridas
Cree una función de Lambda para escribir datos en DynamoDB.	1. Inicie sesión en la cuenta B en. Consola de administración de AWS 2. Abra la consola de Lambda. 3. En el panel de navegación, seleccione Funciones y, a continuación, Crear una función.	AWS general

Tarea	Descripción	Habilidades requeridas
	4. En Nombre, escriba `lambda_write_function` . 5. En Runtime (Tiempo de ejecución), elija Python 3.8 o una versión más reciente. 6. En Cambiar rol de ejecución predeterminado, seleccione Usar un rol existente. 7. En Rol existente, elija el rol de IAM que creó, como `DynamoDB-PutItemAccess` . 8. Elija Crear función. 9. En la pestaña Código, pegue el código de ejemplo que se proporciona en la sección Información adicional de este patrón. Sustituya lo siguiente en el código de muestra: • `<Account-A-ID>` es el ID de la cuenta A. • `<Region>`es Región de AWS donde creó la tabla de DynamoDB. 10. Elija Implementar. 11. Seleccione Probar Esto le pide que configure un evento de prueba. Cree un evento nuevo con el nombre que prefiera, como	

Tarea	Descripción	Habilidades requeridas
	`MyTestEventForWrite`, y guarde la configuración. 12. Elija Test (Probar) de nuevo. Esto ejecuta la función de Lambda con el nombre del evento que ha proporcionado. 13. Compruebe el resultado de la función. Esto indica que la función accedió a la tabla de DynamoDB en la cuenta A y pudo escribir datos en ella. Para obtener más información sobre la creación de funciones de Lambda, consulte la documentación de Lambda.	

Limpieza

Tarea	Descripción	Habilidades requeridas
Delete resources (Eliminar recursos).	Para evitar generar costos asociados a los recursos creados con este patrón, haga lo siguiente para eliminar los recursos: 1. En la cuenta B, elimine la función de Lambda que haya creado para conectarse a DynamoDB.	AWS general

Tarea	Descripción	Habilidades requeridas
	Para obtener instrucciones, consulte la documentación de Lambda. 2. En la cuenta A, elimine la tabla de DynamoDB que creó. Para obtener instrucciones, consulte la documentación de DynamoDB. 3. Para seguir las prácticas recomendadas de seguridad, elimine la política de IAM (`DynamoDB-PutItem-Policy`) cuando ya no sea necesaria. Para obtener más información, consulte la documentación de IAM. 4. Para seguir las prácticas recomendadas de seguridad, elimine el rol de IAM (`DynamoDB-PutItemAccess`) cuando ya no sea necesario. Para obtener más información, consulte la documentación de IAM.	

Resolución de problemas

Problema	Solución
Al crear la función de Lambda, recibe un error `ResourceNotFoundException` .	Confirme que ha introducido correctamente el ID Región de AWS y el ID de la cuenta A. Forman parte del ARN de la tabla de DynamoDB.

Recursos relacionados

- Introducción a DynamoDB (documentación de DynamoDB)
- Introducción a Lambda (documentación de Lambda)
- Uso de políticas basadas en recursos de DynamoDB (documentación de DynamoDB)
- Creación de políticas de IAM (documentación de IAM)
- Lógica de evaluación de políticas entre cuentas (documentación de IAM)
- Referencia de los elementos de las políticas de JSON de IAM (documentación de IAM)

Información adicional

Código de muestra

```
import boto3
from datetime import datetime

dynamodb_client = boto3.client('dynamodb')

def lambda_handler(event, context):
     now = datetime.now().isoformat()
     data = dynamodb_client.put_item(TableName='arn:aws:dynamodb:<Region>:<Account-
A-ID>:table/Table-Account-A', Item={"category": {"S": "Fruit"},"item": {"S":
 "Apple"},"time": {"S": now}})
     return data
```

> **Note**
>
> Cuando se crea el cliente de DynamoDB, se proporciona el ARN de la tabla de DynamoDB en lugar del nombre de la tabla. Esto es necesario para que la función de Lambda se conecte a la tabla de DynamoDB correcta cuando se ejecute.

Configurar el enrutamiento de solo lectura en los grupos de disponibilidad de Always On en SQL Server on AWS

Subhani Shaik, Amazon Web Services

Resumen

Este patrón explica cómo usar la réplica secundaria en espera en SQL Server Always On descargando las cargas de trabajo de solo lectura de la réplica principal a la réplica secundaria.

La duplicación de bases de datos tiene mapeo. one-to-one No puede leer la base de datos secundaria directamente, por lo que debe crear instantáneas. La característica de grupo de disponibilidad Always On se introdujo en Microsoft SQL Server 2012. En versiones posteriores se han introducido importantes funcionalidades, incluido el enrutamiento de solo lectura. En los grupos de disponibilidad de Always On, puede leer los datos directamente desde la réplica secundaria cambiando el modo de réplica a uno de solo lectura.

La solución de grupos de disponibilidad Always On ofrece alta disponibilidad (HA), recuperación de desastres (DR) y una alternativa a la duplicación de bases de datos. Los grupos de disponibilidad Always On funcionan a nivel de base de datos, y maximizan la disponibilidad de un conjunto de bases de datos de usuarios.

SQL Server emplea el mecanismo de enrutamiento de solo lectura para redirigir las conexiones entrantes de solo lectura a la réplica de lectura secundaria. Para ello, debe agregar los siguientes parámetros y valores en la cadena de conexión:

- `ApplicationIntent=ReadOnly`
- `Initial Catalog=<database name>`

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS con una nube privada virtual (VPC), dos zonas de disponibilidad, subredes privadas y un grupo de seguridad
- Dos máquinas Amazon Elastic Compute Cloud (Amazon EC2) con SQL Server 2019 Enterprise Edition Amazon Machine Image con clústeres de conmutación por error de Windows Server (WSFC) configurados a nivel de instancia y un grupo de disponibilidad Always On configurado a

nivel de SQL Server entre el nodo principal `WSFCNODE1` () y el nodo secundario (), que forman parte del `WSFCNODE2` directorio denominado AWS Directory Service for Microsoft Active Directory `tagechtalk.com`

- Uno o más nodos configurados para aceptar `read-only` en la réplica secundaria
- Un oyente con el nombre `SQLAG1` para el grupo de disponibilidad Always On
- SQL Server Database Engine en ejecución con la misma cuenta de servicio en dos nodos
- SQL Server Management Studio (SSMS)
- Una base de datos de prueba llamada `test`

Versiones de producto

- SQL Server 2014 y versiones posteriores

Arquitectura

Pila de tecnología de destino

- Amazon EC2
- AWS Managed Microsoft AD
- Amazon FSx

Arquitectura de destino

El siguiente diagrama muestra cómo el oyente del grupo de disponibilidad (AG) Always On redirige las consultas que contienen el parámetro `ApplicationIntent` en la conexión al nodo secundario correspondiente.

1. Se envía una solicitud al oyente del grupo de disponibilidad Always On.
2. Si la cadena de conexión no tiene el parámetro `ApplicationIntent`, la solicitud se envía a la instancia principal.
3. Si la cadena de conexión lo contiene`ApplicationIntent=ReadOnly`, la solicitud se envía a la instancia secundaria con una configuración de enrutamiento de solo lectura, que es un WSFC con un grupo de disponibilidad Always On.

Tools (Herramientas)

Servicios de AWS

- AWS Directory Service for Microsoft Active Directorypermite que sus cargas de trabajo y AWS recursos compatibles con directorios utilicen Microsoft Active Directory en. Nube de AWS
- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon FSx proporciona sistemas de archivos que admiten los protocolos de conectividad estándares del sector y ofrecen alta disponibilidad y replicación en todos Regiones de AWS los niveles.

Otros servicios

- SQL Server Management Studio (SSMS) es una herramienta para conectar, gestionar y administrar instancias de SQL Server.
- sqlcmd es una utilidad de línea de comandos.

Prácticas recomendadas

Para obtener más información sobre los grupos de disponibilidad Always On, consulte la documentación de SQL Server.

Epics

Configure el enrutamiento de solo lectura

Tarea	Descripción	Habilidades requeridas
Actualice las réplicas a solo lectura.	Para actualizar la réplica principal y la secundaria a solo lectura, conéctese a la réplica principal desde SSMS y ejecute el código del Paso 1 que encontrará en la sección de Información adicional.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree la URL de enrutamiento.	Para crear la URL de enrutamiento para ambas réplicas, ejecute el código del Paso 2 que encontrará en la sección de Información adicional. En este código, `tagechtalk.com` es el nombre del AWS Managed Microsoft AD directorio.	Administrador de base de datos
Cree la lista de enrutamiento.	Para crear la lista de enrutamiento para ambas réplicas, ejecute el código del paso 3 de la sección de información adicional.	Administrador de base de datos
Valide la lista de enrutamiento.	Conéctese a la instancia principal desde SQL Server Management Studio y ejecute el código del Paso 4 que encontrará en la sección de Información adicional para validar la lista de enrutamiento.	Administrador de base de datos

Pruebe el enrutamiento de solo lectura

Tarea	Descripción	Habilidades requeridas
Conéctese mediante el `ApplicationIntent` parámetro.	1. Desde SSMS, conéctese al nombre de oyente del grupo de disponibilidad Always On con `ApplicationIntent=ReadOnly;`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	`Initial Catalog=test .`
	2. Se establecerá una conexión con la réplica secundaria. Para realizar la prueba, ejecute el siguiente comando para mostrar el nombre del servidor conectado.
	`SELECT SERVERPROPERTY('ComputerNamePhysicalNetBios')`
	El resultado devolverá el nombre de la réplica secundaria actual (`WSFCNODE2 `).	

Tarea	Descripción	Habilidades requeridas
Realice una conmutación por error.	1. Desde SSMS, conéctese al nombre de oyente del grupo de disponibilidad Always On. 2. Compruebe que las bases de datos principal y secundaria estén sincronizadas y que no se pierdan datos. 3. Realice una conmutación por error para que la réplica principal actual pase a ser la réplica secundaria, y la réplica secundaria pase a ser la réplica principal. 4. Desde SSMS, conéctese al nombre de oyente del grupo de disponibilidad Always On con `ApplicationIntent=ReadOnly; Initial Catalog=test` . 5. Se establecerá una conexión con la réplica secundaria. Para realizar la prueba, ejecute el siguiente comando para mostrar el nombre del servidor conectado. `SELECT SERVERPROPERTY('ComputerNamePhysicalNetBios')`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Se mostrará el nombre de la réplica secundaria actual (`WSFCNODE1 `).	

Conéctese mediante la utilidad de línea de comandos sqlcmd

Tarea	Descripción	Habilidades requeridas
Conéctese mediante sqlcmd.	Para conectarse desde sqlcmd, ejecute el código del Paso 5 que encontrará en la sección de Información adicional en la línea de comandos. Después de conectarse, ejecute el siguiente comando para mostrar el nombre del servidor conectado. `SELECT SERVERPROPERTY('ComputerNamePhysicalNetBios') .` El resultado devolverá el nombre de la réplica secundaria actual (`WSFCNODE1 `).	Administrador de base de datos

Resolución de problemas

Problema	Solución
No se puede crear el oyente y aparece el mensaje “El clúster WSFC no ha podido poner en línea el recurso Nombre de red”.	Para mayor información, consulte el blog de Microsoft La creación del oyente dio el mensaje de error: “el clúster WSFC no ha podido poner en línea el recurso Nombre de red”.
Posibles problemas, incluidos otros problemas con los oyentes o problemas de acceso a la red.	Consulte Solución de problemas de configuración de grupos de disponibilidad Always On (SQL Server) en la documentación de Microsoft .

Recursos relacionados

- Configure el enrutamiento de solo lectura en un grupo de disponibilidad Always On
- Consulte Solución de problemas de configuración de grupos de disponibilidad Always On (SQL Server)

Información adicional

Paso 1. Actualice las réplicas a solo lectura

```
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE1' WITH (SECONDARY_ROLE
 (ALLOW_CONNECTIONS = READ_ONLY))
GO
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE2' WITH (SECONDARY_ROLE
 (ALLOW_CONNECTIONS = READ_ONLY))
GO
```

Paso 2. Cree la URL de enrutamiento

```
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE1' WITH (SECONDARY_ROLE
 (READ_ONLY_ROUTING_URL = N'TCP://WSFCNode1.tagechtalk.com:1433'))
GO
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE2' WITH (SECONDARY_ROLE
 (READ_ONLY_ROUTING_URL = N'TCP://WSFCNode2.tagechtalk.com:1433'))
```

```
GO
```

Paso 3. Cree la URL de enrutamiento

```
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE1' WITH
 (PRIMARY_ROLE(READ_ONLY_ROUTING_LIST=('WSFCNODE2','WSFCNODE1')));
GO
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE2' WITH (PRIMARY_ROLE
 (READ_ONLY_ROUTING_LIST=('WSFCNODE1','WSFCNODE2')));
GO
```

Paso 4. Cree la lista de enrutamiento

```
SELECT AGSrc.replica_server_name AS PrimaryReplica, AGRepl.replica_server_name AS
 ReadOnlyReplica, AGRepl.read_only_routing_url AS RoutingURL , AGRL.routing_priority
 AS RoutingPriority FROM sys.availability_read_only_routing_lists AGRL INNER JOIN
 sys.availability_replicas AGSrc ON AGRL.replica_id = AGSrc.replica_id INNER JOIN
 sys.availability_replicas AGRepl ON AGRL.read_only_replica_id = AGRepl.replica_id
 INNER JOIN sys.availability_groups AV ON AV.group_id = AGSrc.group_id ORDER BY
 PrimaryReplica
```

Paso 5. Utilidad de comandos SQL

```
sqlcmd -S SQLAG1,1433 -E -d test -K ReadOnly
```

Conectar mediante un túnel SSH en pgAdmin

Jeevan Shetty y Bhanu Ganesh Gudivada, Amazon Web Services

Resumen

Por motivos de seguridad, siempre es bueno colocar las bases de datos en una subred privada. Las consultas a la base de datos se pueden ejecutar conectándose a través de un host bastión de Amazon Elastic Compute Cloud (Amazon EC2) en una subred pública de la nube de Amazon Web Services (AWS). Esto requiere la instalación de software, como pgAdmin DBeaver o, que suelen utilizar los desarrolladores o administradores de bases de datos, en el host de Amazon. EC2

Ejecutar pgAdmin en un servidor Linux y acceder a él a través de un navegador web requiere la instalación de dependencias adicionales y la configuración de permisos.

Como solución alternativa, los desarrolladores o administradores de bases de datos pueden conectarse a una base de datos PostgreSQL mediante pgAdmin para habilitar un túnel SSH desde su sistema local. En este enfoque, pgAdmin utiliza el host de EC2 Amazon en la subred pública como host intermediario antes de conectarse a la base de datos. El diagrama de la sección de arquitectura muestra la configuración.

> **Note**
>
> Asegúrese de que el grupo de seguridad adjunto a la base de datos de PostgreSQL permita la conexión en el puerto 5432 desde el host de Amazon. EC2

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS existente
- Una nube privada virtual (VPC) con una subred pública y una subred privada
- Una EC2 instancia con un grupo de seguridad adjunto
- Base de datos de la edición compatible con Amazon Aurora PostgreSQL con un grupo de seguridad adjunto
- Un par de claves Secure Shell (SSH) para configurar el túnel

Versiones de producto

- pgAdmin versión 6.2+
- Amazon Aurora, edición compatible con PostgreSQL, versión 12.7+

Arquitectura

Pila de tecnología de destino

- Amazon EC2
- Amazon Aurora compatible con PostgreSQL

Arquitectura de destino

El siguiente diagrama muestra el uso de pgAdmin con un túnel SSH para conectarse a través de una puerta de enlace de Internet a EC2 la instancia, que se conecta a la base de datos.

Tools (Herramientas)

Servicios de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.

Otros servicios

- pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.

Epics

Creación de la conexión

Tarea	Descripción	Habilidades requeridas
Cree un servidor.	En pgAdmin, seleccione Crear y, a continuación, Servidor. Para obtener ayuda adicional sobre la configuración de pgAdmin para registrar un servidor, configurar una conexión y conectarse a través de un túnel SSH mediante el cuadro de diálogo del servidor, consulte los enlaces de la sección Recursos relaciona dos.	Administrador de base de datos
Proporcione un nombre para el servidor.	En la pestaña General, introduzca un nombre.	Administrador de base de datos
Ingrese los detalles de base de datos.	En la pestaña Conexión, introduzca los valores siguientes: • Nombre/dirección del host • Puerto • Mantenimiento de bases de datos • Nombre de usuario • Contraseña	Administrador de base de datos
Introduce los detalles EC2 del servidor de Amazon.	En la pestaña Túnel SSH, proporciona los detalles de la EC2 instancia de Amazon	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	que se encuentra en la subred pública. • Establezca Usar túnel SSH en Sí para especificar que pgAdmin debe usar un túnel SSH al conectarse al servidor especificado. • En el campo Host del túnel, especifique el nombre o la dirección IP del host SSH (por ejemplo, 10.x.x.x). • En el campo Puerto del túnel, especifique el puerto del host SSH (por ejemplo, 22). • En el campo Nombre de usuario, introuzca el nombre de un usuario con privilegi os de inicio de sesión en el host SSH (por ejemplo, ec2-user). • Especifique el tipo de autenticación como archivo de identidad para que PGAdmin utilice un archivo de clave privada al conectarse. • Incluya la ubicación del archivo Privacy Enhanced Mail (PEM) en el campo del archivo de identidad . El archivo.pem es el	

Tarea	Descripción	Habilidades requeridas
	par de EC2 claves de Amazon.	
Guardar y conectar.	Seleccione Guardar para completar la configuración y conectarse a la base de datos Aurora compatible con PostgreSQL mediante el túnel SSH.	Administrador de base de datos

Recursos relacionados

- Diálogo del servidor
- Conectar al servidor

Convertir consultas JSON de Oracle en SQL de bases de datos PostgreSQL

Pinesh Singal y Lokesh Gurram, Amazon Web Services

Resumen

Este proceso de migración para pasar del entorno local a la nube de Amazon Web Services (AWS) utiliza la herramienta de conversión de esquemas de AWS (AWS SCT) para convertir el código de una base de datos Orqacle en una base de datos PostgreSQL. AWS SCT convierte automáticamente la mayor parte del código. Sin embargo, las consultas de Oracle relacionadas con JSON no se convierten automáticamente.

A partir de la versión 12.2 de Oracle, Oracle Database admite varias funciones de JSON que ayudan a convertir los datos basados en JSON en datos basados en filas. Sin embargo, AWS SCT no convierte automáticamente los datos basados en JSON a un lenguaje compatible con PostgreSQL.

Este patrón de migración se centra principalmente en convertir manualmente las consultas de Oracle relacionadas con JSON con funciones como `JSON_OBJECT`, `JSON_ARRAYAGG`, y `JSON_TABLE` de una base de datos de Oracle a una base de datos PostgreSQL.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una instancia de base de datos de Oracle local (en funcionamiento)
- Una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para la Edición compatible con PostgreSQL o Amazon Aurora

Limitaciones

- Las consultas relacionadas con JSON requieren un formato AND fijo `KEY` y `VALUE`. Si no se utiliza ese formato, se obtiene un resultado incorrecto.
- Si algún cambio en la estructura de JSON añade pares nuevos `KEY` y `VALUE`en la sección de resultados, se debe cambiar el procedimiento o la función correspondiente en la consulta SQL.
- Algunas funciones relacionadas con JSON se admiten en versiones anteriores de Oracle y PostgreSQL, pero con menos capacidades.

Versiones de producto

- Oracle Database, versión 12.2 y posterior
- Amazon RDS para PostgreSQL o Aurora, compatible con PostgreSQL, versión 9.5 y versiones posteriores
- Última versión de AWS SCT (probadas con la versión 1.0.664)

Arquitectura

Pila de tecnología de origen

- Una instancia de base de datos de Oracle con la versión 19c

Pila de tecnología de destino

- Una instancia de base de datos compatible con Amazon RDS para PostgreSQL o Aurora PostgreSQL con la versión 13

Arquitectura de destino

1. Utilice AWS SCT con el código de función JSON para convertir el código fuente de Oracle a PostgreSQL.
2. La conversión produce archivos.sql migrados compatibles con PostgreSQL.
3. Convierta manualmente los códigos de función JSON de Oracle no convertidos en códigos de función JSON de PostgreSQL.
4. Ejecute los archivos.sql en la instancia de base de datos compatible con PostgreSQL de Aurora de destino.

Tools (Herramientas)

Servicios de AWS

- Amazon Aurora es un motor de base de datos relacional completamente administrado diseñado para la nube y compatible con MySQL y PostgreSQL.

- Amazon Relational Database Service (Amazon RDS) para PostgreSQL le ayuda a configurar, utilizar y escalar una base de datos relacional de PostgreSQL en la nube de AWS.
- La Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado, lo que incluye las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino.

Otros servicios

- Oracle SQL Developer es un entorno de desarrollo integrado que simplifica el desarrollo y la administración de bases de datos de Oracle, tanto en implementaciones tradicionales como en implementaciones basadas en la nube.
- pgAdmin o. DBeaver pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que le ayuda a crear, mantener y utilizar objetos de bases de datos. DBeaveres una herramienta de base de datos universal.

Prácticas recomendadas

La consulta de Oracle tiene el tipo `CAST` como valor predeterminado cuando se utiliza la función `JSON_TABLE`. Una buena práctica es utilizarla también `CAST` en PostgreSQL, utilizando caracteres dobles mayores que (>>).

Para obtener más información, consulte Postgres_SQL_read_JSON en la sección Información adicional.

Epics

Genere los datos JSON en las bases de datos de Oracle y PostgreSQL

Tarea	Descripción	Habilidades requeridas
Guarde los datos JSON en la base de datos de Oracle.	Cree una tabla en la base de datos de Oracle y almacene los datos JSON en la columna `CLOB`. Utilice el Oracle_Table_Creation_Insert_Script que	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	se encuentra en la sección Información adicional.	
Guarde los datos JSON en la base de datos PostgreSQL.	Cree una tabla en la base de datos PostgreSQL y almacene los datos JSON en la columna `TEXT`. Utilice el archivo Postgres_Table_Creation_Insert_Script que se encuentra en la sección Información adicional.	Ingeniero de migraciones

Convierte el JSON al formato ROW

Tarea	Descripción	Habilidades requeridas
Convertir los datos JSON en la base de datos de Oracle.	Escriba una consulta SQL de Oracle para leer los datos JSON en formato ROW. Para obtener más detalles y ejemplos de sintaxis, consulte Oracle_SQL_read_JSON en la sección Información adicional.	Ingeniero de migraciones
Convierta los datos JSON en la base de datos PostgreSQL.	Escriba una consulta de PostgreSQL para leer los datos JSON en formato ROW. Para obtener más detalles y ejemplos de sintaxis, consulte Oracle_SQL_read_JSON en la sección Información adicional.	Ingeniero de migraciones

Convertir manualmente los datos JSON mediante la consulta SQL e informe el resultado en formato JSON

Tarea	Descripción	Habilidades requeridas
Realizar agregaciones y validaciones en la consulta SQL de Oracle.	Para convertir manualmente los datos de JSON, realice una unión, agregación y validación en la consulta SQL de Oracle e informe el resultado en formato JSON. Utilice el código que aparece en Oracle_SQL_JSON_Aggregation_JOIN en la sección Información adicional. 1. JOIN: los datos con formato JSON se pasan como parámetro de entrada a la consulta. Se realiza una unión interna entre estos datos estáticos y los datos JSON de la tabla de base de datos de Oracle `aws_test_table` . 2. Agregación con validación: los datos JSON tienen `KEY VALUE` parámetros con valores como `accountNumber` , `parentAccountNumber` , `businessUnitId` y `positionId` , que se utilizan para las agregaciones `SUM` y `COUNT`. 3. Formato JSON: después de la unión y la agregació	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	n, los datos se presentan en formato JSON mediante `JSON_OBJECT` y `JSON_ARRAYAGG` .	

Tarea	Descripción	Habilidades requeridas
Realice agregaciones y validaciones en la consulta SQL de Postgres.	Para convertir manualmente los datos de JSON, realice una unión, agregación y validación en la consulta de PostgreSQL e informe el resultado en formato JSON. Use el código que aparece en Postgres_SQL_JSON_AGGREGATION_JOIN en la sección Información adicional. 1. JOIN: los datos con formato JSON (`tab1`) se pasan como parámetro de entrada a la consulta de la cláusula `WITH`. Se realiza una unión entre estos datos estáticos y los datos JSON, que se encuentran en la tabla `tab`. También se hace una unión con la cláusula `WITH`, que contiene datos de JSON en la tabla `aws_test_pg_table` . 2. Agregación: los datos de JSON tienen parámetros `KEY` y `VALUE` con valores como `accountNumber` , `parentAccountNumber` , `businessUnitId` , y `positionId` , que se utilizan para las agregaciones `SUM` y `COUNT`.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	3. Formato JSON: después de la unión y la agregación, los datos se presentan en formato JSON mediante `JSON_BUILD_OBJECT` y `JSON_AGG`.	

Convertir el procedimiento de Oracle en una función de PostgreSQL que contenga consultas JSON

Tarea	Descripción	Habilidades requeridas
Convierta las consultas JSON del procedimiento de Oracle en filas.	Para el procedimiento de Oracle de ejemplo, utilice la consulta de Oracle anterior y el código de Oracle_Procedure_with_JSON_Query en la sección Información adicional.	Ingeniero de migraciones
Convierta las funciones de PostgreSQL que tienen consultas JSON en datos basados en filas.	Para las funciones de PostgreSQL de ejemplo, utilice la consulta de PostgreSQL anterior y el código que se encuentra en Postgres_function_with_JSON_Query en la sección Información adicional.	Ingeniero de migraciones

Recursos relacionados

- Funciones JSON de Oracle
- Funciones JSON de PostgreSQL
- Ejemplos de funciones JSON de Oracle

- Ejemplos de funciones JSON de PostgreSQL
- Herramienta de conversión de esquemas de AWS

Información adicional

Para convertir el código JSON de la base de datos de Oracle a la base de datos PostgreSQL, utilice los siguientes scripts en orden.

1. Oracle_Table_Creation_Insert_Script

```
create table aws_test_table(id number,created_on date default sysdate,modified_on
 date,json_doc clob);

REM INSERTING into EXPORT_TABLE
SET DEFINE OFF;
Insert into aws_test_table (ID,CREATED_ON,MODIFIED_ON,json_doc)
values (1,to_date('02-AUG-2022 12:30:14','DD-MON-YYYY HH24:MI:SS'),to_date('02-AUG-2022
 12:30:14','DD-MON-YYYY HH24:MI:SS'),TO_CLOB(q'[{
  "metadata" : {
    "upperLastNameFirstName" : "ABC XYZ",
    "upperEmailAddress" : "abc@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "032323323",
    "displayName" : "Abc, Xyz",
    "firstName" : "Xyz",
    "lastName" : "Abc",
    "emailAddress" : "abc@gmail.com",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0100",
    "arrayPattern" : " -'",
    "a]')
|| TO_CLOB(q'[ccount" : {
      "companyId" : "SMGE",
      "businessUnitId" : 7,
      "accountNumber" : 42000,
      "parentAccountNumber" : 32000,
      "firstName" : "john",
      "lastName" : "doe",
      "street1" : "retOdertcaShr ",
      "city" : "new york",
```

```
      "postalcode" : "XY ABC",
      "country" : "United States"
    },
    "products" : [
      {
        "appUserGuid" : "i0acc4450000001823fbad478e2eab8a0",
        "id" : "0000000046",
]')
|| TO_CLOB(q'[        "name" : "ProView",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}]'));
Insert into aws_test_table (ID,CREATED_ON,MODIFIED_ON,json_doc) values (2,to_date('02-
AUG-2022 12:30:14','DD-MON-YYYY HH24:MI:SS'),to_date('02-AUG-2022 12:30:14','DD-MON-
YYYY HH24:MI:SS'),TO_CLOB(q'[{
  "metadata" : {
    "upperLastNameFirstName" : "PQR XYZ",
    "upperEmailAddress" : "pqr@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "54534343",
    "displayName" : "Xyz, pqr",
    "firstName" : "pqr",
    "lastName" : "Xyz",
    "emailAddress" : "pqr@gmail.com",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0090",
    "arrayPattern" : " -'",
    "account" : {
      "companyId" : "CARS",
      "busin]')
|| TO_CLOB(q'[essUnitId" : 6,
      "accountNumber" : 42001,
      "parentAccountNumber" : 32001,
      "firstName" : "terry",
      "lastName" : "whitlock",
      "street1" : "UO  123",
      "city" : "TOTORON",
      "region" : "NO",
```

```
      "postalcode" : "LKM 111",
      "country" : "Canada"
    },
    "products" : [
      {
        "appUserGuid" : "ia744d7790000016899f8cf3f417d6df6",
        "id" : "0000000014",
        "name" : "ProView eLooseleaf",
      ]')
|| TO_CLOB(q'[  "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}]'));

commit;
```

2. Postgres_Table_Creation_Insert_Script

```
create table aws_test_pg_table(id int,created_on date ,modified_on date,json_doc text);
insert into aws_test_pg_table(id,created_on,modified_on,json_doc)
values(1,now(),now(),'{
  "metadata" : {
    "upperLastNameFirstName" : "ABC XYZ",
    "upperEmailAddress" : "abc@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "032323323",
    "displayName" : "Abc, Xyz",
    "firstName" : "Xyz",
    "lastName" : "Abc",
    "emailAddress" : "abc@gmail.com",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0100",
    "arrayPattern" : " -",
    "account" : {
      "companyId" : "SMGE",
      "businessUnitId" : 7,
      "accountNumber" : 42000,
      "parentAccountNumber" : 32000,
```

```
      "firstName" : "john",
      "lastName" : "doe",
      "street1" : "retOdertcaShr ",
      "city" : "new york",
      "postalcode" : "XY ABC",
      "country" : "United States"
    },
    "products" : [
      {
        "appUserGuid" : "i0acc4450000001823fbad478e2eab8a0",
        "id" : "0000000046",
        "name" : "ProView",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}');


insert into aws_test_pg_table(id,created_on,modified_on,json_doc)
values(2,now(),now(),'{
  "metadata" : {
    "upperLastNameFirstName" : "PQR XYZ",
    "upperEmailAddress" : "pqr@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "54534343",
    "displayName" : "Xyz, pqr",
    "firstName" : "pqr",
    "lastName" : "Xyz",
    "emailAddress" : "a*b**@h**.k**",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0090",
    "arrayPattern" : " -",
    "account" : {
      "companyId" : "CARS",
      "businessUnitId" : 6,
      "accountNumber" : 42001,
      "parentAccountNumber" : 32001,
      "firstName" : "terry",
      "lastName" : "whitlock",
```

```
      "street1" : "UO  123",
      "city" : "TOTORON",
      "region" : "NO",
      "postalcode" : "LKM 111",
      "country" : "Canada"
    },
    "products" : [
      {
        "appUserGuid" : "ia744d7790000016899f8cf3f417d6df6",
        "id" : "0000000014",
        "name" : "ProView eLooseleaf",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}');
```

3. Oracle_SQL_READ_JSON

Los siguientes bloques de código muestran cómo convertir los datos JSON de Oracle a formato de fila.

Ejemplo de consulta y sintaxis

```
SELECT   JSON_OBJECT(
 'accountCounts' VALUE JSON_ARRAYAGG(
           JSON_OBJECT(
               'businessUnitId' VALUE business_unit_id,
                       'parentAccountNumber' VALUE parent_account_number,
                       'accountNumber' VALUE account_number,
                       'totalOnlineContactsCount' VALUE online_contacts_count,
                       'countByPosition' VALUE
                   JSON_OBJECT(
                       'taxProfessionalCount' VALUE tax_count,
                       'attorneyCount' VALUE attorney_count,
                       'nonAttorneyCount' VALUE non_attorney_count,
                       'clerkCount' VALUE clerk_count
                              ) ) ) ) FROM
    (SELECT   tab_data.business_unit_id,
           tab_data.parent_account_number,
           tab_data.account_number,
```

```
           SUM(1) online_contacts_count,
           SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE 0 END) tax_count,
           SUM(CASE    WHEN tab_data.position_id = '0100' THEN 1 ELSE 0 END)
attorney_count,
           SUM(CASE    WHEN tab_data.position_id = '0090' THEN 1 ELSE 0 END)
non_attorney_count,
           SUM(CASE    WHEN tab_data.position_id = '0050' THEN 1 ELSE 0 END)
clerk_count
       FROM aws_test_table scco,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
COLUMNS (
         parent_account_number NUMBER PATH
          '$.data.account.parentAccountNumber',
           account_number NUMBER PATH '$.data.account.accountNumber',
           business_unit_id NUMBER PATH '$.data.account.businessUnitId',
           position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
           ) AS tab_data
           INNER JOIN JSON_TABLE ( '{
       "accounts": [{
         "accountNumber": 42000,
         "parentAccountNumber": 32000,
         "businessUnitId": 7
       }, {
         "accountNumber": 42001,
         "parentAccountNumber": 32001,
         "businessUnitId": 6
       }]
     }', '$.accounts[*]' ERROR ON ERROR
     COLUMNS (
     parent_account_number PATH '$.parentAccountNumber',
     account_number PATH '$.accountNumber',
     business_unit_id PATH '$.businessUnitId')
     ) static_data
     ON ( static_data.parent_account_number = tab_data.parent_account_number
          AND static_data.account_number = tab_data.account_number
          AND static_data.business_unit_id = tab_data.business_unit_id )
       GROUP BY
           tab_data.business_unit_id,
           tab_data.parent_account_number,
           tab_data.account_number );
```

El documento JSON almacena los datos como colecciones. Cada colección puede tener pares KEY y VALUE. Cada VALUE puede tener anidados pares KEY y VALUE. En la siguiente tabla se proporciona información sobre la lectura del VALUE específico del documento JSON.

KEY	HIERARCHY or PATH to be used to get the VALUE	VALUE
`profileType`	`metadata` -> `profileType`	«P»
`positionId`	`data` -> `positionId`	«0100»
`accountNumber`	`data` -> account -> `accountNumber`	42000

En la tabla anterior, KEY `profileType` es una VALUE de las `metadata` KEY. El KEY `positionId` es un VALUE de los `data` KEY. El KEY `accountNumber` es un VALUE de los `account`KEY, y el `account` KEY es un VALUE de los `data`KEY.

Ejemplo de documento JSON

```
{
  "metadata" : {
    "upperLastNameFirstName" : "ABC XYZ",
    "upperEmailAddress" : "abc@gmail.com",
"profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "032323323",
    "displayName" : "Abc, Xyz",
    "firstName" : "Xyz",
    "lastName" : "Abc",
    "emailAddress" : "abc@gmail.com",
    "productRegistrationStatus" : "Not registered",
"positionId" : "0100",
    "arrayPattern" : " -",
    "account" : {
      "companyId" : "SMGE",
      "businessUnitId" : 7,
"accountNumber" : 42000,
      "parentAccountNumber" : 32000,
      "firstName" : "john",
      "lastName" : "doe",
      "street1" : "retOdertcaShr ",
      "city" : "new york",
      "postalcode" : "XY ABC",
```

```
      "country" : "United States"
    },
    "products" : [
      {
        "appUserGuid" : "i0acc4450000001823fbad478e2eab8a0",
        "id" : "0000000046",
        "name" : "ProView",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}
```

Consulta SQL que se utiliza para obtener los campos seleccionados del documento JSON

```
select parent_account_number,account_number,business_unit_id,position_id from
 aws_test_table aws,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
COLUMNS (
parent_account_number NUMBER PATH '$.data.account.parentAccountNumber',
account_number NUMBER PATH '$.data.account.accountNumber',
business_unit_id NUMBER PATH '$.data.account.businessUnitId',
position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'
)) as sc
```

En la consulta anterior, `JSON_TABLE` es una función integrada en Oracle que convierte los datos JSON en formato de fila. La función JSON_TABLE espera parámetros en formato JSON.

Cada elemento `COLUMNS` tiene un valor predefinido `PATH`, y cuando hay un `VALUE` adecuado para un determinado elemento `KEY`, se devuelve en formato de fila.

Resultado de la consulta anterior

PARENT_AC COUNT_NUMBER	ACCOUNT_NUMBER	BUSINESS_UNIT_ID	POSITION_ID
32000	42000	7	0100
32001	42001	6	0090

4. Postgres_SQL_READ_JSON

Ejemplo de consulta y sintaxis

```
select *
from (
select (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER as
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER as accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER as businessUnitId,
(json_doc::json->'data'->>'positionId')::VARCHAR as positionId
from aws_test_pg_table) d ;
```

En Oracle, `PATH` se utiliza para identificar el `KEY` y `VALUE` especifico. Sin embargo, PostgreSQL utiliza un modelo `HIERARCHY` para leer `KEY` y `VALUE` desde JSON. Los mismos datos de JSON que se mencionan en `Oracle_SQL_Read_JSON` se utilizan en los siguientes ejemplos.

No se admiten consultas SQL de tipo CAST

(Si fuerza el tipo de texto `CAST`, la consulta fallará y se producirá un error de sintaxis).

```
select *
from (
select (json_doc::json->'data'->'account'->'parentAccountNumber') as
 parentAccountNumber,
(json_doc::json->'data'->'account'->'accountNumber')as accountNumber,
(json_doc::json->'data'->'account'->'businessUnitId') as businessUnitId,
(json_doc::json->'data'->'positionId')as positionId
from aws_test_pg_table) d ;
```

Si se utiliza un operador una vez mayor (>), se devolverá el `VALUE` definido para ese `KEY`. Por ejemplo, `KEY`: `positionId`, y `VALUE`: `"0100"`.

No se permite escribir el tipo `CAST` cuando se utiliza el operador una vez mayor (>).

Se admiten consultas SQL de tipo CAST

```
select *
from (
select (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER as
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER as accountNumber,
```

```
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER as businessUnitId,
(json_doc::json->'data'->>'positionId')::varchar as positionId
from aws_test_pg_table) d ;
```

Para usar el tipo `CAST`, debe usar un operador mayor del doble. Si utiliza el operador una vez mayor, la consulta devuelve el `VALUE` definido (por ejemplo `KEY`: `positionId`, y `VALUE`: `"0100"`). Si se utiliza el operador mayor del doble (>>), se devolverá el valor real definido para ese valor `KEY` (por ejemplo, `KEY`: `positionId`, y `VALUE`: `0100` sin comillas dobles).

En el caso anterior, `parentAccountNumber` es el tipo `CAST` a `INT`, `accountNumber` es el tipo `CAST` a `INT`, `businessUnitId` es el tipo `CAST` a `INT`, y `positionId` es el tipo `CAST` a `VARCHAR`.

En las tablas siguientes se muestran los resultados de las consultas que explican el papel del operador único mayor que (>) y del operador doble mayor que (>>).

En la primera tabla, la consulta utiliza el único operador mayor que (>). Cada columna es de tipo JSON y no se puede convertir en otro tipo de datos.

parentAccountNumber	Número de cuenta	businessUnitId	ID de puesto
2003565430	2003564830	7	«0100»
2005284042	2005284042	6	“0090”
2000272719	2000272719	1	«0100»

En la segunda tabla, la consulta utiliza el operador doble mayor que (>>). Cada columna admite el tipo `CAST` en función del valor de la columna. Por ejemplo, en este caso `INTEGER`.

parentAccountNumber	Número de cuenta	businessUnitId	ID de puesto
2003565430	2003564830	7	0100
2005284042	2005284042	6	0090
2000272719	2000272719	1	0100

5. Oracle_SQL_JSON_AGGREGATION_JOIN

Consulta de ejemplo

```
SELECT
    JSON_OBJECT(
        'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               ) ) ) )
FROM
    (SELECT
             tab_data.business_unit_id,
             tab_data.parent_account_number,
             tab_data.account_number,
             SUM(1) online_contacts_count,
             SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE 0 END) tax_count,
             SUM(CASE    WHEN tab_data.position_id = '0100' THEN 1 ELSE 0 END)
 attorney_count,
             SUM(CASE    WHEN tab_data.position_id = '0090' THEN 1 ELSE 0 END)
 non_attorney_count,
             SUM(CASE    WHEN tab_data.position_id = '0050' THEN 1 ELSE 0 END)
 clerk_count
        FROM aws_test_table scco,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
 COLUMNS (
          parent_account_number NUMBER PATH
           '$.data.account.parentAccountNumber',
            account_number NUMBER PATH '$.data.account.accountNumber',
            business_unit_id NUMBER PATH '$.data.account.businessUnitId',
            position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
            ) AS tab_data
            INNER JOIN JSON_TABLE ( '{
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
```

```
          "businessUnitId": 7
        }, {
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }', '$.accounts[*]' ERROR ON ERROR
      COLUMNS (
      parent_account_number PATH '$.parentAccountNumber',
      account_number PATH '$.accountNumber',
      business_unit_id PATH '$.businessUnitId')
      ) static_data
      ON ( static_data.parent_account_number = tab_data.parent_account_number
           AND static_data.account_number = tab_data.account_number
           AND static_data.business_unit_id = tab_data.business_unit_id )
        GROUP BY
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number
    );
```

Para convertir los datos de nivel de fila al formato JSON, Oracle tiene funciones integradas como `JSON_OBJECT`, `JSON_ARRAY`, `JSON_OBJECTAGG` y `JSON_ARRAYAGG`.

- `JSON_OBJECT` acepta dos parámetros: `KEY` y `VALUE`. El parámetro `KEY` debe estar codificado de forma rígida o ser de naturaleza estática. El parámetro `VALUE` se deriva de la salida de la tabla.
- `JSON_ARRAYAGG` acepta `JSON_OBJECT` como parámetro. Esto ayuda a agrupar el conjunto de `JSON_OBJECT` elementos en forma de lista. Por ejemplo, si tiene un elemento `JSON_OBJECT` que tiene varios registros (múltiples pares `KEY` y `VALUE`en el conjunto de datos), `JSON_ARRAYAGG` agrega el conjunto de datos y crea una lista. Según el lenguaje de estructura de datos, `LIST` es un grupo de elementos. En este contexto, `LIST` es un grupo de elementos `JSON_OBJECT`.

En el siguiente ejemplo, se muestra un elemento `JSON_OBJECT`.

```
{
   "taxProfessionalCount": 0,
   "attorneyCount": 0,
   "nonAttorneyCount": 1,
   "clerkCount": 0
}
```

En el siguiente ejemplo, se muestran dos elementos `JSON_OBJECT`, con `LIST` indicado mediante llaves cuadradas (`[ ]`).

```
[
    {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
,
    {
        "taxProfessionalCount": 2,
        "attorneyCount": 1,
        "nonAttorneyCount": 3,
        "clerkCount":4
      }
]
```

Ejemplo de consulta SQL

```
SELECT
    JSON_OBJECT(
        'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               )
                        )
                                          )
              )
FROM
    (SELECT
            tab_data.business_unit_id,
            tab_data.parent_account_number,
```

```
            tab_data.account_number,
            SUM(1) online_contacts_count,
            SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE   0 END
            )      tax_count,
            SUM(CASE    WHEN tab_data.position_id = '0100' THEN        1    ELSE
0 END
            )      attorney_count,

            SUM(CASE    WHEN tab_data.position_id = '0090' THEN        1    ELSE
0 END
            )      non_attorney_count,

            SUM(CASE    WHEN tab_data.position_id = '0050' THEN        1    ELSE
0 END
            )      clerk_count

        FROM
            aws_test_table scco,  JSON_TABLE ( json_doc, '$' ERROR ON ERROR
            COLUMNS (
            parent_account_number NUMBER PATH '$.data.account.parentAccountNumber',
            account_number NUMBER PATH '$.data.account.accountNumber',
            business_unit_id NUMBER PATH '$.data.account.businessUnitId',
            position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
            ) AS tab_data
            INNER JOIN JSON_TABLE ( '{
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }', '$.accounts[*]' ERROR ON ERROR
      COLUMNS (
      parent_account_number PATH '$.parentAccountNumber',
      account_number PATH '$.accountNumber',
      business_unit_id PATH '$.businessUnitId')
      ) static_data ON ( static_data.parent_account_number =
tab_data.parent_account_number
                          AND static_data.account_number = tab_data.account_number
```

```
                          AND static_data.business_unit_id =
 tab_data.business_unit_id )
        GROUP BY
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number
    );
```

Ejemplo de resultado de la consulta SQL anterior

```
{
  "accountCounts": [
    {
      "businessUnitId": 6,
      "parentAccountNumber": 32001,
      "accountNumber": 42001,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
      "businessUnitId": 7,
      "parentAccountNumber": 32000,
      "accountNumber": 42000,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

6. Postgres_SQL_JSON_Aggregation_JOIN

Las funciones integradas de PostgresQL `JSON_BUILD_OBJECT` y `JSON_AGG` convierten los datos de nivel de fila a formato JSON. PostgreSQL `JSON_OBJECT` y `JSON_AGG`son equivalentes a Oracle `JSON_BUILD_OBJECT` y `JSON_ARRAYAGG`.

Consulta de ejemplo

```
select
JSON_BUILD_OBJECT ('accountCounts',
    JSON_AGG(
        JSON_BUILD_OBJECT ('businessUnitId',businessUnitId
        ,'parentAccountNumber',parentAccountNumber
        ,'accountNumber',accountNumber
        ,'totalOnlineContactsCount',online_contacts_count,
        'countByPosition',
            JSON_BUILD_OBJECT (
            'taxProfessionalCount',tax_professional_count
            ,'attorneyCount',attorney_count
            ,'nonAttorneyCount',non_attorney_count
            ,'clerkCount',clerk_count
            )
        )
    )
)
from (
with tab as (select * from (
select (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER as
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER as accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER as businessUnitId,
(json_doc::json->'data'->>'positionId')::varchar as positionId
from aws_test_pg_table) a ) ,
tab1 as ( select
(json_array_elements(b.jc -> 'accounts') ->> 'accountNumber')::integer accountNumber,
(json_array_elements(b.jc -> 'accounts') ->> 'businessUnitId')::integer
 businessUnitId,
(json_array_elements(b.jc -> 'accounts') ->> 'parentAccountNumber')::integer
 parentAccountNumber
from (
select '{
        "accounts": [{
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
```

```
        }, {
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }]
      }'::json as jc) b)
select
tab.businessUnitId::text,
tab.parentAccountNumber::text,
tab.accountNumber::text,
SUM(1) online_contacts_count,
SUM(CASE WHEN tab.positionId::text = '0095' THEN 1 ELSE 0  END)
 tax_professional_count,
SUM(CASE WHEN tab.positionId::text = '0100' THEN 1 ELSE 0  END)      attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0090' THEN      1  ELSE      0 END)
 non_attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0050' THEN      1  ELSE      0 END)
 clerk_count
from tab1,tab
where tab.parentAccountNumber::INTEGER=tab1.parentAccountNumber::INTEGER
and tab.accountNumber::INTEGER=tab1.accountNumber::INTEGER
and tab.businessUnitId::INTEGER=tab1.businessUnitId::INTEGER
GROUP BY      tab.businessUnitId::text,
            tab.parentAccountNumber::text,
            tab.accountNumber::text) a;
```

Ejemplo de salida de la consulta anterior

Las salidas de Oracle y PostgreSQL son exactamente las mismas.

```
{
  "accountCounts": [
    {
      "businessUnitId": 6,
      "parentAccountNumber": 32001,
      "accountNumber": 42001,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
```

```
    {
      "businessUnitId": 7,
      "parentAccountNumber": 32000,
      "accountNumber": 42000,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

7. Oracle_Procedure_with_JSON_Query

Este código convierte el procedimiento de Oracle en una función de PostgreSQL que tiene consultas JSON SQL. Muestra cómo la consulta transpone JSON a filas y viceversa.

```
CREATE OR REPLACE PROCEDURE p_json_test(p_in_accounts_json IN varchar2,
 p_out_accunts_json  OUT varchar2)
IS
BEGIN
/*
p_in_accounts_json paramter should have following format:
       {
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }
*/
SELECT
    JSON_OBJECT(
        'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
```

```
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               ) ) ) )
into p_out_accunts_json
FROM
    (SELECT
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number,
            SUM(1) online_contacts_count,
            SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE 0 END) tax_count,
            SUM(CASE    WHEN tab_data.position_id = '0100' THEN 1 ELSE 0 END)
 attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0090' THEN 1 ELSE 0 END)
 non_attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0050' THEN 1 ELSE 0 END)
 clerk_count
        FROM aws_test_table scco,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
            COLUMNS (
            parent_account_number NUMBER PATH '$.data.account.parentAccountNumber',
            account_number NUMBER PATH '$.data.account.accountNumber',
            business_unit_id NUMBER PATH '$.data.account.businessUnitId',
            position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
            ) AS tab_data
            INNER JOIN JSON_TABLE ( p_in_accounts_json, '$.accounts[*]' ERROR ON ERROR

      COLUMNS (
      parent_account_number PATH '$.parentAccountNumber',
      account_number PATH '$.accountNumber',
      business_unit_id PATH '$.businessUnitId')
      ) static_data
      ON ( static_data.parent_account_number = tab_data.parent_account_number
           AND static_data.account_number = tab_data.account_number
           AND static_data.business_unit_id = tab_data.business_unit_id )
        GROUP BY
            tab_data.business_unit_id,
            tab_data.parent_account_number,
```

```
            tab_data.account_number
    );
EXCEPTION
WHEN OTHERS THEN
   raise_application_error(-20001,'Error while running the JSON query');
END;
/
```

Ejecutando el procedimiento

El siguiente bloque de código explica cómo puede ejecutar el procedimiento de Oracle creado anteriormente con una entrada JSON de ejemplo en el procedimiento. También proporciona el resultado o la salida de este procedimiento.

```
set serveroutput on;
declare
v_out varchar2(30000);
v_in varchar2(30000):= '{
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }';
begin
  p_json_test(v_in,v_out);
  dbms_output.put_line(v_out);
end;
/
```

Resultado del procedimiento

```
{
  "accountCounts": [
    {
      "businessUnitId": 6,
      "parentAccountNumber": 32001,
      "accountNumber": 42001,
      "totalOnlineContactsCount": 1,
```

```
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
      "businessUnitId": 7,
      "parentAccountNumber": 32000,
      "accountNumber": 42000,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

8. Postgres_Function_with_JSON_Query

Función de ejemplo

```
CREATE OR REPLACE  FUNCTION f_pg_json_test(p_in_accounts_json  text)
RETURNS text
LANGUAGE plpgsql
AS
$$
DECLARE
 v_out_accunts_json   text;
BEGIN
SELECT
JSON_BUILD_OBJECT ('accountCounts',
    JSON_AGG(
        JSON_BUILD_OBJECT ('businessUnitId',businessUnitId
        ,'parentAccountNumber',parentAccountNumber
        ,'accountNumber',accountNumber
        ,'totalOnlineContactsCount',online_contacts_count,
        'countByPosition',
            JSON_BUILD_OBJECT (
            'taxProfessionalCount',tax_professional_count
```

```
            ,'attorneyCount',attorney_count
            ,'nonAttorneyCount',non_attorney_count
            ,'clerkCount',clerk_count
            ))))
INTO v_out_accunts_json
FROM (
WITH tab AS (SELECT * FROM (
SELECT (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER AS
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER AS accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER AS businessUnitId,
(json_doc::json->'data'->>'positionId')::varchar AS positionId
FROM aws_test_pg_table) a ) ,
tab1 AS ( SELECT
(json_array_elements(b.jc -> 'accounts') ->> 'accountNumber')::integer accountNumber,
(json_array_elements(b.jc -> 'accounts') ->> 'businessUnitId')::integer businessUnitId,
(json_array_elements(b.jc -> 'accounts') ->> 'parentAccountNumber')::integer
 parentAccountNumber
FROM (
SELECT p_in_accounts_json::json AS jc) b)
SELECT
tab.businessUnitId::text,
tab.parentAccountNumber::text,
tab.accountNumber::text,
SUM(1) online_contacts_count,
SUM(CASE WHEN tab.positionId::text = '0095' THEN 1 ELSE 0  END)
 tax_professional_count,
SUM(CASE WHEN tab.positionId::text = '0100' THEN 1 ELSE 0  END)      attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0090' THEN      1  ELSE      0 END)
 non_attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0050' THEN      1  ELSE      0 END)
 clerk_count
FROM tab1,tab
WHERE tab.parentAccountNumber::INTEGER=tab1.parentAccountNumber::INTEGER
AND tab.accountNumber::INTEGER=tab1.accountNumber::INTEGER
AND tab.businessUnitId::INTEGER=tab1.businessUnitId::INTEGER
GROUP BY      tab.businessUnitId::text,
            tab.parentAccountNumber::text,
            tab.accountNumber::text) a;
RETURN v_out_accunts_json;
END;
$$;
```

Ejecución de la función

```
select    f_pg_json_test('{
        "accounts": [{
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }, {
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }]
      }')   ;
```

Salida de función

La siguiente salida de es similar a la salida del procedimiento de Oracle. La diferencia es que esta salida está en formato de texto.

```
{
  "accountCounts": [
    {
      "businessUnitId": "6",
      "parentAccountNumber": "32001",
      "accountNumber": "42001",
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
      "businessUnitId": "7",
      "parentAccountNumber": "32000",
      "accountNumber": "42000",
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
```

```
      }
    }
  ]
}
```

Copie tablas de Amazon DynamoDB entre cuentas mediante AWS Backup

Ramkumar Ramanujam, Amazon Web Services

Resumen

Cuando se trabaja con Amazon DynamoDB AWS, un caso de uso común es copiar o sincronizar tablas de DynamoDB en entornos de desarrollo, pruebas o ensayo con los datos de la tabla que se encuentran en el entorno de producción. Como práctica estándar, cada entorno utiliza una Cuenta de AWS diferente.

AWS Backup admite la copia de seguridad y la restauración de datos entre regiones y cuentas para DynamoDB, Amazon Simple Storage Service (Amazon S3) y otros. Servicios de AWS Este patrón proporciona los pasos para utilizar la copia de seguridad y la restauración AWS Backup entre cuentas para copiar tablas de DynamoDB entre ellas. Cuentas de AWS

Requisitos previos y limitaciones

Requisitos previos

- Dos activos Cuentas de AWS que pertenecen a la misma organización en AWS Organizations
- Permisos para crear tablas de DynamoDB en ambas cuentas
- AWS Identity and Access Management Permisos (IAM) para crear y usar bóvedas AWS Backup

Limitaciones

- El origen y el destino Cuentas de AWS deben formar parte de la misma organización en. AWS Organizations

Arquitectura

Pila de tecnología de destino

- AWS Backup
- Amazon DynamoDB

Arquitectura de destino

1. Cree la copia de seguridad de la tabla de DynamoDB en AWS Backup el almacén de copias de seguridad de la cuenta de origen.
2. Copie la copia de seguridad en el almacén de copias de seguridad de la cuenta de destino.
3. Restaure la tabla de DynamoDB en la cuenta de destino mediante la copia de seguridad del almacén de copias de seguridad de la cuenta de destino.

Automatización y escala

Puede utilizarla AWS Backup para programar las copias de seguridad para que se ejecuten a intervalos específicos.

Tools (Herramientas)

- AWS Backupes un servicio totalmente gestionado para centralizar y automatizar la protección de datos tanto en la nube como en las instalaciones. Servicios de AWS Con este servicio, puede configurar las políticas de respaldo y monitorear la actividad de sus AWS recursos en un solo lugar. Le permite automatizar y consolidar las tareas de copia de seguridad que antes se realizaban servicio por servicio y elimina la necesidad de crear scripts personalizados y procesos manuales.
- Amazon DynamoDB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido y predecible, así como una perfecta escalabilidad.

Epics

Activa AWS Backup las funciones en las cuentas de origen y destino

Tarea	Descripción	Habilidades requeridas
Active las características avanzadas de copia de seguridad de DynamoDB y entre cuentas.	Tanto en la fuente como en la de destino Cuentas de AWS, haga lo siguiente: 1. En el Consola de administración de AWS, abra la AWS Backup consola.	AWS DevOps, ingeniero de migración

Tarea	Descripción	Habilidades requeridas
	2. Seleccione Settings (Configuración). 3. En Advanced features for Amazon DynamoDB backups (Características avanzadas para copias de seguridad de Amazon DynamoDB), confirme que la opción Advanced features esté activada o seleccione Enable (Activar). 4. En Cross-account management (Administ ración multicuenta), seleccione Enable (Activar) para Cross-account backup (Copia de seguridad multicuenta).	

Crear almacenes de copia de seguridad en las cuentas de origen y destino

Tarea	Descripción	Habilidades requeridas
Cree almacenes de copias de seguridad.	Tanto en el origen como en el destino Cuentas de AWS, haga lo siguiente: 1. En la consola de AWS Backup, seleccione Almacenes de copias de seguridad. 2. Seleccione Create Backup vault (Crear almacén de copias de seguridad).	AWS DevOps, ingeniero de migración

Tarea	Descripción	Habilidades requeridas
	3. Copie el nombre de recurso de Amazon (ARN) del almacén de copias de seguridad y guárdelo. Al copiar la copia ARNs de seguridad de la tabla de DynamoDB entre las cuentas de origen y destino, se necesitarán las bóvedas de copia de seguridad de origen y destino.	

Realizar copias de seguridad y restaurar mediante almacenes de copias de seguridad

Tarea	Descripción	Habilidades requeridas
En la cuenta de origen, cree una copia de seguridad de la tabla de DynamoDB.	Para crear una copia de seguridad de la tabla de DynamoDB en la cuenta de origen, realice lo siguiente: 1. En la página del AWS Backup panel de control, elija Crear copia de seguridad bajo demanda. 2. En la sección Settings (Configuración), para Resource type (Tipo de recurso), seleccione DynamoDB y, a continuac ión, seleccione el nombre de la tabla.	AWS DevOps, DBA, ingeniero de migración

Tarea	Descripción	Habilidades requeridas
	3. En la lista desplegable Backup Vault (Almacén de copias de seguridad), seleccione el almacén que creó en la cuenta de origen. 4. Seleccione el Retention period (Periodo de conservación) que desee. 5. Seleccione Create on-demand backup (Crear copia de seguridad bajo demanda). Se creará un nuevo trabajo de copia de seguridad. Para supervisar el estado del trabajo de copia de seguridad , en la página AWS Backup Trabajos, seleccione la pestaña Trabajos de copia de seguridad. En esta pestaña se muestran todos los trabajos de copia de seguridad activos, en curso y finalizados.	

Tarea	Descripción	Habilidades requeridas
Copie la copia de seguridad de la cuenta de origen a la cuenta de destino.	Una vez finalizado el trabajo de copia de seguridad, copie la copia de seguridad de la tabla de DynamoDB del almacén de copias de seguridad de la cuenta de origen al almacén de copias de seguridad de la cuenta de destino. Para copiar el almacén de copias de seguridad, realice lo siguiente en la cuenta de origen: 1. En la consola de AWS Backup, seleccione Almacenes de copias de seguridad. 2. En Backups (Copias de seguridad), seleccione la copia de seguridad de la tabla de DynamoDB. 3. Seleccione Actions (Acciones), Copy (Copiar). 4. Introduzca el Región de AWS de la cuenta de destino. 5. Para el External vault ARN (Nombre de recurso de Amazon de almacén externo), escriba el ARN del almacén de copias de	AWS DevOps, ingeniero de migración, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	seguridad que creó en la cuenta de destino. 6. Para copiar las copias de seguridad de la cuenta de origen a la cuenta de destino, sitúese en el almacén de copias de seguridad de la cuenta de destino y habilite el acceso de una cuenta diferente.	
Restaurar la copia de seguridad en la cuenta de destino.	En el objetivo Cuenta de AWS, haga lo siguiente: 1. En la consola de AWS Backup, seleccione Almacenes de copias de seguridad. 2. En Backups (Copias de seguridad), seleccione la copia de seguridad que copió de la cuenta de origen. 3. Seleccione Actions (Acciones), Restore (Restaurar). 4. Especifique el nombre de la tabla de DynamoDB de destino que desea restaurar .	AWS DevOps, DBA, ingeniero de migración

Recursos relacionados

- Uso AWS Backup con DynamoDB

- Crear copias de seguridad en Cuentas de AWS
- AWS Backup precios

Copiar tablas de Amazon DynamoDB entre cuentas mediante una implementación personalizada

Ramkumar Ramanujam, Amazon Web Services

Resumen

Cuando se trabaja con Amazon DynamoDB en Amazon Web Services (AWS), un caso de uso habitual consiste en copiar o sincronizar tablas de DynamoDB en entornos de desarrollo, de prueba o de ensayo con datos de la tabla que se encuentra en el entorno de producción. Como práctica estándar, cada entorno utiliza una cuenta AWS diferente.

DynamoDB ahora admite copias de seguridad entre cuentas mediante AWS Backup. Para obtener información sobre los costos de almacenamiento asociados al uso de AWS Backup, consulte los precios de AWS Backup. Cuando se utiliza AWS Backup para copiar entre cuentas, las cuentas de origen y de destino deben formar parte de una organización de AWS Organizations. Existen otras soluciones para realizar copias de seguridad y restauraciones entre cuentas mediante servicios de AWS, como AWS Glue. Sin embargo, el uso de esas soluciones aumenta el tamaño de las aplicaciones, ya que es necesario implementar y mantener más servicios de AWS.

También puede utilizar Amazon DynamoDB Streams para capturar los cambios en la tabla de la cuenta de origen. A continuación, puede iniciar una función de AWS Lambda y realizar los cambios correspondientes en la tabla de destino de la cuenta de destino. Sin embargo, esa solución se aplica a los casos de uso en los que las tablas de origen y de destino deben mantenerse siempre sincronizadas. Es posible que no se aplique a los entornos de desarrollo, pruebas y uso transitorio en los que los datos se actualizan con frecuencia.

Este patrón proporciona los pasos para implementar una solución personalizada para copiar una tabla de Amazon DynamoDB de una cuenta a otra. Este patrón se puede implementar mediante lenguajes de programación comunes, como C#, Java y Python. Recomendamos utilizar un lenguaje que sea compatible con un AWS SDK.

Requisitos previos y limitaciones

Requisitos previos

- Dos cuentas de AWS activas
- Tablas de DynamoDB en ambas cuentas

- Configuración de políticas y roles de AWS Identity and Access Management (IAM)
- Conocimiento de cómo acceder a las tablas de Amazon DynamoDB mediante cualquier lenguaje de programación común, como C#, Java o Python

Limitaciones

Este patrón se aplica a las tablas de DynamoDB de alrededor de 2 GB o menos. Con una lógica adicional para gestionar las interrupciones de conexión o sesión, las limitaciones y los errores y reintentos, también se puede utilizar para tablas más grandes.

La operación de escaneo de DynamoDB, que lee los elementos de la tabla de origen, solo puede recuperar hasta 1 MB de datos en una sola llamada. En el caso de tablas más grandes, de más de 2 GB, esta limitación puede aumentar el tiempo total necesario para realizar una copia completa de la tabla.

Arquitectura

El siguiente diagrama muestra la implementación personalizada entre las cuentas de AWS de origen y destino. Las políticas de IAM y los tokens de seguridad se utilizan con la implementación personalizada. Los datos se leen desde Amazon DynamoDB en la cuenta de origen y se escriben en DynamoDB en la cuenta de destino.

Automatización y escala

Este patrón se aplica a las tablas de DynamoDB de tamaño más pequeño, de unos 2 GB.

Para aplicar este patrón a tablas más grandes, aborde los problemas siguientes:

- Durante la operación de copia de la tabla, se mantienen dos sesiones activas, utilizando diferentes tokens de seguridad. Si la operación de copia de la tabla tarda más que los tiempos de caducidad del token, debe implementar una lógica para actualizar los tokens de seguridad.
- Si no se aprovisionan suficientes unidades de capacidad de lectura (RCUs) y unidades de capacidad de escritura (WCUs), es posible que se limiten las lecturas o escrituras en la tabla de origen o destino. Asegúrese de atrapar y gestionar estas excepciones.
- Controle cualquier otro error o excepción y establezca un mecanismo de reintento para volver a intentarlo o continuar desde el punto en el que se produjo el error en la operación de copia.

Tools (Herramientas)

Herramientas

- Amazon DynamoDB: Amazon DynamoDB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido y predecible, así como una perfecta escalabilidad.
- Las herramientas adicionales necesarias variarán según el lenguaje de programación que se elija para la implementación. Por ejemplo, si usa C#, necesitará Microsoft Visual Studio y los siguientes NuGet paquetes:
  - `AWSSDK`
  - `AWSSDK.DynamoDBv2`

Código

El siguiente fragmento de código de Python elimina y vuelve a crear una tabla de DynamoDB mediante la biblioteca Boto3.

No utilice el `AWS_ACCESS_KEY_ID` ni el `AWS_SECRET_ACCESS_KEY` de un nombre de usuario de IAM porque se trata de credenciales a largo plazo, que deben evitarse para el acceso programático a los servicios de AWS. Para obtener más información sobre cómo usar credenciales de seguridad temporales, consulte la sección Prácticas recomendables.

Las credenciales `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY` y `TEMPORARY_SESSION_TOKEN` utilizadas en el siguiente fragmento de código son credenciales temporales obtenidas de AWS Security Token Service (AWS STS).

```
import boto3
import sys
import json

#args = input-parameters = GLOBAL_SEC_INDEXES_JSON_COLLECTION,
 ATTRIBUTES_JSON_COLLECTION, TARGET_DYNAMODB_NAME, TARGET_REGION, ...

#Input param: GLOBAL_SEC_INDEXES_JSON_COLLECTION
#[{"IndexName":"Test-index","KeySchema":[{"AttributeName":"AppId","KeyType":"HASH"},
{"AttributeName":"AppType","KeyType":"RANGE"}],"Projection":
{"ProjectionType":"INCLUDE","NonKeyAttributes":["PK","SK","OwnerName","AppVersion"]}}]

#Input param: ATTRIBUTES_JSON_COLLECTION
```

```
#[{"AttributeName":"PK","AttributeType":"S"},
{"AttributeName":"SK","AttributeType":"S"},
{"AttributeName":"AppId","AttributeType":"S"},
{"AttributeName":"AppType","AttributeType":"N"}]

region = args['TARGET_REGION']
target_ddb_name = args['TARGET_DYNAMODB_NAME']

global_secondary_indexes = json.loads(args['GLOBAL_SEC_INDEXES_JSON_COLLECTION'])
attribute_definitions = json.loads(args['ATTRIBUTES_JSON_COLLECTION'])

# Drop and create target DynamoDB table
dynamodb_client = boto3.Session(
        aws_access_key_id=args['AWS_ACCESS_KEY_ID'],
        aws_secret_access_key=args['AWS_SECRET_ACCESS_KEY'],
        aws_session_token=args['TEMPORARY_SESSION_TOKEN'],
    ).client('dynamodb')

# Delete table
print('Deleting table: ' + target_ddb_name + ' ...')

try:
    dynamodb_client.delete_table(TableName=target_ddb_name)

    #Wait for table deletion to complete
    waiter = dynamodb_client.get_waiter('table_not_exists')
    waiter.wait(TableName=target_ddb_name)
    print('Table deleted.')
except dynamodb_client.exceptions.ResourceNotFoundException:
    print('Table already deleted / does not exist.')
    pass

print('Creating table: ' + target_ddb_name + ' ...')

table = dynamodb_client.create_table(
    TableName=target_ddb_name,
    KeySchema=[
        {
            'AttributeName': 'PK',
            'KeyType': 'HASH'  # Partition key
        },
        {
            'AttributeName': 'SK',
            'KeyType': 'RANGE'  # Sort key
```

```
        }
    ],
    AttributeDefinitions=attribute_definitions,
    GlobalSecondaryIndexes=global_secondary_indexes,
    BillingMode='PAY_PER_REQUEST'
)

waiter = dynamodb_client.get_waiter('table_exists')
waiter.wait(TableName=target_ddb_name)

print('Table created.')
```

Prácticas recomendadas

Credenciales temporales

Como práctica recomendada de seguridad, al acceder a los servicios de AWS mediante programación, se debe evitar utilizar `AWS_ACCESS_KEY_ID` y `AWS_SECRET_ACCESS_KEY` de un usuario de IAM, ya que se trata de credenciales a largo plazo. Intente utilizar siempre credenciales temporales para acceder a los servicios de AWS mediante programación.

Así, por ejemplo, un desarrollador codifica de forma rígida la dirección `AWS_ACCESS_KEY_ID` y `AWS_SECRET_ACCESS_KEY` de un usuario de IAM en la aplicación durante el desarrollo, pero no elimina los valores codificados antes de incorporar los cambios en el repositorio de código. Estas credenciales expuestas pueden ser utilizadas por usuarios de forma involuntaria o malintencionada, lo que puede tener graves consecuencias (especialmente si las credenciales expuestas tienen privilegios de administrador). Estas credenciales expuestas se deben desactivar o eliminar inmediatamente mediante la consola de IAM o interfaz de la línea de comandos de AWS (AWS CLI).

Para obtener credenciales temporales para el acceso mediante programación a los servicios de AWS, utilice AWS STS. Las credenciales temporales son válidas solo durante el tiempo especificado (de 15 minutos a 36 horas). La duración máxima permitida de las credenciales temporales varía en función de factores como la configuración de los roles y el encadenamiento de funciones. Para obtener más información acerca de AWS STS, consulte la documentación.

Epics

Configurar tablas de DynamoDB

Tarea	Descripción	Habilidades requeridas
Cree tablas de DynamoDB.	Cree tablas de DynamoDB, con índices, en las cuentas de AWS de origen y de destino. Configure el aprovisionamiento de capacidad como modo bajo demanda, lo que permite a DynamoDB read/write escalar las capacidades de forma dinámica en función de la carga de trabajo. Como alternativa, puede utilizar la capacidad aprovisionada con 4000 y 4000. RCUs WCUs	Desarrollador de aplicaciones, administrador de bases de datos e ingeniero de migraciones
Rellene la tabla de origen.	Rellene la tabla de DynamoDB de la cuenta de origen con datos de prueba. Tener al menos 50 MB o más de datos de prueba le ayuda a ver el consumo máximo y medio RCUs consumido durante la copia de la tabla. A continuación, puede cambiar el aprovisionamiento de capacidad según sea necesario.	Desarrollador de aplicaciones, administrador de bases de datos e ingeniero de migraciones

Configurar las credenciales para acceder a las tablas de DynamoDB

Tarea	Descripción	Habilidades requeridas
Cree roles de IAM para acceder a las tablas de DynamoDB de origen y destino.	Cree un rol de IAM en la cuenta de origen con permisos de acceso (lectura) a la tabla de DynamoDB de la cuenta de origen. Agregue la cuenta de origen como entidad de confianza para este rol. Cree un rol de IAM en la cuenta de destino con permisos de acceso (creación , lectura, actualización, eliminación) a la tabla de DynamoDB de la cuenta de destino. Agregue la cuenta de destino como entidad de confianza para este rol.	Desarrollador de aplicaciones, AWS DevOps

Copiar datos de tablas de una cuenta a otra

Tarea	Descripción	Habilidades requeridas
Obtenga credenciales temporales para los roles de IAM.	Obtenga credenciales temporales para el rol de IAM creado en la cuenta de origen. Obtenga credenciales temporales para el rol de	Desarrollador de aplicación, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	IAM creado en la cuenta de destino. Una forma de obtener las credenciales temporales para el rol de IAM es usar AWS STS desde la AWS CLI. `aws sts assume-role --role-arn arn:aws:iam::<account-id>:role/<role-name> --role-session-name <session-name> --profile <profile-name>` Utilice el perfil de AWS adecuado (correspondiente a la cuenta de origen o de destino). Para obtener más información sobre cómo obtener credencia les temporales consulte lo siguiente: • AWS Security Token Service API Reference (Referencia de API del servicio de token de seguridad de AWS) • Getting IAM role credentials for CLI access (Obtener las credenciales del rol de IAM para el acceso a la CLI)	

Tarea	Descripción	Habilidades requeridas
Inicialice los clientes de DynamoDB para el acceso a DynamoDB de origen y destino.	Inicialice los clientes de DynamoDB, que proporcio na AWS SDK, para las tablas de DynamoDB de origen y destino. • Para el cliente DynamoDB de origen, utilice las credenciales temporales obtenidas de la cuenta de origen. • Para el cliente DynamoDB de destino, utilice las credenciales temporales obtenidas de la cuenta de destino. Para obtener más información sobre cómo realizar solicitud es mediante credenciales temporales de IAM, consulte la Documentación de AWS.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Eliminar y recrear la tabla de destino.	Elimine y vuelva a crear la tabla de DynamoDB de destino (junto con los índices) en la cuenta de destino mediante el cliente DynamoDB de la cuenta de destino. Eliminar todos los registros de una tabla de DynamoDB es una operación costosa porque consume aprovisionamiento. WCUs Al eliminar y volver a crear la tabla, se evitan esos costos adicionales. Puede añadir índices a una tabla después de crearla, pero esto requiere de 2 a 5 minutos más. Resulta más eficiente crear índices durante la creación de la tabla, pasando la colección de índices a la llamada `createTable` .	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Realice la copia de la tabla.	Repita los pasos siguientes hasta que se copien todos los datos: • Realice un análisis de la tabla de la cuenta de origen mediante el cliente DynamoDB de origen. Cada escaneo de DynamoDB recupera solo 1 MB de datos de la tabla, por lo que debe repetir esta operación hasta que se lean todos los elementos o registros. • Para cada conjunto de elementos escaneados, escriba los elementos en la tabla de la cuenta de destino, con el cliente de DynamoDB de destino, mediante la llamada `BatchWriteItem` del SDK de AWS para DynamoDB. De este modo, se reduce el número de solicitudes `PutItem` que se envían a DynamoDB. • `BatchWriteItem` tiene un límite de 25 operaciones de escritura o incorporación, es decir, de hasta 16 MB. Debe añadir una lógica para acumular hasta 25 objetos escaneados antes de	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	llamar a `BatchWriteItem`. `BatchWriteItem` devuelve una lista de los elementos que no se han podido copiar correctamente. Con esta lista, agregue una lógica de reintento para realizar otra llamada de `BatchWriteItem` únicamente con los elementos que no se hayan realizado correctamente. Para obtener más información, consulte la implementación de referencia en C# (para eliminar, crear y rellenar tablas) en la sección de adjuntos. También se adjunta un ejemplo de archivo de notación de JavaScript objetos (JSON) de configuración de tablas.	

Recursos relacionados

- Documentación de Amazon DynamoDB
- Creación de un usuario de IAM en su cuenta de AWS
- AWS SDKs
- Using temporary credentials with AWS resources (Usar credenciales temporales con recursos de AWS)

Información adicional

Este patrón se implementó con C# para copiar una tabla de DynamoDB con 200 000 elementos (el tamaño medio de los elementos es de 5 KB y el tamaño de la tabla de 250 MB). La tabla de DynamoDB de destino se configuró con una capacidad aprovisionada de 4000 y 4000. RCUs WCUs

La operación completa de copia de la tabla (de la cuenta de origen a la cuenta de destino), incluida la eliminación y la recreación de la tabla, duró 5 minutos. Capacidad total de unidades consumidas: 30 000 RCUs y aproximadamente 400 000. WCUs

Para obtener más información sobre los modos de capacidad de DynamoDB, consulte Read/Write capacity mode (Modo de capacidad de lectura/escritura) en la documentación de AWS.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Crear informes detallados de costos y uso para Amazon RDS y Amazon Aurora

Lakshmanan Lakshmanan y Sudarshan Narasimhan, Amazon Web Services

Resumen

Este patrón muestra cómo realizar un seguimiento de los costos de uso de los clústeres de Amazon Relational Database Service (Amazon RDS) o Amazon Aurora mediante la configuración de etiquetas de asignación de costos definidas por el usuario. Puede usar estas etiquetas para crear informes detallados de costos y uso en el explorador de costos de AWS para clústeres en varias dimensiones. Por ejemplo, puede realizar un seguimiento de los costos de uso a nivel de equipo, proyecto o centro de costos y, a continuación, analizar los datos en Amazon Athena.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una o más instancias de Amazon RDS o Amazon Aurora

Limitaciones

Para conocer las restricciones de etiquetado, consulte la Guía del usuario de facturación de AWS.

Arquitectura

Pila de tecnología de destino

- Amazon RDS o Amazon Aurora
- AWSInforme de uso y costos
- Explorador de costos de AWS
- Amazon Athena

Flujo de trabajo y arquitectura

El flujo de trabajo de etiquetado y análisis consta de los siguientes pasos:

1. Un ingeniero de datos, un administrador de bases de datos o un administrador de AWS crea etiquetas de asignación de costos definidas por el usuario para los clústeres de Amazon RDS o Aurora.
2. Un administrador de AWS activa las etiquetas.
3. Las etiquetas envían los metadatos al explorador de costos de AWS.
4. Un ingeniero de datos, un administrador de bases de datos o un administrador de AWS crea un informe mensual de asignación de costos.
5. Un ingeniero de datos, un administrador de bases de datos o un administrador de AWS analiza el informe mensual de asignación de costos mediante Amazon Athena.

En el siguiente diagrama, se muestra cómo aplicar etiquetas para realizar un seguimiento de los costos de uso de las instancias de Amazon RDS o Aurora.

El siguiente diagrama de arquitectura muestra cómo el informe de asignación de costos se integra con Amazon Athena para su análisis.

El informe de asignación de costos mensual se almacena en un bucket de Amazon S3 que especifique. Al configurar Athena con la CloudFormation plantilla de AWS, tal y como se describe en la sección Epics, la plantilla incluye varios recursos adicionales, como un rastreador de AWS Glue, una base de datos de AWS Glue, un evento del Amazon Simple Notification System (Amazon SNS), funciones de AWS Lambda y roles de AWS Identity and Access Management (IAM) para las funciones de Lambda. A medida que llegan nuevos archivos de datos de costos al bucket de S3, las notificaciones de eventos se utilizan para reenviar estos archivos a una función de Lambda para su procesamiento. La función de Lambda inicia un trabajo de rastreador de AWS Glue para crear o actualizar la tabla en el catálogo de datos de AWS Glue. Esta tabla se usa a continuación para consultar datos en Athena.

Tools (Herramientas)

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.

- Amazon Aurora es un motor de base de datos relacional completamente administrado diseñado para la nube y compatible con MySQL y PostgreSQL.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- AWS CloudFormation es un servicio de infraestructura como código (IaC) que le permite modelar, aprovisionar y administrar fácilmente recursos de AWS y de terceros.
- El Explorador de costos de AWS permite ver y analizar los costos y el uso.

Epics

Crear y activar etiquetas para su clúster de Amazon RDS o Aurora

Tarea	Descripción	Habilidades requeridas
Cree etiquetas de asignación de costos definidas por el usuario para su clúster de Amazon RDS o Aurora.	Para añadir etiquetas a un clúster de Amazon RDS o Aurora nuevo o existente, siga las instrucciones de Cómo añadir, publicar y eliminar etiquetas de la Guía del usuario de Amazon Aurora. **Note** Para obtener información sobre cómo configurar un clúster de Amazon Aurora, consulte las instrucciones para MySQL y PostgreSQL en la Guía del usuario de Amazon Aurora.	Administrador de AWS, ingeniero de datos, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Active las etiquetas de asignación de costos definidas por el usuario.	Siga las instrucciones de Activación de etiquetas de asignación de costos definidas por el usuario en la Guía del usuario de facturación de AWS.	Administrador de AWS

Crear informes de uso y costo

Tarea	Descripción	Habilidades requeridas
Cree y configure informes de costos y uso para sus clústeres.	1. Inicie sesión en la consola de administración de AWS y abra la consola de facturación de AWS. 2. En el panel de navegación, elija Reportes de uso y costo. 3. Seleccione Crear informe. 4. Proporcione un nombre para el informe, mantenga la configuración predeterminada para las demás opciones y, a continuación, seleccione Siguiente. 5. Seleccione Configurar y proporcione los detalles de un bucket de S3 existente. También puede elegir crear un bucket de S3 nuevo desde esta pantalla. Elija Siguiente.	Propietario de la aplicación, administrador de AWS, administrador de bases de datos, AWS general, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	6. Verifique la política predeterminada que se aplicará a su bucket, seleccione la casilla de confirmación y, a continuación, seleccione Guardar. 7. En Prefijo de ruta de informe, especifique el prefijo que desee anexar al nombre del informe. 8. En Granularidad temporal, seleccione Cada hora, Cada día o Cada mes, en función de la frecuencia con la que desee que se recopilen los datos para el informe. 9. Para el Informe de control de versiones, seleccione si desea que las nuevas versiones del informe se creen por separado o que se sobrescriba el informe existente con cada versión. 10. Para Habilitar la integración de datos de informes para, seleccione Amazon Athena. Verifique que el tipo de compresión esté establecido en Parquet. 11. Elija Siguiente. 12. Revise la configuración del informe y, a continuac	

Tarea	Descripción	Habilidades requeridas
	ión, seleccione Revisar y completar. Los datos estarán disponibles en 24 horas.	

Analizar los datos de los informes de costos y uso

Tarea	Descripción	Habilidades requeridas
Analice los datos del informe de costos y uso.	1. Configure y utilice Athena para analizar los datos del informe. Para obtener instrucciones, consulte Consultar informes de costos y uso de con Amazon Athena en la Guía del usuario de informes de costos y uso de AWS. Le recomendamos que utilice la CloudFormation plantilla de AWS proporcionada por Athena. 2. Ejecute consultas de Athena. Por ejemplo, puede utilizar la siguiente consulta SQL para comprobar el estado de la actualización de datos. `select status from cost_and_usage_data_status`	Propietario de la aplicación, administrador de AWS, administrador de bases de datos, AWS general, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte Ejecutar consultas de Amazon Athena en la Guía del usuario de los informes de costos y uso de AWS. **Note** Cuando ejecute su consulta de SQL, asegúrese de que la base de datos correcta esté seleccionada en la lista desplegable.	

Recursos relacionados

Referencias

- Configuración de Athena con CloudFormation plantillas de AWS (recomendado)
- Configuración manual de Athena
- Ejecutar consultas de Amazon Athena
- Cargar datos de informes en otros recursos

Tutoriales y videos

- Analice los informes de costos y uso con Amazon Athena (vídeo) YouTube

Implemente instancias de clústeres de conmutación por error de SQL Server en Amazon EC2 y Amazon FSx mediante Terraform

Mark Hudson y Matt Burgess, Amazon Web Services

Resumen

Este patrón utiliza Terraform para implementar instancias de clústeres de conmutación por error de SQL Server (FCIs) en los nodos del clúster de conmutación por error de Windows Server (WSFC) de Amazon Elastic Compute Cloud (Amazon). EC2 Además, el patrón utiliza el almacenamiento FSx compartido de Amazon para los datos y los archivos de registro.

Cuando se migran las bases de datos de SQL Server a AWS, la primera opción es Amazon RDS for SQL Server. Sin embargo, a veces Amazon RDS for SQL Server no es adecuado y SQL Server debe implementarse en EC2 Amazon en una arquitectura de alta disponibilidad. En esta solución, los servidores SQL Server FCIs se instalan en todos los nodos de WSFC.

El módulo Terraform incluido en este patrón aprovisiona hasta dos instancias de Amazon EC2 SQL Server. Un sistema de archivos de Amazon FSx para Windows File Server actúa como testigo del quórum y almacena los datos compartidos y los archivos de registro. Independientemente del número de instancias configuradas, los nodos de instancia de SQL Server siempre crearán un clúster de FCI y se unirán a él para garantizar la paridad del entorno. (Normalmente, una instancia se configura para entornos de desarrollo y dos instancias para entornos de producción). Para las configuraciones que utilizan dos nodos para una alta disponibilidad, se aprovisiona un equilibrador de carga de red interno. El equilibrador de carga de red utiliza una sonda de estado configurada en el clúster de la FCI para identificar qué nodo es el principal.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.
- Amazon Virtual Private Cloud (Amazon VPC) con dos subredes en zonas de disponibilidad independientes.
- Conjunto de opciones de DHCP de Amazon VPC. Configure el nombre de dominio para que se resuelva en su nombre de dominio de Active Directory y los servidores de nombres de dominio y NetBIOS para que apunten a sus controladores de dominio de Active Directory. Para obtener más información, consulte Configuración de VPC en Información adicional.

- AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD).
- Imagen de máquina de Amazon (AMI) personalizada. Para obtener más información, consulte Configuración de AMI en Información adicional.
- Bucket de Amazon Simple Storage Service (Amazon S3) que incluye la imagen ISO de SQL Server. Este requisito previo solo es necesario si se utiliza EC2 Image Builder con el `component.yaml` archivo proporcionado para crear la AMI personalizada.
- AWS Key Management Service (AWS KMS) clave de cifrado.
- De forma predeterminada, SQL Server se instala con una clave de producto de la edición para desarrolladores. Se espera que los sistemas de producción utilicen una clave de producto válida que la variable correspondiente transmita al módulo.

Limitaciones

- Esta solución requiere AWS Managed Microsoft AD. Sin embargo, si lo prefiere, puede utilizar una implementación de Active Directory autoadministrada en su lugar. Para ello, modifique el módulo Amazon FSx Terraform incluido para eliminar el `active_directory_id` atributo. A continuación, añada los cuatro atributos necesarios para la autoadministración de Active Directory, tal y como se muestra en la documentación de Terraform.
- SQL Server está configurado para usar la autenticación de modo mixto. Si lo prefiere, puede utilizar la autenticación solo de Windows. Para ello, en el script de datos de usuario proporcionado, elimine los parámetros `/SECURITYMODE` y `/SAPWD` que se proporcionan al comando `setup.exe`. Puede eliminar el archivo `sql_accounts.tf` y modificar el archivo `instances.tf` para eliminar la entrada `sql_sa_password`.
- Al eliminar un clúster implementado, debe eliminar los objetos de computadora virtual correspondientes y los objetos de equipo individuales de Active Directory. Para eliminar los objetos, utilice las herramientas administrativas de Active Directory.
- Algunos Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

Esta solución se probó con las siguientes versiones:

- Windows Server 2019
- SQL Server 2019
- Terraform v0.13.0

Arquitectura

Pila de tecnología de origen

- SQL Server

Pila de tecnología de destino

- FCI de SQL Server en nodos WSFC mediante Amazon EC2
- Servidor FSx de archivos Amazon para Windows
- Bucket de Amazon S3
- AWS Secrets Manager
- AWS Managed Microsoft AD
- AWS KMS
- AWS Identity and Access Management (IAM)

Arquitectura de destino

En el siguiente diagrama se muestra la arquitectura para esta solución.

En el diagrama se muestra lo siguiente:

- Una función de IAM que proporciona a las EC2 instancias acceso a AWS KMS Secrets Manager
- Dos nodos de SQL Server implementados en EC2 instancias de Amazon en subredes privadas en dos zonas de disponibilidad
- Un equilibrador de carga de red para facilitar las conexiones a la instancia activa de SQL Server (no se implementa al configurar un clúster de un solo nodo)
- Sistema de archivos Amazon FSx para Windows File Server implementado en ambas subredes privadas para el almacenamiento compartido por los nodos de SQL Server

- Secrets Manager para almacenar las credenciales y la configuración de Active Directory y SQL Server
- Bucket de Amazon S3 para almacenar la imagen de instalación de SQL Server
- AWS Managed Microsoft AD para la autenticación de Windows
- AWS KMS para crear la clave de cifrado

Automatización y escala

Puede automatizar el despliegue de la arquitectura de destino mediante los módulos de Terraform que se encuentran en el GitHub repositorio. Debe modificar el archivo `terraform.tfvars` para incluir valores variables específicos de su entorno. El depósito de Amazon S3, AWS Managed Microsoft AD los componentes, la clave de AWS KMS cifrado y algunos secretos son requisitos previos para esta implementación y no se incluyen en el código de Terraform.

Tools (Herramientas)

Servicios de AWS

- AWS Directory Service for Microsoft Active Directorypermite que sus cargas de trabajo y AWS recursos compatibles con directorios utilicen Microsoft Active Directory en. Nube de AWS En este patrón, AWS Managed Microsoft AD se utiliza para la autenticación de Windows Server y SQL Server y para el DNS.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática escalable en el Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez. En este patrón, las instancias del clúster de conmutación por error de SQL Server se instalan en las EC2 instancias de Amazon.
- EC2 Image Builder le ayuda a automatizar la creación, la administración y el despliegue de imágenes de servidor personalizadas.
- Amazon FSx for Windows File Server proporciona almacenamiento compartido totalmente gestionado en Windows Server. Siguiendo este patrón, en el FSx caso de Windows, File Server proporciona almacenamiento compartido para los datos y los archivos de registro de SQL Server y para el testigo de quórum.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos. En este patrón, se utiliza para cifrar los secretos de Secrets Manager, el

almacenamiento de SQL Server en los volúmenes de Amazon Elastic Block Store (Amazon EBS) y el FSx sistema de archivos de Windows File Server.

- AWS Secrets Manager lo ayuda a reemplazar las credenciales codificadas en su código, incluidas contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación. En este patrón, las credenciales de Active Directory para instalar y ejecutar SQL Server, las credenciales de usuario `sa` y la información de conexión a la base de datos se almacenan en Secrets Manager.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos. Este patrón utiliza un bucket de Amazon S3 para almacenar la imagen de instalación de SQL Server.
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Otras herramientas

- Microsoft SQL Server FCIs se instala en los nodos del clúster de Windows Server. Además, se pueden instalar en varias subredes. En este patrón, las instancias FCI de SQL Server se instalan en los nodos de WSFC.
- Terraform es una herramienta de infraestructura como código (IaC) que facilita usar el código para aprovisionar y administrar los recursos y la infraestructura en la nube. En este patrón, Terraform se usa para crear los recursos y configurar las instancias FCI de SQL Server.
- Los clústeres de conmutación por error de Windows Server proporcionan características de infraestructura que respaldan la alta disponibilidad de las aplicaciones de servidor alojadas, como SQL Server. En este patrón, los nodos de la FCI utilizan la funcionalidad WSFC para proporcionar una alta disponibilidad local mediante la redundancia a nivel de instancia.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub cluster-amazon-elastic-compute-cloud-amazon-fsx-microsoft -sql-server. Los siguientes recursos están disponibles en el repositorio:

- Un archivo `README.md` que proporciona una descripción general de la solución e información adicional sobre la instalación y el uso

- Un conjunto básico de archivos de configuración de Terraform y un módulo FSx específico de Amazon para aprovisionar los componentes de este patrón
- Un script de configuración de instancias que se ejecuta como un script de datos EC2 de usuario de Amazon
- Un archivo `component.yaml` que Image Builder puede usar para crear una AMI personalizada

Prácticas recomendadas

Seguridad y creación de parches

- Las instalaciones y configuraciones de requisitos previos de la AMI son los requisitos mínimos para implementar clústeres FCI de SQL Server. Es posible que se necesiten configuraciones y software adicionales para cumplir con los estándares y requisitos de seguridad de su organización.
- Después de la implementación, aplique los parches de Windows de forma continua. Parchee directamente las instancias en ejecución o cree una nueva AMI con los últimos parches de Windows y sustituya las instancias (una por una) por la nueva AMI. AWS publica AMIs mensualmente un nuevo Windows que contiene los últimos parches, controladores y agentes de lanzamiento del sistema operativo. Le recomendamos que compruebe las AMI más recientes al lanzar nuevas instancias o al crear sus propias imágenes personalizadas.
- Las EC2 instancias de Amazon están configuradas para permitir todo el tráfico saliente. Cuando se implementan en un entorno de producción, se deben establecer reglas de salida en el grupo de seguridad para restringir este tráfico a los destinos requeridos.
- El sistema de archivos del servidor de archivos FSx para Windows puede registrar automáticamente los registros de auditoría para compartir archivos y acceder a archivos y carpetas y enviarlos al destino deseado si así lo requiere su entorno.
- Rote automáticamente los secretos de Secrets Manager de forma regular. Para el par de claves de EC2 instancia de Amazon, considere una solución de rotación automática, tal como se describe en Cómo usar AWS Secrets Manager para almacenar y rotar pares de claves SSH de forma segura. Para las credenciales de Active Directory y los secretos de credenciales de `sa` de SQL Server, configure la rotación automática de acuerdo con sus políticas de administración de contraseñas.

Administración de Active Directory

- Como parte del clúster de FCI, Windows genera un objeto de nombre de equipo (CNO) en Active Directory. El CNO responde a las solicitudes de DNS y reenvía el tráfico al nodo SQL activo. No recomendamos usar este DNS proporcionado por Active Directory. El TTL es demasiado

alto para proporcionar un tiempo de conmutación por error razonable y, a menudo, tarda más de 5 minutos en reflejar la nueva dirección IP principal. Por el contrario, para las instalaciones de alta disponibilidad, el equilibrador de carga de red interno está configurado para realizar la conmutación por error en 30 segundos.

- Se necesita un administrador de dominio de Active Directory para crear el clúster. Este requisito se debe a los elevados permisos necesarios para crear los objetos del clúster y modificar los permisos en Active Directory. Sin embargo, no es necesario que los servicios de SQL Server se ejecuten como administrador de dominio. Por lo tanto, se recomienda crear un segundo usuario de Active Directory para este fin. Sin embargo, puede eliminar este usuario si los servicios se ejecutan como usuario administrador del dominio. En ese caso, el usuario administrador del dominio debe agregarse al grupo de administradores de Active Directory que se crea como parte de este patrón.

Epics

Configuración de las credenciales del clúster

Tarea	Descripción	Habilidades requeridas
Cree grupos de Active Directory.	En AWS Managed Microsoft AD, cree los siguientes grupos: • Grupo de administradores de clústeres: este grupo se agregará al grupo de administradores local de cada nodo del clúster. • Grupo de escritorios remotos del clúster: este grupo se agregará al grupo local de usuarios de escritorio remoto de cada nodo del clúster. Para obtener más información, consulte Crear un AWS	Administrador de AD

Tarea	Descripción	Habilidades requeridas
	Managed Microsoft AD grupo en la AWS documentación.	
Cree usuarios de Active Directory.	En AWS Managed Microsoft AD, cree los siguientes usuarios • Usuario administrador de dominio: utilice esta cuenta para crear el clúster. • Usuario de dominio: los servicios de SQL Server utilizarán esta cuenta para ejecutarse. Añada este usuario al grupo de administradores de clústeres que creó en la tarea anterior. Para obtener más informaci ón, consulte Crear un AWS Managed Microsoft AD usuario en la AWS documenta ción.	Administrador de AD

Tarea	Descripción	Habilidades requeridas
Añada credenciales de Active Directory a los secretos.	Use Secrets Manager para crear cuatro secretos para almacenar la siguiente información: • Nombre de usuario del administrador del dominio • Contraseña del usuario administrador del dominio. • Nombre de usuario del dominio • Contraseña del usuario del dominio Para obtener más informaci ón, consulte Crear un AWS Secrets Manager secreto en la AWS documentación.	Administrador de AWS

Prepare el entorno

Tarea	Descripción	Habilidades requeridas
Cree la AMI de Windows.	Cree una AMI de Windows personalizada que incluya las configuraciones y el software necesarios. Para obtener más información, consulte Detalles adicionales.	Administrador de AWS, AWS DevOps
Instale Terraform.	Para instalar Terraform, siga las instrucciones del sitio web de Terraform.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Clone el repositorio de este patrón. Para obtener más información, consulte Clonación de un repositorio en el GitHub sitio web.	AWS DevOps

Instalación del clúster

Tarea	Descripción	Habilidades requeridas
Modifique las variables de Terraform.	Actualice el archivo `terraform.tfvars` suministrado para establecer todas las variables en los valores adecuados para su entorno. Por ejemplo, actualice las variables `domain_group_administrators` y `domain_group_rdp_users` para usar su nombre de dominio de Active Directory y el nombre de los grupos de Active Directory creados anteriormente.	AWS DevOps
Inicialice Terraform.	Para ver la implementación propuesta, navegue hasta la raíz del repositorio. Use la interfaz de la línea de comandos (CLI) de Terraform para ejecutar `terraform`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`init` y luego ejecutar `terraform plan`.	
Implemente los recursos.	Para implementar el clúster de SQL y los recursos asociados , utilice la CLI de Terraform para ejecutar `terraform apply`.	AWS DevOps, administrador de AWS

Tarea	Descripción	Habilidades requeridas
Valide la implementación.	Para validar la implement ación, siga estos pasos: 1. Conéctese a una de las EC2 instancias de Amazon de Windows implementadas mediante Remote Desktop. 2. Para obtener más informaci ón, consulta Conectarte a tu instancia de Windows mediante RDP en la AWS documentación. 3. Abra el administrador de clústeres de conmutaci ón por error de Windows. Valide que se haya creado el clúster y que el rol de SQL Server se haya creado y se esté ejecutando. 4. Para probar la conectivi dad y la autenticación con SQL Server, utilice una herramienta de base de datos como SQL Server Management Studio para conectarse al punto de conexión de SQL Server. (El valor del punto de conexión se guarda en Secrets Manager). Para obtener más informaci ón, consulte Connect to Microsoft SQL Server on	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	Amazon EC2 en la AWS documentación.	

Resolución de problemas

Problema	Solución
Se completó el aprovisionamiento de Terraform , pero el administrador de clústeres de conmutación por error de Windows no muestra que se haya creado un clúster o que el clúster se encuentre en un estado no operativo.	La instalación completa de los recursos y la configuración de los clústeres pueden tardar entre 45 y 60 minutos. Una vez que Terraform se haya completado, el script de datos de usuario debe ejecutarse hasta su finalización, lo que requiere varios reinicios . Para supervisar el progreso, puede utilizar el directorio `Checkpoints` de la unidad `C:\` e iniciar sesión en la instalación de SQL Server en `C:\Program Data\Microsoft SQL Server\150\Log` . Cuando haya terminado, aparecerá el mensaje de instalación completa en el archivo `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\UserdataExecution.log` .
Tras aprovisionar un clúster en funcionamiento, no se puede utilizar Terraform para eliminar y volver a crear el clúster. Terraform finaliza, pero el clúster no está configurado correctamente.	Parte del proceso de aprovisionamiento implica registrar máquinas y objetos virtuales en el DNS de Active Directory y Active Directory. Cuando existen nombres de equipo para los nodos del EC2 clúster de Amazon y el nodo del clúster, la FCI no se puede inicializar correctamente y se produce un error en el aprovisionamiento. Para solucionar este problema, siga estos pasos:

Problema	Solución
	1. Elimine los EC2 nodos de Amazon, el ordenador virtual del clúster y el identificador del clúster en los usuarios y ordenadores de Active Directory. 2. Elimine la entrada de DNS del equipo virtual del clúster en el DNS de Active Directory. 3. Ejecute el siguiente comando para eliminar el recurso `terragrunt destroy -target=random_string.cluster_id` de Terraform de la cadena aleatoria del clúster. Esta acción eliminará las EC2 instancias de Amazon existentes. 4. Ejecute `terraform apply` y espere los siguientes tres recursos nuevos: dos EC2 instancias de Amazon de FCI y 1 identificador de clúster de cadena aleatoria.

Recursos relacionados

AWS documentación

- Cree imágenes personalizadas con Image Builder
- Cree una clave KMS
- Crear un depósito de uso general
- Crear una política clave
- Creando tu AWS Managed Microsoft AD

Información adicional

Información del módulo Terraform

Este módulo utiliza una combinación de configuración de AMI y configuración de datos de usuario para obtener una buena combinación de tiempo de aprovisionamiento y estabilidad. Durante el

aprovisionamiento, Windows requiere varios reinicios y esperas. Se ha implementado un método de puntos de control para evitar que se produzcan bucles infinitos durante los reinicios de los datos de usuario persistentes. Los datos de usuario están configurados para ser persistentes. Por lo tanto, los scripts de configuración de los datos de usuario deben seguir desarrollándose para que sean idempotentes. La idempotencia agiliza el proceso de actualización, ya que permite intercambiar instancias durante un ciclo de actualización sin necesidad de realizar una configuración manual para volver a unir los clústeres de la FCI o volver a crearlos.

Cadenas de conexión de SQL Server y clústeres de conmutación por error

El módulo publicará un secreto con la dirección del punto conexión que debe usarse en las cadenas de conexión de esta base de datos. El nombre del secreto sigue este formato: `{environment_name}/sqlserver/{cluster_name}/endpoint`. Para las instalaciones en las que solo se utiliza un nodo, puede esperar que sea la dirección IP de la interfaz de SQL Server de la EC2 instancia de Amazon. Para instalaciones de alta disponibilidad (dos instancias), puede esperar que sea el nombre DNS del equilibrador de carga de red interno.

Este módulo IPs no admite los clústeres virtuales de conmutación por error. Una IP virtual debe permanecer en la misma subred para que funcione. En AWS, una sola subred no puede abarcar varias zonas de disponibilidad. Por lo tanto, el uso de la IPs tecnología virtual eliminaría la posibilidad de que este módulo se considere de alta disponibilidad.

A cada EC2 instancia de Amazon se le asignan tres direcciones IP privadas. El uso es como se indica a continuación:

- IP principal para el tráfico de red: la IP de origen para el tráfico de salida.
- Comunicaciones FCI: se utilizan para mantener el estado y la sincronización del clúster de conmutación por error.
- SQL Server (puerto TCP 1433): oyente y también escucha el tráfico intermitente para determinar qué instancia es la principal.

Configuración de la VPC

Los requisitos previosincluyen un conjunto de opciones de DHCP configurado para usar Active Directory para la resolución de DNS. Sin embargo, este requisito previo no es obligatorio. El requisito más importante es que las EC2 instancias puedan resolver tu nombre de dominio de Active Directory. El cumplimiento de este requisito se puede lograr de otras maneras, como mediante el uso de Amazon Route 53 Resolver puntos finales. Para obtener más información, consulte Integración de la

resolución de DNS de su servicio de directorio con Amazon Route 53 Resolvers (entrada AWS del blog).

Configuración de AMI

La AMI utilizada en este patrón debe contener los siguientes requisitos previos de software y configuraciones:

1. Descargue y amplíe los archivos de instalación de SQL Server 2019 a `C:\SQL_Install_media`.
2. Instale las siguientes características de Windows:
   - `Install-WindowsFeature Failover-Clustering`
   - `Install-WindowsFeature RSAT-AD-PowerShell`
   - `Install-WindowsFeature RSAT-AD-Tools`
   - `Install-WindowsFeature RSAT-Clustering-Mgmt`
   - `Install-WindowsFeature RSAT-Clustering-PowerShell`
   - `Install-WindowsFeature RSAT-Clustering-CmdInterface`
3. Deshabilite el firewall de Windows como se indica a continuación:
   - `Get-NetFirewallProfile | Set-NetFirewallProfile -Enabled False`
4. Habilite el método de autenticación CredSSP (sustituya `<domain>` por el nombre de dominio de Windows de su organización) de la siguiente manera:
   - `Enable-WSManCredSSP -Role "Server" -Force`
   - `Enable-WSManCredSSP -Role "Client" -DelegateComputer *.<domain>.com -Force`
5. Establezca las siguientes claves de registro:
   - Permita las credenciales de autenticación NTLM:
     - `HKLM:\Software\Policies\Microsoft\Windows\CredentialsDelegation`
       - Nombre: `AllowFreshCredentialsWhenNTLMOnly`
       - Valor: 1
       - Tipo: `REG_DWORD`
   - Permita que los ordenadores de dominio local utilicen NTLM desde: PowerShell
     - Ruta: `HKLM:\Software\Policies\Microsoft\Windows\CredentialsDelegation\AllowFreshCredentialsWhenNTLMOnly`
       - Nombre: 1

    - Valor: `wsman/*.<domain>.com`
    - Tipo: `REG_SZ`
6. Configure la PowerShell galería de la siguiente manera:
    - `[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12`
    - `Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force`
    - `Set-PSRepository -Name PSGallery -InstallationPolicy Trusted`
7. Instale los siguientes PowerShell módulos de Windows*:
    - `Install-Module -Name ComputerManagementDsc`
    - `Install-Module -Name FailOverClusterDsc`
    - `Install-Module -Name PSDscResources`
    - `Install-Module -Name xSmbShare`
    - `Install-Module -Name xActiveDirectory`
    - `Install-Module -Name SqlServer`

Para usar Image Builder para crear la AMI, siga las instrucciones de Crear una canalización de imágenes mediante el asistente de consola de EC2 Image Builder en la documentación de Image Builder. Para crear el componente de la receta con los requisitos previos anteriores, siga estos pasos:

1. Descargue el archivo component.yaml de la carpeta del `ami` repositorio. GitHub
2. Copie el contenido en un nuevo componente de Image Builder.
3. Actualice los siguientes marcadores de posición con su información:
    - `<domain>`: su nombre de dominio de Active Directory
    - `<bucket_name>`: nombre del bucket de Amazon S3 que contiene la imagen de SQL Server

Emule las matrices PL/SQL asociativas de Oracle en Amazon Aurora PostgreSQL y Amazon RDS for PostgreSQL

Rajkumar Raghuwanshi, Bhanu Ganesh Gudivada y Sachin Khanna, Amazon Web Services

Resumen

Este patrón describe cómo emular matrices PL/SQL asociativas de Oracle con posiciones de índice vacías en entornos Amazon Aurora PostgreSQL y Amazon RDS for PostgreSQL. También describe algunas de las diferencias entre las matrices PL/SQL asociativas de Oracle y las matrices PostgreSQL con respecto a la forma en que cada una gestiona las posiciones de índice vacías durante las migraciones.

Ofrecemos una alternativa de PostgreSQL al uso de funciones de `aws_oracle_ext` para gestionar posiciones de índice vacías al migrar una base de datos de Oracle. Este patrón utiliza una columna adicional para almacenar las posiciones del índice y mantiene la gestión de matrices dispersas por parte de Oracle, a la vez que incorpora las capacidades nativas de PostgreSQL.

Oracle

En Oracle, las recopilaciones pueden inicializarse como vacías y rellenarse mediante el método de recopilación `EXTEND`, que añade elementos `NULL` a la matriz. Cuando se trabaja con matrices PL/SQL asociativas indexadas por`PLS_INTEGER`, el `EXTEND` método agrega `NULL` elementos secuencialmente, pero los elementos también se pueden inicializar en posiciones de índice no secuenciales. Cualquier posición de índice que no esté inicializada de forma explícita permanece vacía.

Esta flexibilidad permite estructuras de matriz dispersas en las que los elementos se pueden rellenar en posiciones arbitrarias. Al recorrer las recopilaciones utilizando un `FOR LOOP` con límites `FIRST` y `LAST`, solo se procesan los elementos inicializados (`NULL` o sin un valor definido), mientras que las posiciones vacías se omiten.

PostgreSQL (Amazon Aurora y Amazon RDS)

PostgreSQL gestiona los valores vacíos de forma diferente a los valores `NULL`. Almacena los valores vacíos como entidades distintas que utilizan un byte de almacenamiento. Cuando una matriz tiene valores vacíos, PostgreSQL asigna posiciones de índice secuenciales igual que los valores no vacíos. Sin embargo, la indexación secuencial requiere un procesamiento adicional porque el sistema debe recorrer en iteraciones todas las posiciones indexadas, incluidas las vacías. Esto hace que la creación de matrices tradicional sea ineficiente para conjuntos de datos dispersos.

AWS Schema Conversion Tool

El AWS Schema Conversion Tool () normalmente gestiona las migraciones mediante funciones AWS SCT. Oracle-to-PostgreSQL `aws_oracle_ext` En este patrón, proponemos un enfoque alternativo que utiliza las capacidades nativas de PostgreSQL, que combina los tipos de matrices de PostgreSQL con una columna adicional para almacenar las posiciones del índice. A continuación, el sistema puede recorrer en iteraciones las matrices utilizando únicamente la columna de índice.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Permisos de administrador en AWS Identity and Access Management (IAM)
- Una instancia compatible con Amazon RDS o Aurora PostgreSQL
- Habilidades de arquitecto o desarrollador de bases de datos con Oracle y PostgreSQL

Limitaciones

- Algunas Servicios de AWS no están disponibles en todos. Regiones de AWS Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

Este patrón se probó con las siguientes versiones:

- Amazon Aurora PostgreSQL 13.3
- Amazon RDS para PostgreSQL 13.3
- AWS SCT 1.0.674
- Oracle 19c EE

Arquitectura

Pila de tecnología de origen

- On-premises Base de datos Oracle

Pila de tecnología de destino

- PostgreSQL de Amazon Aurora
- Amazon RDS para PostgreSQL

Arquitectura de destino

En el diagrama se muestra lo siguiente:

- Una instancia de base de datos de origen de Amazon RDS para Oracle.
- Una instancia de Amazon EC2 AWS SCT para convertir las funciones de Oracle al equivalente de PostgreSQL
- Una base de datos de destino compatible con Amazon Aurora PostgreSQL.

Tools (Herramientas)

Servicios de AWS

- Amazon Aurora es un motor de base de datos relacional completamente administrado diseñado para la nube y compatible con MySQL y PostgreSQL.
- Amazon Aurora PostgreSQL-Compatible Edition es un motor de base de datos ACID-compliant relacional totalmente gestionado que le ayuda a configurar, operar y escalar las implementaciones de PostgreSQL.
- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Relational Database Service (Amazon RDS) lo ayuda a configurar, utilizar y escalar una base de datos relacional en la Nube de AWS.
- Amazon Relational Database Service (Amazon RDS) para Oracle lo ayuda a configurar, utilizar y escalar una base de datos relacional de Oracle en la Nube de AWS.
- Amazon Relational Database Service (Amazon RDS) para PostgreSQL lo ayuda a configurar, utilizar y escalar una base de datos relacional de PostgreSQL en la Nube de AWS.
- AWS Schema Conversion Tool (AWS SCT) admite migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayoría del código personalizado a un formato compatible con la base de datos de destino.

Otras herramientas

- Oracle SQL Developer es un entorno de desarrollo integrado que simplifica el desarrollo y la administración de bases de datos de Oracle, tanto en implementaciones tradicionales como en implementaciones basadas en la nube.
- pgAdmin es una herramienta de administración de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos. En este patrón, pgAdmin se conecta a la instancia de base de datos de RDS para PostgreSQL y consulta los datos. También puede utilizar el cliente de la línea de comandos psql.

Prácticas recomendadas

- Pruebe los límites de los conjuntos de datos y los escenarios periféricos.
- Considere la posibilidad de implementar la gestión de errores para condiciones de índice fuera de los límites.
- Optimice las consultas para evitar analizar conjuntos de datos dispersos.

Epics

Comportamiento de las matrices asociativas de Oracle (origen)

Tarea	Descripción	Habilidades requeridas

Cree un PL/SQL bloque fuente en Oracle.	Cree un PL/SQL bloque de origen en Oracle que utilice la siguiente matriz asociativa:
	`DECLARE`
	`  TYPE country_codes IS TABLE OF VARCHAR2(100) INDEX BY pls_integer;`
	`  cc country_codes;`
	`  cc_idx NUMBER := NULL;`
	`BEGIN`
	`  cc(7) := 'India';`
	`  cc(3) := 'UK';`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	<pre> cc(5) := 'USA';
	    cc(0) := 'China';
	    cc(-2) := 'Invalid'
	;
	    dbms_output.put_li
	ne('cc_length:' ||
	 cc.COUNT);
	    IF (cc.COUNT > 0)
	 THEN
	        cc_idx :=
	 cc.FIRST;
	        FOR i IN
	 1..cc.COUNT LOOP
	            dbms_outp
	ut.put_line('cc_id
	x:' || cc_idx || '
	 country:' || cc(cc_idx
	));
	            cc_idx :=
	 cc.next(cc_idx);
	        END LOOP;
	    END IF;
	END;</pre>	

Ejecute el PL/SQL bloque.	Ejecute el PL/SQL bloque fuente en Oracle. Si hay brechas entre los valores de índice de una matriz asociativa, no se almacena ningún dato en esas brechas. Esto permite que el bucle de Oracle itere únicamente a través de las posiciones del índice.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

Revise la salida.	Se insertaron cinco elementos en la matriz (`cc`) a intervalos no consecutivos. El recuento de matrices se muestra en el resultado siguiente:
	`cc_length:5`
	`cc_idx:-2 country:I`
	`nvalid`
	`cc_idx:0 country:China`
	`cc_idx:3 country:UK`
	`cc_idx:5 country:USA`
	`cc_idx:7 country:India`
		Administrador de base de datos

Comportamiento de la matriz asociativa de PostgreSQL (destino)

Tarea	Descripción	Habilidades requeridas

Cree un PL/pgSQL bloque de destino en PostgreSQL.	Cree un PL/pgSQL bloque de destino en PostgreSQL que utilice la siguiente matriz asociativa:
	`DO $$`
	`DECLARE`
	`cc character varying(100)[];`
	`cc_idx integer := NULL;`
	`BEGIN`
	`cc[7] := 'India';`
	`cc[3] := 'UK';`
	`cc[5] := 'USA';`
	`cc[0] := 'China';`
	`cc[-2] := 'Invalid'`
	`;`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	<pre> RAISE NOTICE
	 'cc_length: %',
	 ARRAY_LENGTH(cc, 1);
	    IF (ARRAY_LE
	NGTH(cc, 1) > 0) THEN
	        FOR i IN
	 ARRAY_LOWER(cc,
	 1)..ARRAY_UPPER(cc,
	 1)
	        LOOP
	            RAISE NOTICE
	 'cc_idx:% country:%',
	 i, cc[i];
	        END LOOP;
	    END IF;
	END;
	$$;</pre>	

Ejecute el bloque. PL/pgSQL	Ejecute el PL/pgSQL bloque de destino en PostgreSQL. Si hay brechas entre los valores de índice de una matriz asociativa, no se almacena ningún dato en esas brechas. Esto permite que el bucle de PostgreSQL itere solo a través de las posiciones del índice.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

Revise la salida.	La longitud de la matriz es superior a 5 porque NULL se almacena en las brechas entre las posiciones del índice. Como se muestra en el siguiente resultado, el bucle completa 10 iteraciones para recuperar 5 valores de la matriz.
	`cc_length:10`
	`cc_idx:-2 country:I`
	`nvalid`
	`cc_idx:-1 country:<`
	`NULL>`
	`cc_idx:0 country:China`
	`cc_idx:1 country:<`
	`NULL>`
	`cc_idx:2 country:<`
	`NULL>`
	`cc_idx:3 country:UK`
	`cc_idx:4 country:<`
	`NULL>`
	`cc_idx:5 country:USA`
	`cc_idx:6 country:<`
	`NULL>`
	`cc_idx:7 country:India`
		Administrador de base de datos

Emulación del comportamiento de una matriz asociativa de Oracle

Tarea	Descripción	Habilidades requeridas
Cree un PL/pgSQL bloque de destino con una matriz y un tipo definido por el usuario.	Para optimizar el rendimien to y adaptarlo a la funcional idad de Oracle, podemos crear un tipo definido por el	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	usuario que almacene tanto las posiciones del índice como sus datos correspon dientes. Este enfoque reduce las iteraciones innecesarias al mantener las asociaciones directas entre los índices y los valores. `DO $$ DECLARE cc country_codes[]; cc_append country_c odes := NULL; i record; BEGIN cc_append.idx = 7; cc_append.val = 'India'; cc := array_app end(cc, cc_append); cc_append.idx = 3; cc_append.val = 'UK'; cc := array_app end(cc, cc_append); cc_append.idx = 5; cc_append.val = 'USA'; cc := array_app end(cc, cc_append); cc_append.idx = 0; cc_append.val = 'China'; cc := array_app end(cc, cc_append); cc_append.idx = -2; cc_append.val = 'Invalid';`	

Tarea	Descripción	Habilidades requeridas

	<pre> cc := array_app
	end(cc, cc_append);
	    RAISE NOTICE
	 'cc_length: %',
	 ARRAY_LENGTH(cc, 1);
	    IF (ARRAY_LE
	NGTH(cc, 1) > 0) THEN
	        FOR i IN (
	            SELECT
	                *
	            FROM
	
	 unnest(cc)
	            ORDER BY
	                idx)
	                LOOP
	
	 RAISE NOTICE 'cc_idx:
	% country:%', i.idx,
	 i.val;
	                END
	 LOOP;
	    END IF;
	END;
	$$;</pre>	

Ejecuta el PL/pgSQL bloque.	Ejecuta el PL/pgSQL bloque objetivo. Si hay brechas entre los valores de índice de una matriz asociativa, no se almacena ningún dato en esas brechas. Esto permite que el bucle de PostgreSQL itere solo a través de las posiciones del índice.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

Revise la salida.	Como se muestra en el siguiente resultado, el tipo definido por el usuario almacena solo los elementos de datos rellenados, lo que significa que la longitud de la matriz coincide con el número de valores. Como resultado, las iteraciones de `LOOP` se optimizan para procesar solo los datos existentes, lo que elimina la necesidad de rastrear las posiciones vacías.
	`cc_length:5`
	`cc_idx:-2 country:Invalid`
	`cc_idx:0 country:China`
	`cc_idx:3 country:UK`
	`cc_idx:5 country:USA`
	`cc_idx:7 country:India`
		Administrador de base de datos

Resolución de problemas

Problema	Solución
Error de indexación fuera de los límites • Problema: `ERROR: array subscript out of bounds` al acceder a los elementos de la matriz • Causa: se intenta acceder a una posición de índice que no existe en la matriz de tipos definida por el usuario	Puede validar la existencia del índice antes del acceso utilizando un filtro de `WHERE` cláusulas en la `idx` columna al desanidar la matriz, o bien puede implementar controles de límites en el código. PL/pgSQL

Problema	Solución
Gestión de valores NULOS • Problema: aparecen valores NULL inesperados en los resultados de la consulta al recorrer la matriz • Causa: los elementos de la matriz no se inicializaron correctamente con ambos `val` campos antes de `idx` añadirlos	Asegúrese de que ambos campos del tipo definido por el usuario estén rellenados antes de usarlos. `array_append()` Añada comprobaciones NULL explícitas de la siguiente manera: `IF cc_append.val IS NOT NULL THEN cc := array_append(cc, cc_append); END IF;`

Recursos relacionados

AWS documentación

- AWS blog de base de datos
- Manual de estrategias de migración de Oracle a Aurora PostgreSQL

Otra documentación

- Matrices asociativas de Oracle
- Funciones y operadores de matriz de PostgreSQL
- Tipos de PostgreSQL definidos por el usuario

Información adicional

Consideraciones sobre el rendimiento

- Este enfoque reduce la sobrecarga de iteración en un 50% o más para las matrices dispersas en comparación con las matrices PostgreSQL nativas con marcadores de posición NULL.
- La eficiencia del almacenamiento mejora porque solo se almacenan los datos reales, no las posiciones de índice vacías.

Notas de compatibilidad

- Este patrón mantiene la semántica de matrices dispersas de Oracle y, al mismo tiempo, utiliza las capacidades de matrices nativas de PostgreSQL.
- La solución es compatible con todas las versiones de PostgreSQL que admiten tipos compuestos definidos por el usuario.

Habilite conexiones cifradas para instancias de base de datos de PostgreSQL en Amazon RDS

Rohit Kapoor, Amazon Web Services

Resumen

Amazon Relational Database Service (Amazon RDS) admite el cifrado SSL en instancias de base de datos PostgreSQL. Con SSL, puede cifrar una conexión de PostgreSQL entre sus aplicaciones y sus instancias de base de datos de Amazon RDS para PostgreSQL. De forma predeterminada, Amazon RDS for SSL/TLS PostgreSQL utiliza y espera que todos los clientes se conecten mediante cifrado. SSL/TLS Amazon RDS para PostgreSQL admite las versiones 1.1 y 1.2 de TLS.

En este patrón se describe cómo puede habilitar conexiones cifradas para una instancia de base de datos de Amazon RDS para PostgreSQL. Puede usar el mismo proceso para habilitar conexiones cifradas en Amazon Aurora compatible con PostgreSQL.

Requisitos previos y limitaciones

- Una cuenta de AWS activa
- Una instancia de base de datos de Amazon RDS para PostgreSQL
- Un paquete SSL

Arquitectura

Tools (Herramientas)

- pgAdmin es una plataforma de administración y desarrollo de código abierto para PostgreSQL. Puede usar pgAdmin en Linux, Unix, macOS y Windows para administrar los objetos de su base de datos en PostgreSQL 10 y versiones posteriores.
- Los editores de PostgreSQL proporcionan una interfaz más fácil de usar que le ayuda a crear, desarrollar y ejecutar consultas, así como a editar el código según sus necesidades.

Prácticas recomendadas

- Supervise las conexiones de bases de datos no seguras.

- Audite los derechos de acceso a la base de datos.
- Asegúrese de que las copias de seguridad y las instantáneas estén cifradas en reposo.
- Supervise el acceso a bases de datos.
- Evite los grupos de acceso sin restricciones.
- Mejora tus notificaciones con Amazon GuardDuty.
- Supervise el cumplimiento de las políticas con regularidad.

Epics

Descargue un certificado de confianza e impórtelo a su almacén de confianza

Tarea	Descripción	Habilidades requeridas
Cargue un certificado de confianza en su computadora.	Para agregar certificados al almacén de entidades emisoras de certificados raíz de confianza de su equipo, siga estos pasos. (Estas instrucciones usan Windows Server como ejemplo). 1. En Windows Server, seleccione Iniciar, Ejecutar y, a continuación, escriba mmc. 2. En la consola, elija Archivo, Agregar/Quitar complemento. 3. En Complementos disponibles, elija Certificados y, a continuación, elija Agregar. 4. En Este complemento siempre administrará los certificados de, elija Cuenta	DevOps ingeniero, ingeniero de migración, DBA

Tarea	Descripción	Habilidades requeridas
	de equipo y pulse Siguiente . 5. Seleccione Equipo local y, a continuación, Finalizar. 6. Si no tiene más complemen tos que añadir a la consola, pulse Aceptar. 7. En el árbol de la consola, haga doble clic en Certifica dos. 8. Haga clic con el botón derecho en Entidades emisoras de certificados raíz. 9. Seleccione Todas las tareas, Importar para importar los certificados descargados. 10. Siga los pasos del asistente de importación de certifica dos.	

Fuerza las conexiones SSL.

Tarea	Descripción	Habilidades requeridas
Cree un grupo de parámetro s y establezca el parámetro rds.force_ssl.	Si la instancia de base de datos PostgreSQL tiene un grupo de parámetros personali zado, edite dicho grupo y cambie `rds.force_ssl` a 1.	DevOps ingeniero, ingeniero de migración, DBA

Tarea	Descripción	Habilidades requeridas
	Si la instancia de base de datos usa el grupo de parámetros predeterminado sin `rds.force_ssl` habilitado, cree un nuevo grupo de parámetros. Puede modificar el nuevo grupo de parámetros usando la API de Amazon RDS o bien manualmente siguiendo estos pasos. Para crear un nuevo grupo de parámetros: 1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon RDS para la región de AWS que aloja la instancia de base de datos. 2. En el panel de navegació n, seleccione Grupos de parámetros. 3. Elija Crear grupo de parámetros y defina los siguientes valores: • En Familia de grupo de parámetros, elija postgres14. • En Nombre de grupo, escriba pgsql-<da tabase_instance>-ssl.	

Tarea	Descripción	Habilidades requeridas
	• En Descripción, introduzca una descripción en formato libre para el grupo de parámetros que va a añadir. • Seleccione Crear. 4. Elija el grupo de parámetros que ha creado. 5. En Parameter group actions (Acciones de grupos de parámetros), seleccione Edit (Editar). 6. Busque rds.force_ssl y cambie su configuración a 1. **Note** Realice pruebas del cliente antes de cambiar este parámetro. 7. Seleccione Save changes (Guardar cambios). Para asociar el grupo de parámetros a su instancia de base de datos PostgreSQL: 1. En la consola de Amazon RDS, en el panel de navegación, elija Bases de datos y, a continuación,	

Tarea	Descripción	Habilidades requeridas
	seleccione la instancia de base de datos PostgreSQL. 2. Elija Modificar. 3. En Configuración adicional, seleccione el nuevo grupo de parámetros y, a continuación, elija Continuar. 4. En Programar modificaciones, elija Aplicar inmediatamente. 5. Elija Modify DB instance (Modificar la instancia de la base de datos). Para obtener más información, consulte la documentación de Amazon RDS.	
Fuerza las conexiones SSL.	Conéctese a la instancia de base de datos de Amazon RDS para PostgreSQL. Los intentos de conexión que no usan SSL se rechazan con un mensaje de error. Para obtener más información, consulte la documentación de Amazon RDS.	DevOps ingeniero, ingeniero de migración, DBA

Instale la extensión SSL

Tarea	Descripción	Habilidades requeridas

Instale la extensión SSL.	1. Inicie una conexión psql o pgAdmin como Administrador de base de datos.
	2. Llame a la función ssl_is_used () para determinar si se está usando SSL.
	`select ssl_is_used();`
	La función devuelve `t` si la conexión usa SSL; de lo contrario, devuelve `f`.
	3. Instale la extensión SSL.
	`create extension sslinfo;`
	`show ssl;`
	`select ssl_cipher();`
	Para obtener más información, consulte la documentación de Amazon RDS.
		DevOps ingeniero, ingeniero de migración, DBA

Configure su cliente PostgreSQL para SSL

Tarea	Descripción	Habilidades requeridas
Configure un cliente para SSL.	Al usar SSL, puede iniciar el servidor PostgreSQL con soporte para conexiones cifradas que empleen protocolos TLS. El servidor	DevOps ingeniero, ingeniero de migración, DBA

Tarea	Descripción	Habilidades requeridas

	escucha tanto las conexiones estándar como las SSL en el mismo puerto TCP, y negocia con cualquier cliente que se conecte si debe utilizar SSL. Por defecto, esto es una una opción de cliente.
	
	Si usa el cliente psql:
	
	1. Asegúrese de que el certificado Amazon RDS se ha cargado en su computadora local.
	2. Inicie una conexión de cliente SSL añadiendo lo siguiente:
	
	`psql postgres -h SOMEHOST.amazonaws.com -p 8192 -U someuser sslmode=verify-full sslrootcert=rds-ssl-ca-cert.pem`
	`select ssl_cipher();`
	
	Para otros clientes de PostgreSQL:
	
	• Modifique el parámetro de clave pública de la aplicación correspondiente. Esto puede estar disponible como una opción, como parte de su cadena de	

Tarea	Descripción	Habilidades requeridas
	conexión, o como una propiedad en la página de conexión en las herramien tas de la interfaz gráfica de usuario. Consulte las siguientes páginas para estos clientes: • Documentación de pgAdmin • Documentación de JDBC	

Resolución de problemas

Problema	Solución
No se puede descargar el certificado SSL.	Compruebe la conexión al sitio web y vuelva a intentar descargar el certificado en su computadora local.

Recursos relacionados

- Documentación de Amazon RDS para PostgreSQL
- Uso de SSL con una instancia de base de datos PostgreSQL (documentación de Amazon RDS)
- TCP/IP Conexiones seguras con SSL (documentación de PostgreSQL)
- Uso de SSL (documentación de JDBC)

Cifrar una instancia de base de datos de Amazon RDS para PostgreSQL existente

Piyush Goyal, Shobana Raghu y Yaser Raja, Amazon Web Services

Resumen

Este patrón explica cómo cifrar una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para PostgreSQL en la nube de AWS con un tiempo de inactividad mínimo. Este proceso también funciona para instancias de base de datos de Amazon RDS para MySQL.

Puede habilitar el cifrado para una instancia de base de datos de Amazon RDS cuando la cree, pero no después de haberla creado. Sin embargo, puede añadir cifrado a una instancia de base de datos sin cifrar creando una instantánea de la instancia de base de datos y, a continuación, creando una copia cifrada de esa instantánea. A continuación, puede restaurar una instancia de base de datos a partir de la instantánea encriptada para obtener una copia encriptada de su instancia de base de datos original. Si su proyecto permite un tiempo de inactividad (al menos en el caso de las transacciones de escritura) para esta actividad, esto es todo lo que tiene que hacer. Cuando esté disponible la nueva copia cifrada de la instancia de base de datos, podrá dirigir sus aplicaciones a la nueva base de datos. Sin embargo, si su proyecto no permite un tiempo de inactividad significativo para esta actividad, necesitará un enfoque alternativo que le ayude a minimizar dicho tiempo de inactividad. Este patrón emplea AWS Database Migration Service (AWS DMS) para migrar y replicar continuamente los datos, de modo que la transición a la nueva base de datos cifrada se podrá realizar con un tiempo de inactividad mínimo.

En las instancias de base de datos cifradas de Amazon RDS se utiliza el algoritmo de cifrado AES-256 estándar del sector para cifrar los datos en el servidor que aloja la instancia de base de datos de Amazon RDS. Una vez cifrados los datos, Amazon RDS se encarga de la autenticación de acceso y del descifrado de los datos de forma transparente, con un impacto mínimo en el desempeño. No es necesario modificar las aplicaciones cliente de base de datos para utilizar el cifrado.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una instancia de base de datos de Amazon RDS para PostgreSQL sin encriptar

- Experiencia trabajando con tareas de AWS DMS (creación, modificación o detención) (consulte Trabajar con tareas de AWS DMS en la documentación de AWS DMS)
- Familiaridad con AWS Key Management Service (AWS KMS) para el cifrado de bases de datos (consulte la documentación de AWS KMS)

Limitaciones

- Únicamente se puede activar el cifrado para una instancia de base de datos de Amazon RDS al crearla, no después de que se ha creado.
- Los datos de las tablas no registradas no se podrán restaurar mediante instantáneas. Para obtener más información, consulte Prácticas recomendadas para trabajar con PostgreSQL.
- No se puede tener una réplica de lectura cifrada de una instancia de base de datos sin cifrar ni una réplica de lectura sin cifrar de una instancia de base de datos cifrada.
- No se puede restaurar una copia de seguridad ni una instantánea sin cifrar en una instancia de base de datos cifrada.
- AWS DMS no transfiere automáticamente las secuencias, por lo que necesitará pasos adicionales para gestionarlas.

Para obtener más información, consulte Limitaciones de las instancias de base de datos cifradas de Amazon RDS en la documentación de Amazon RDS.

Arquitectura

Arquitectura de origen

- Instancia de base de datos de RDS sin cifrar

Arquitectura de destino

- Instancia de base de datos de RDS cifrada
  - La instancia de base de datos de RDS de destino se crea restaurando la copia de instantánea de base de datos de la instancia de base de datos de RDS de origen.
  - Al restaurar la instantánea, se emplea una clave de AWS KMS para el cifrado.
  - Para migrar los datos, se emplea una tarea de replicación de AWS DMS.

Tools (Herramientas)

Herramientas usadas para habilitar el cifrado:

- Clave de AWS KMS prara encriptar: Cuando crea una instancia de base de datos cifrada, puede elegir una clave administrada por el cliente o la clave de AWS KMS para Amazon RDS para cifrar la instancia de base de datos. Si no especifica el identificador de clave para una clave administrada por el cliente, Amazon RDS utiliza la clave administrada de AWS para la nueva instancia de base de datos. Amazon RDS crea una clave administrada de AWS para Amazon RDS para su cuenta de AWS. Su cuenta de AWS tiene una clave administrada de AWS diferente para Amazon RDS para cada región de AWS. Para obtener más información sobre el uso de claves de KMS para el cifrado de Amazon RDS, consulte Cifrar recursos de Amazon RDS.

Herramientas utilizadas para la replicación continua:

- AWS DMS: puede usar AWS Database Migration Service (AWS DMS) para replicar los cambios desde la base de datos de origen a la base de datos de destino. Es importante mantener sincronizadas las bases de datos de origen y destino para poder reducir al mínimo el tiempo de inactividad. Para obtener información sobre la configuración de AWS DMS y la creación de tareas, consulte la documentación de AWS DMS.

Epics

Cree una instantánea de la instancia de base de datos de origen y cífrela

Tarea	Descripción	Habilidades requeridas
Compruebe los detalles de la instancia de base de datos PostgreSQL de origen.	En la consola de Amazon RDS, seleccione la instancia de base de datos PostgreSQL de origen. En la pestaña Configuración, asegúrese de que el cifrado no esté habilitado en esta instancia. Para ver una ilustración de la	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	pantalla, consulte la sección de Información adicional.	
Crear la instantánea de base de datos.	Cree una instantánea de la base de datos de la instancia que desea encriptar. La cantidad de tiempo que tarda en crearse una instantánea depende del tamaño de su base de datos. Para obtener instrucciones, consulte Crear una instantánea de base de datos en la documentación de Amazon RDS.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cifre la instantánea.	En el panel de navegación de la consola de Amazon RDS, elija Instantáneas y, a continuación, seleccione la instantánea de base de datos que ha creado. En Actions (Acciones), elija Copy Snapshot (Copiar instantánea). Indique la región de AWS de destino y el nombre de la copia de la instantánea de base de datos en los campos correspondientes. Seleccione la casilla de verificación Habilitar el cifrado. En Master Key, especifique el identificador de la clave de KMS que se debe usar para cifrar la copia de la instantánea de base de datos. Elija Copy Snapshot. Para más información, consulte Copiar una instantánea en la documentación de Amazon RDS.	Administrador de base de datos

Prepare la instancia de base de datos de destino

Tarea	Descripción	Habilidades requeridas
Restaurare la instantánea de la base de datos.	En la consola de Amazon RDS, seleccione Instantáneas. Elija la instantánea cifrada que ha creado. En Actions (Acciones), seleccion	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	e Restore Snapshot (Restaura r instantánea). Para Identific ador de Instancia de la base de datos, proporcione un nombre único para la nueva instancia de la base de datos. Revise los detalles de la instancia y, a continuac ión, seleccione Restaurar instancia de base de datos. Se creará una nueva instancia de base de datos cifrada a partir de la instantánea. Para más información, consulte Restauración a partir de una instantánea de la base de datos en la documentación de Amazon RDS.	
Migre los datos mediante AWS DMS.	En la consola de AWS DMS, cree una tarea de AWS DMS. En Tipo de migración , elija Migración de los datos existentes y réplica de los cambios en curso. En Configuración de tareas, en el Modo de preparación de la tabla de destino, seleccione Truncar. Para más informaci ón, consulte Crear una tarea en la documentación de AWS DMS.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Habilitar la validación de datos.	En Configuración de tareas, seleccione Habilitar validación. Esto le permite comparar los datos de origen con los de destino para verificar que los datos se han migrado correctamente.	Administrador de base de datos
Deshabilite las restricciones en la instancia de base de datos de destino.	Desactive todos los desencadenantes y restricciones de clave externa en la instancia de base de datos de destino y, a continuación, inicie la tarea de AWS DMS. Para obtener más información sobre cómo deshabilitar los desencadenantes y restricciones de clave externa, consulte la documentación de AWS DMS.	Administrador de base de datos
Compruebe los datos.	Una vez completada la carga, compruebe los datos de la instancia de base de datos de destino para asegurarse de que coinciden con los datos de origen. Para obtener más información consulte la AWS DMS data validation (Validación de datos de AWS DMS) en la documentación de AWS DMS.	Administrador de base de datos

Transición a la instancia de base de datos de destino

Tarea	Descripción	Habilidades requeridas
Detenga las operaciones de escritura en la instancia de base de datos de origen.	Detenga las operaciones de escritura en la instancia de base de datos de origen para que pueda comenzar el tiempo de inactividad de la aplicación. Compruebe que AWS DMS haya completad o la replicación de los datos en el proceso. Habilite los desencadenantes y claves externas en la instancia de base de datos de destino.	Administrador de base de datos
Actualice las secuencias de la base de datos	Si la base de datos de origen contiene números de secuencia, compruebe y actualice las secuencias en la base de datos de destino.	Administrador de base de datos
Configure el punto de conexión de la aplicación.	Configure las conexiones de la aplicación para usar los nuevos puntos de conexión de la instancia de base de datos de Amazon RDS. La instancia de base de datos ya está cifrada.	Administrador de base de datos, propietario de la aplicación

Recursos relacionados

- Creación de una tarea de AWS DMS
- Supervisión de las tareas de replicación mediante Amazon CloudWatch
- Monitorización de tareas de AWS DMS

- Actualización de la clave de cifrado de Amazon RDS

Información adicional

Comprobar el cifrado de la instancia de base de datos PostgreSQL de origen:

Notas adicionales para este patrón:

- Habilite la replicación en PostgreSQL estableciendo el parámetro `rds.logical_replication` en 1.

Nota importante: Las ranuras de replicación retienen los archivos de registro de escritura anticipada (WAL) hasta que los archivos se consumen externamente, por ejemplo, mediante `pg_recvlogical`, mediante trabajos de extracción, transformación y carga (ETL) o mediante AWS DMS. Al establecer el valor del parámetro `rds.logical_replication` en 1, AWS DMS establece los parámetros `wal_level`, `max_wal_senders`, `max_replication_slots` y `max_connections`. Si hay ranuras de replicación lógica pero no se consumen los archivos WAL retenidos por la ranura de replicación, es posible que aumente el uso del disco del registro de transacciones y disminuya el espacio de almacenamiento libre. Para obtener más información y los pasos para resolver este problema, consulte el artículo ¿Cómo puedo identificar la causa del error «No queda espacio en el dispositivo» o «» DiskFull en Amazon RDS for PostgreSQL? en el centro de conocimiento de AWS Support.

- Los cambios de esquema que realice en la instancia de base de datos de origen tras crear la instantánea de base de datos no quedarán reflejados en la instancia de base de datos de destino.
- Después de crear una instancia de base de datos encriptada, no puede cambiar la clave KMS utilizada por esa instancia de base de datos. Asegúrese de determinar los requisitos de su clave de KMS antes de crear la instancia de base de datos cifrada.
- Debe deshabilitar los desencadenantes y claves externas en la instancia de base de datos de destino antes de ejecutar la tarea de AWS DMS. Podrá volver a habilitarlos cuando se complete la tarea.

Imponga el etiquetado automático de las bases de datos de Amazon RDS en el lanzamiento

Susanne Kangnoh y Archit Mathur, Amazon Web Services

Resumen

Amazon Relational Database Service (Amazon RDS) es un servicio web que facilita la configuración, el funcionamiento y la escala de una base de datos relacional en la nube de Amazon Web Services (AWS). Proporciona una capacidad rentable y de tamaño ajustable para una base de datos relacional estándar y se ocupa de las tareas de administración de bases de datos comunes.

Las etiquetas le permiten clasificar los recursos de AWS de diversas maneras. El etiquetado de bases de datos relacionales es útil cuando tiene muchos recursos en la cuenta y desea identificar rápidamente un recurso específico en función de las etiquetas. Puede utilizar etiquetas de Amazon RDS para añadir metadatos personalizados a las instancias de base de datos de RDS. Una etiqueta es una marca que consta de una clave y un valor definidos por el usuario. Le recomendamos que cree un conjunto de etiquetas coherente para satisfacer los requisitos de su organización.

Este patrón proporciona una CloudFormation plantilla de AWS que le ayuda a supervisar y etiquetar las instancias de base de datos de RDS. La plantilla crea un evento de Amazon CloudWatch Events que vigila el DBInstance evento AWS CloudTrail Create. (CloudTrail captura las llamadas a la API de Amazon RDS como eventos). Cuando detecta este evento, llama a una función de AWS Lambda que aplica automáticamente las claves de etiquetas y los valores que usted defina. La plantilla también envía una notificación de que la instancia ha sido etiquetada mediante Amazon Simple Notification Service (Amazon SNS).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un bucket de Amazon Simple Storage Service (Amazon S3) para cargar el código de Lambda.
- Una dirección de correo electrónico activa en la que recibir las notificaciones de etiquetado.

Limitaciones

- La solución es compatible con CloudTrail Create DBInstance events. No crea notificaciones para ningún otro evento.

Arquitectura

Arquitectura de flujo de trabajo

Automatización y escala

- Puede utilizar la CloudFormation plantilla de AWS varias veces para distintas regiones y cuentas de AWS. Debe ejecutar la plantilla solo una vez en cada región o cuenta.

Tools (Herramientas)

Servicios de AWS

- AWS CloudTrail: AWS CloudTrail es un servicio de AWS que le ayuda con la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de su cuenta de AWS. Las acciones realizadas por un usuario, un rol o un servicio de AWS se registran como eventos en CloudTrail.
- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS. CloudWatch Events se da cuenta de los cambios operativos a medida que se producen y toma las medidas correctivas necesarias, mediante el envío de mensajes en respuesta al entorno, la activación de funciones, la introducción de cambios y la recopilación de información sobre el estado.
- AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable que se puede utilizar para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio web que permite a las aplicaciones, los usuarios finales y los dispositivos enviar y recibir al instante notificaciones desde la nube.

Codigo

Este patrón incluye un adjunto con dos archivos:

- `index.zip` es un archivo comprimido que incluye el código de Lambda de este patrón.
- `rds.yaml`es una CloudFormation plantilla que despliega el código Lambda.

Consulte la sección Epics para obtener información sobre cómo usar estos archivos.

Epics

Implementar el código de Lambda

Tarea	Descripción	Habilidades requeridas
Cargue el código en un bucket de S3.	Cree un bucket de S3 nuevo o utilice un bucket de S3 ya existente para cargar el archivo adjunto `index.zip` (código de Lambda). Este bucket debe estar en la misma región de AWS que los recursos (instancias de base de datos de RDS) que desea supervisar.	Arquitecto de la nube
Implemente la plantilla CloudFormation .	Abra la consola de Cloudform ation en la misma región de AWS que el bucket de S3 e implemente el archivo `rds.yaml` que se incluye en el archivo adjunto. En la siguiente Epic, proporcione los valores de los parámetros.	Arquitecto de la nube

Complete los parámetros de la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Proporcione el nombre del bucket de S3.	Escriba el nombre del bucket de S3 que ha creado o	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	seleccionado en la primera Epic. Este bucket de S3 contiene el archivo.zip del código Lambda y debe estar en la misma región de AWS que CloudFormation la plantilla y las instancias de base de datos de RDS que desea supervisar.	
Proporcione la clave de S3.	Proporcione la ubicación del archivo .zip del código de Lambda en su bucket de S3, sin barras diagonales iniciales (por ejemplo, `index.zip` o `controls/index.zip`).	Arquitecto de la nube
Proporcione una dirección de correo electrónico.	Proporcione una dirección de correo electrónico activa en la que desee recibir notificac iones de infracciones.	Arquitecto de la nube
Especifique un nivel de registro.	Especifique el nivel de registro y el detalle. `Info` designa mensajes informativos detallados sobre el progreso de la aplicación y solo debe usarse para la depuración. `Error` designa los eventos de error que aún podrían permitir que la aplicación siguiera ejecutándose. `Warning` designa situaciones potencial mente dañinas.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Introduzca las claves y los valores de las etiquetas de sus instancias de base de datos de RDS.	Escriba las claves de etiqueta y los valores que desea aplicar automáticamente a la instancia de RDS. Para más información, consulte Etiquetar recursos de base de datos de Amazon en la documentación de AWS.	Arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirme la suscripción de correo electrónico.	Cuando la CloudFormation plantilla se implementa correctamente, envía un mensaje de correo electrónico de suscripción a la dirección de correo electrónico que proporcionó. Debe confirmar esta suscripción de correo electrónico para recibir notificaciones de cuando se han etiquetado sus instancias.	Arquitecto de la nube

Recursos relacionados

- Creación de un bucket (documentación de Amazon S3)
- Etiquetado de los recursos de Amazon RDS (documentación de Amazon Aurora)
- Carga de objetos (documentación de Amazon S3)
- Creación de una regla de CloudWatch eventos que se active en una llamada a la API de AWS mediante AWS CloudTrail (CloudWatch documentación de Amazon)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Estime el costo de una tabla de DynamoDB para la capacidad bajo demanda

Moinul Al-Mamun, Amazon Web Services

Resumen

Amazon DynamoDB es una base de datos transaccional NoSQL que proporciona una latencia de milisegundos de un solo dígito incluso a escala de petabytes. Esta oferta sin servidor de Amazon Web Services (AWS) se está haciendo popular debido a su rendimiento y escalabilidad consistentes. No es necesario aprovisionar la infraestructura subyacente. Su única tabla puede crecer hasta petabytes.

Con el modo de capacidad bajo demanda, usted paga por solicitud por las lecturas y escrituras de datos que la aplicación realiza en las tablas. Los cargos de AWS se basan en las unidades de solicitud de lectura (RRUs) y las unidades de solicitud de escritura (WRUs) acumuladas en un mes. DynamoDB supervisa el tamaño de la tabla de forma continua durante todo el mes para determinar los cargos de almacenamiento. Admite copias de seguridad continuas con point-in-time-recovery (PITR). DynamoDB supervisa el tamaño de la tabla habilitada para PITR de forma continua durante todo el mes para determinar los cargos de la copia.

Para estimar el costo de DynamoDB para un proyecto, es importante calcular cuánto RRU, WRU y almacenamiento se consumirán en las diferentes etapas del ciclo de vida del producto. Para obtener una estimación aproximada de los costes, puede utilizar la calculadora de precios de AWS, pero debe proporcionar un número aproximado de RRUs y los requisitos de almacenamiento de la tabla. WRUs Puede resultar difícil estimarlos al principio del proyecto. La calculadora de precios de AWS no tiene en cuenta la tasa de crecimiento de los datos ni el tamaño de los elementos, ni el número de lecturas y escrituras de la tabla base y de los índices secundarios globales (GSIs) por separado. Para utilizar la calculadora de precios de AWS, debe estimar todos esos aspectos a fin de suponer cifras aproximadas de la WRU, la RRU y el tamaño del almacenamiento a fin de obtener una estimación de los costos.

Este patrón proporciona un mecanismo y una plantilla de Microsoft Excel reutilizable para estimar los factores de costo básicos de DynamoDB, como los costos de escritura, lectura, almacenamiento, copia de seguridad y recuperación, para el modo de capacidad bajo demanda. Es más detallada que la calculadora de precios de AWS y considera la tabla base y GSIs los requisitos de forma independiente. También tiene en cuenta la tasa de crecimiento mensual de los datos por artículo y prevé los costos para tres años.

Requisitos previos y limitaciones

Requisitos previos

- Conocimientos básicos de DynamoDB y diseño de modelos de datos de DynamoDB
- Conocimientos básicos sobre los precios de DynamoDB, WRU, RRU, almacenamiento y copia de seguridad y recuperación (para obtener más información, consulte Precios de la capacidad bajo demanda)
- Conocimiento de los datos, el modelo de datos y el tamaño de los elementos en DynamoDB
- Conocimientos de DynamoDB GSIs

Limitaciones

- La plantilla proporciona un cálculo aproximado, pero no es adecuada para todas las configuraciones. Para obtener una estimación más precisa, debe medir el tamaño individual de cada elemento de la tabla base y. GSIs
- Para obtener una estimación más precisa, debe tener en cuenta el número esperado de escrituras (insertar, actualizar y eliminar) y lecturas de cada elemento en un mes promedio.
- Este patrón permite estimar únicamente los costos de escritura, lectura, almacenamiento y copia de seguridad y recuperación para los próximos años, sobre la base de hipótesis de crecimiento fijo de los datos.

Tools (Herramientas)

Servicios de AWS

- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.

Otras herramientas

- La Calculadora de precios de AWS es una herramienta de planificación basada en la web destinada a crear presupuestos para los casos de uso de AWS.

Prácticas recomendadas

Para ayudar a mantener los costos bajos, tenga en cuenta las siguientes prácticas recomendadas de diseño de DynamoDB.

- Diseño de claves de partición: utilice una clave de partición de alta cardinalidad para distribuir la carga de manera uniforme.
- Patrón de diseño de lista de adyacencia: utilice este patrón de diseño para la gestión one-to-many y many-to-many las relaciones.
- Índice disperso: utilice un índice disperso para su. GSIs Cuando crea un GSI, especifica una clave de partición y, de forma opcional, una clave de clasificación. Solo los elementos de la tabla base que contienen la clave de partición de GSI correspondiente aparecen en el índice disperso. Esto ayuda a mantener GSIs el tamaño más pequeño.
- Sobrecarga de índices: utilice el mismo GSI para indexar varios tipos de elementos.
- Partición de escritura de GSI: particione de manera inteligente para distribuir los datos entre las particiones y realice consultas más rápidas y eficientes.
- Elementos grandes: solo almacene los metadatos dentro de la tabla, guarde el blob en Amazon S3 y guarde la referencia en DynamoDB. Divida los elementos grandes en varios elementos e indexe de manera eficiente mediante claves de clasificación.

A fin de conocer más prácticas recomendadas de diseño, consulte la Guía para desarrolladores de Amazon DynamoDB.

Epics

Extraiga la información de los artículos de su modelo de datos de DynamoDB

Tarea	Descripción	Habilidades requeridas
Obtener el tamaño del artículo.	1. Compruebe cuántos tipos diferentes de objetos vas a almacenar en su tabla. 2. Para calcular el tamaño de cada elemento en kilobytes, añada el tamaño de clave y valor de cada atributo.	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	3. Calcule el tamaño del elemento para una tabla base y para cada GSI.	

Tarea	Descripción	Habilidades requeridas

Calcule el costo de escritura.	Para estimar el coste de escritura en el modo de capacidad bajo demanda, primero hay que medir la cantidad que se WRUs consumirá en un mes. Para ello, debe tener en cuenta los siguientes factores:
	• Número de operaciones de creación, actualización y eliminación para cada elemento en un mes.
	• Número de disponibles GSIs. Considere cada índice de forma independi ente.
	  • Tamaño medio de un elemento del índice
	  • Número de tiempos de sincronización en un índice
	• ¿Cuántas cosas nuevas (por ejemplo, componentes o productos) se añadirán a la tabla cada mes? La cantidad de elementos que se añaden puede variar cada mes, pero puede suponer una tasa de crecimiento media en función de sus modelos de negocio.
		Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte la sección Additional information (Información adicional).	
Calcule el costo de lectura.	Para estimar el coste de lectura en el modo bajo demanda, primero hay que medir cuántas se RRUs consumirán en un mes. Para ello, debe tener en cuenta los siguientes factores: • Número de disponibles GSIs. Considere cada índice de forma independiente. • Tamaño medio de un elemento del índice • Número medio de lecturas por producto al mes. • Número total de elementos disponibles (componentes o productos) en la tabla de DynamoDB.	Desarrollador de aplicaciones, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
Calcule el tamaño y el costo del almacenamiento.	En primer lugar, calcule el requisito de almacenamiento mensual promedio en función del tamaño del artículo de la tabla. A continuación, calcule el costo de almacenamiento multiplicando el tamaño de almacenamiento por el precio por GB de almacenamiento de su región de AWS. Si ya ha introducido datos para estimar el costo de escritura, no es necesario que los vuelva a introduci r para calcular el tamaño de almacenamiento. De lo contrario, para estimar el tamaño de almacenamiento, debe tener en cuenta los siguientes factores: • Número de elementos de datos en un módulo (producto) según el diseño de la tabla. • Tamaño medio de los elementos en kilobytes. • Número de disponibles GSIs. Considere cada índice de forma independi ente. • Tamaño medio de un elemento del índice	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	• ¿Cuántas cosas nuevos productos se añadirán a la tabla cada mes? La cantidad de productos que se añaden puede variar cada mes, pero puede suponer una tasa de crecimiento media en función de sus modelos de negocio. En este ejemplo, se utiliza una media de 10 millones de productos nuevos cada mes.	

Introduzca la información del artículo y el objeto en la plantilla de Excel

Tarea	Descripción	Habilidades requeridas
Descargue la plantilla de Excel de la sección de adjuntos y ajústela para que se adapte a su tabla de casos de uso.	1. Descargue la plantilla de Excel. 2. Ajuste el módulo de negocios y GSIs, según el diseño de su mesa.	Ingeniero de datos
Introduzca la información en la plantilla de Excel.	1. Actualice la información del artículo en la hoja. Actualice los datos solo en las celdas naranjas. 2. Ajuste los números de los objetos: ¿cuánto se puede añadir a la tabla cada mes? 3. Actualice los precios de la WRU y la RRU por millón para su región de AWS.	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	4. Actualice los precios de almacenamiento y copias de seguridad por GB al mes para su región de AWS. 5. Actualice el precio de recuperación por GB para su región de AWS. En la plantilla, hay tres elementos o entidades: información, metadatos y relación. Hay dos GSIs. Para su caso de uso, si necesita más elementos, cree filas nuevas. Si necesitas más GSIs, copia un bloque de GSI existente y pégalo para crear tantos bloques de GSI como necesites. A continuación, ajuste los cálculos de las columnas SUM y TOTAL.	

Recursos relacionados

Referencias

- Precios de Amazon DynamoDB para capacidad bajo demanda
- Calculadora de precios de AWS para DynamoDB
- Prácticas recomendadas para el diseño y la arquitectura con DynamoDB
- Introducción a DynamoDB

Guías y patrones

- Modelado de datos con Amazon DynamoDB

- Costos de almacenamiento estimados para una tabla de Amazon DynamoDB

Información adicional

Ejemplo de cálculo de costos de escritura

El diseño del modelo de datos de DynamoDB muestra tres elementos por producto y un tamaño medio de artículo de 4 KB. Al añadir un producto nuevo a la tabla base de DynamoDB, consume el número de elementos * (tamaño del elemento/unidad de escritura de 1 KB) = 3 * (4/1) = 12 WRU. En este ejemplo, si se escribe 1 KB, el producto consume 1 WRU.

Lea el ejemplo de cálculo de costos

Para obtener la estimación de la RRU, considere el promedio de cuántas veces se leerá cada elemento en un mes. Por ejemplo, el elemento de información se leerá, en promedio, 10 veces en un mes, el elemento de metadatos se leerá dos veces y el elemento de relación se leerá cinco veces. En la plantilla de ejemplo, la RRU total de todos los componentes = número de componentes nuevos creados al mes * RRU por componente al mes = 10 millones * 17 RRU = 170 millones de RRU cada mes.

Cada mes, se añadirán elementos nuevos (componentes o productos) y el número total de productos aumentará con el tiempo. Por lo tanto, los requisitos de RRU también aumentarán con el tiempo.

- Durante el primer mes, el consumo de RRU será de 170 millones.
- Durante el segundo mes, el consumo de RRU será 2 * 170 millones, es decir, 340 millones.
- Durante el primer mes, el consumo de RRU será de 3 * 170 millones, es decir, 510 millones.

El siguiente gráfico muestra una previsión mensual del consumo y los costos de la RRU.

Tenga en cuenta que los precios en el gráfico son solo ilustrativos. Para crear previsiones precisas para su caso de uso, consulte la página de precios de AWS y utilice esos precios en la hoja de Excel.

Ejemplos de cálculos de costos de almacenamiento, copia de seguridad y recuperación

El almacenamiento, la copia de seguridad y la restauración de DynamoDB están conectados entre sí. La copia de seguridad está conectada directamente con el almacenamiento y la recuperación está directamente relacionada con el tamaño de la copia de seguridad. A medida que aumente el tamaño

de la tabla, los costos correspondientes de almacenamiento, copia de seguridad y restauración aumentarán proporcionalmente.

Tamaño y costo del almacenamiento

El costo del almacenamiento aumentará con el tiempo en función de la tasa de crecimiento de los datos. Por ejemplo, supongamos que el tamaño medio de un componente o producto en la tabla base GSIs es de 11 KB y que cada mes se añadirán 10 millones de productos nuevos a la tabla de base de datos. En ese caso, el tamaño de la tabla de DynamoDB aumentará (11 KB * 10 millones) /1024/1024 = 105 GB al mes. El primer mes, el tamaño de almacenamiento de la tabla será de 105 GB, el segundo será de 105 + 105 = 210 GBs, y así sucesivamente.

- Durante el primer mes, el costo del almacenamiento será de 105 GB * el precio de almacenamiento por GB para su región de AWS.
- Durante el segundo mes, el costo del almacenamiento será de 210 GB * el precio de almacenamiento por GB para su región.
- Durante el tercer mes, el costo del almacenamiento será de 315 GB * el precio de almacenamiento por GB para su región.

Para conocer el tamaño y el costo del almacenamiento para los próximos tres años, consulte la sección Tamaño del almacenamiento y previsión.

de la copia de seguridad

El costo de las copias de seguridad aumentará con el tiempo en función de la tasa de crecimiento de los datos. Al activar la copia de seguridad continua con point-in-time-recovery (PITR), los cargos por copia de seguridad continua se basan en una media de GB de almacenamiento al mes. En un mes natural, el tamaño medio de las copias de seguridad sería el mismo que el tamaño de almacenamiento de la tabla, aunque el tamaño real podría ser un poco diferente. Como se añadirán productos nuevos cada mes, el tamaño total de almacenamiento y el tamaño de las copias de seguridad aumentarán con el tiempo. Por ejemplo, durante el primer mes, el tamaño medio de las copias de seguridad de 105 GB podría aumentar a 210 GB durante el segundo mes.

- Durante el primer mes, el costo de la copia de seguridad será de 105 GB al mes * el precio de la copia de seguridad continua por GB para su región de AWS.
- Durante el segundo mes, el costo de la copia de seguridad será de 210 GB al mes * el precio de la copia de seguridad continua por GB para su región.

- Durante el tercer mes, el costo de la copia de seguridad será de 315 GB al mes * el precio de la copia de seguridad continua por GB para su región.
- … y así sucesivamente.

El costo de la copia de seguridad se incluye en el gráfico de la sección Previsión del tamaño y el costo del almacenamiento.

Costo de recuperación

Cuando realiza copias de seguridad continuas con la PITR habilitada, los cargos por la operación de recuperación se basan en el tamaño de la restauración. Cada vez que restaure, pagará en función de los gigabytes de datos restaurados. Si el tamaño de la tabla es grande y realiza la restauración varias veces en un mes, será costosa.

Para estimar el costo de la restauración, en este ejemplo se supone que se realiza una recuperación del PITR una vez al mes al final del mes. En el ejemplo, se utiliza el tamaño medio mensual de la copia de seguridad como tamaño de los datos de restauración de ese mes. Durante el primer mes, el tamaño medio de la copia de seguridad es de 105 GB, y para la recuperación al final del mes, el tamaño de los datos de restauración sería de 105 GB. Para el segundo mes, serían 210 GBs, y así sucesivamente.

El costo de recuperación aumentará con el tiempo en función de la tasa de crecimiento de los datos.

- Durante el primer mes, el costo de recuperación será de 105 GB * el precio de recuperación por GB para su región de AWS.
- Durante el segundo mes, el costo de recuperación será de 210 GB * el precio de restauración por GB para su región.
- Durante el tercer mes, el costo de recuperación será de 315 GB * el precio de restauración por GB para su región.

Para obtener más información, consulte la pestaña Almacenamiento, copia de seguridad y recuperación de la plantilla de Excel y el gráfico de la siguiente sección.

Previsión del tamaño y los costos del almacenamiento

En la plantilla, el tamaño de almacenamiento facturable real se calcula restando 25 GB al mes de la capa gratuita de la clase de tabla estándar. En la hoja, obtendrá un gráfico de pronóstico dividido en valores mensuales.

El siguiente gráfico de ejemplo prevé el tamaño de almacenamiento mensual en GB, el costo de almacenamiento facturable, el costo de las copias de seguridad bajo demanda y el costo de recuperación para los próximos 36 meses naturales. Todos los costos están en USD. A partir del gráfico, queda claro que los costos de almacenamiento, copia de seguridad y recuperación aumentan proporcionalmente al aumento del tamaño del almacenamiento.

Tenga en cuenta que los precios en el gráfico son solo ilustrativos. Para crear previsiones precisas para su caso de uso, consulte la página de precios de AWS y utilice esos precios en la hoja de Excel.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Costos de almacenamiento estimados para una tabla de Amazon DynamoDB

Moinul Al-Mamun, Amazon Web Services

Resumen

Amazon DynamoDB es una base de datos transaccional NoSQL que proporciona una latencia de milisegundos de un solo dígito incluso a escala de petabytes. Esta popular oferta sin servidor de ofrece un rendimiento y una escalabilidad AWS consistentes. No es necesario aprovisionar almacenamiento y su única tabla puede crecer hasta petabytes.

DynamoDB supervisa el tamaño de la tabla de forma continua durante todo el mes para determinar los cargos de almacenamiento. AWS a continuación, le cobrará por el tamaño medio del almacenamiento en gigabytes. Cuanto más crezca su tabla con el tiempo, más crecerán sus costos de almacenamiento. Para calcular el coste de almacenamiento, puede utilizar la calculadora de AWS precios, pero debe proporcionar el tamaño aproximado de la tabla, incluidos los índices secundarios globales (GSIs), lo que resulta muy difícil de estimar al principio del proyecto. Además, la calculadora AWS de precios no tiene en cuenta la tasa de crecimiento de los datos.

Este patrón proporciona un mecanismo y una plantilla de Microsoft Excel reutilizable para calcular el tamaño y el costo del almacenamiento de DynamoDB. Considera los requisitos de almacenamiento para la tabla base y los de GSIs forma independiente. Calcula el tamaño del almacenamiento teniendo en cuenta el tamaño de los elementos individuales y la tasa de crecimiento de los datos a lo largo del tiempo.

Para obtener una estimación, inserte dos datos en la plantilla:

- El tamaño del elemento individual en kilobytes de la tabla base y GSIs
- Cuántos objetos o productos nuevos se podrían añadir a la tabla, en promedio, en un mes (por ejemplo, 10 millones)

La plantilla genera un gráfico de previsión de costos y almacenamiento para los próximos tres años, como se muestra en el siguiente ejemplo.

Requisitos previos y limitaciones

Requisitos previos

- Conocimientos básicos de DynamoDB, incluido el almacenamiento y los precios de DynamoDB
- Conocimiento de los datos, el modelo de datos y el tamaño de los elementos en DynamoDB
- Conocimiento de los índices secundarios globales de DynamoDB () GSIs

Limitaciones

- La plantilla proporciona un cálculo aproximado, pero no es adecuada para todas las configuraciones. Para obtener una estimación más precisa, debe medir el tamaño individual de cada elemento de la tabla base y. GSIs
- Este patrón permite estimar únicamente el tamaño y los costos de almacenamiento para los próximos años, sobre la base de hipótesis de crecimiento fijo de los datos.

Tools (Herramientas)

Servicios de AWS

- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.

Otras herramientas

- AWS La calculadora de precios es una herramienta de planificación basada en la web que puede utilizar para crear estimaciones para sus casos de AWS uso.

Epics

Extraiga la información de los artículos de su modelo de datos de DynamoDB

Tarea	Descripción	Habilidades requeridas
Obtener el tamaño del artículo.	1. Determine cuántos tipos diferentes de objetos va a almacenar en su tabla.	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	2. Para calcular el tamaño de cada elemento en kilobytes , añada el tamaño de `Key` y `Value` de cada atributo. 3. Calcule el tamaño del elemento para una tabla base y para cada GSI.	
Obtenga el número de objetos que se han agregado en un mes.	Calcule cuántos component es u objetos se añadirán a la tabla de DynamoDB, de media, en un mes.	Ingeniero de datos

Introduzca la información del artículo y el objeto en la plantilla de Excel

Tarea	Descripción	Habilidades requeridas
Descargue y ajuste la hoja de cálculo de Excel.	1. Descargue la plantilla de Excel del documento adjunto. 2. Ajuste el módulo empresari al y GSIs, en función del diseño de su mesa.	Ingeniero de datos
Introduzca la información en la plantilla de Excel.	1. Actualice la información del elemento en la hoja. 2. Ajuste los números de los objetos: ¿cuánto se puede añadir a la tabla cada mes? 3. Actualice los precios de almacenamiento por GB al mes para su Región de AWS.	Ingeniero de datos

Recursos relacionados

- Precios de la capacidad bajo demanda para Amazon DynamoDB
- AWS Calculadora de precios para DynamoDB

Información adicional

Tenga en cuenta que la plantilla adjunta solo prevé el tamaño y el costo del almacenamiento para la clase de tabla de almacenamiento estándar. En función de la previsión de los costos de almacenamiento y teniendo en cuenta el tamaño individual del artículo y la tasa de crecimiento del producto o del objeto, puede estimar lo siguiente:

- Costo de exportación de datos
- Precio de copias de seguridad y recuperación
- Requisitos de almacenamiento de datos.

Costo del almacenamiento de datos de Amazon DynamoDB

DynamoDB supervisa el tamaño de la tabla de forma continua durante todo el mes para determinar los cargos de almacenamiento. DynamoDB mide el tamaño de los datos facturables al agregar el tamaño de byte sin procesar de los datos y una capacidad de almacenamiento por elemento que depende de las características que haya habilitado. Para obtener más información, consulte la Guía para desarrolladores de DynamoDB.

El precio del almacenamiento de datos depende de la clase de tabla. Los primeros 25 GB almacenados cada mes son gratuitos si utiliza la clase de tabla estándar de DynamoDB. Para obtener más información sobre los costes de almacenamiento de las clases de tablas Estándar y Estándar de Acceso Infrecuente, en distintas categorías Regiones de AWS, consulte Precios de la capacidad bajo demanda.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Calcule el tamaño del motor de Amazon RDS para una base de datos de Oracle mediante informes de AWR

Abhishek Verma y Eduardo Valentim, Amazon Web Services

Resumen

Al migrar una base de datos Oracle a Amazon Relational Database Service (Amazon RDS) o Amazon Aurora, el cálculo de la CPU, la memoria y el I/O disco de la base de datos de destino es un requisito clave. Puede estimar la capacidad requerida de la base de datos de destino analizando los informes del repositorio automático de cargas de trabajo (AWR) de Oracle. Este patrón explica cómo utilizar los informes de AWR para estimar estos valores.

La base de datos Oracle de origen puede estar en las instalaciones o alojada en una instancia de Amazon Elastic Compute Cloud (Amazon EC2), o puede ser una instancia de base de datos de Amazon RDS for Oracle. La base de datos de destino puede ser cualquier base de datos de Amazon RDS o Aurora.

> **Note**
>
> Las estimaciones de capacidad serán más precisas si el motor de base de datos de destino es Oracle. En el caso de otras bases de datos de Amazon RDS, el tamaño del motor puede variar debido a las diferencias en la arquitectura de la base de datos.

Le recomendamos que realice la prueba de rendimiento antes de migrar la base de datos de Oracle.

Requisitos previos y limitaciones

Requisitos previos

- Una licencia de Oracle Database Enterprise Edition y una licencia de Oracle Diagnostics Pack para descargar los informes de AWR.

Versiones de producto

- Todas las ediciones de bases de datos de Oracle para las versiones 11g (versiones 11.2.0.3.v1 y posteriores) y hasta 12.2, 18c y 19c.

- Este patrón no cubre Oracle Engineered Systems ni Oracle Cloud Infrastructure (OCI).

Arquitectura

Pila de tecnología de origen

Uno de los siguientes:

- Una base de datos de Oracle en las instalaciones
- Una base de datos de Oracle en una instancia EC2
- Una instancia de base de datos de Amazon RDS para Oracle

Pila de tecnología de destino

- Cualquier base de datos de Amazon RDS a Amazon Aurora.

Arquitectura de destino

Para obtener información sobre el proceso de migración completo, consulte el patrón Migración de una base de datos de Oracle a Aurora PostgreSQL mediante AWS DMS y AWS SCT.

Automatizar y escalar

Si tiene que migrar varias bases de datos de Oracle y desea utilizar métricas de rendimiento adicionales, puede automatizar el proceso siguiendo los pasos descritos en la entrada del blog Dimensionar correctamente las instancias de Amazon RDS a escala en función de las métricas de rendimiento de Oracle.

Tools (Herramientas)

- El Repositorio automático de cargas de trabajo (AWR) de Oracle es un repositorio integrado en las bases de datos de Oracle. Recopila y almacena periódicamente los datos de actividad y carga de trabajo del sistema, que luego son analizados por el Monitor de diagnóstico automático de bases de datos (ADDM). AWR toma instantáneas de los datos de rendimiento del sistema periódicamente (de forma predeterminada, cada 60 minutos) y almacena la información (de forma predeterminada, hasta 8 días). Puede utilizar las vistas y los informes de AWR para analizar estos datos.

Prácticas recomendadas

- Para calcular las necesidades de recursos de la base de datos de destino, puede utilizar un único informe de AWR, varios informes de AWR o vistas de AWR dinámicas. Le recomendamos que utilice varios informes de AWR durante el período de máxima carga para estimar los recursos necesarios para gestionar esos picos de carga. Además, las vistas dinámicas proporcionan más puntos de datos que lo ayudan a calcular las necesidades de recursos con mayor precisión.
- Debe estimar las IOPS solo para la base de datos que planea migrar, no para otras bases de datos y procesos que utilizan el disco.
- Para calcular cuánto I/O utiliza la base de datos, no utilices la información de la sección Perfil de carga del informe AWR. En su lugar, usa la sección I/O Perfil, si está disponible, o ve a la sección Estadísticas de actividad de la instancia y consulta los valores totales de las operaciones físicas de lectura y escritura.
- Cuando estime el uso de la CPU, le recomendamos que utilice el método de métricas de la base de datos en lugar de las estadísticas del sistema operativo (SO), ya que se basa en la CPU que utilizan únicamente las bases de datos. (Las estadísticas del sistema operativo también incluyen el uso de la CPU por parte de otros procesos). También debería consultar las recomendaciones relacionadas con la CPU en el informe de ADDM para mejorar el rendimiento tras la migración.
- Tenga en cuenta los límites de I/O rendimiento (rendimiento de Amazon Elastic Block Store (Amazon EBS) y rendimiento de red, para el tamaño de instancia específico a la hora de determinar el tipo de instancia correcto.
- Realice la prueba de rendimiento antes de la migración para validar el tamaño del motor.

Epics

Crear un informe de AWR

Tarea	Descripción	Habilidades requeridas
Habilite el informe AWR.	Para activar el informe, siga las instrucciones de la documentación de Oracle.	Administrador de base de datos
Compruebe el periodo de retención.	Para comprobar el periodo de retención del informe AWR, utilice la siguiente consulta.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`SQL> SELECT snap_interval,retention FROM dba_hist_wr_control;`	
Genere la instantánea.	Si el intervalo de instantáneas de AWR no es lo suficientemente detallado como para captar el pico de carga de trabajo, puede generar el informe de AWR manualmente. Para generar la instantánea de AWR manual, utilice la siguiente consulta. `SQL> EXEC dbms_workload_repository.create_snapshot;`	Administrador de base de datos
Compruebe las instantáneas recientes.	Para comprobar las instantáneas de AWR recientes, utilice la siguiente consulta. `SQL> SELECT snap_id, to_char(begin_interval_time,'dd/MON/yy hh24:mi') Begin_Interval, to_char(end_interval_time,'dd/MON/yy hh24:mi') End_Interval FROM dba_hist_snapshot ORDER BY 1;`	Administrador de base de datos

I/O Calcule los requisitos de disco

Tarea	Descripción	Habilidades requeridas
Elija un método.	Las IOPS son la medida estándar de las operacion es de entrada y salida por segundo en un dispositivo de almacenamiento e incluyen las operaciones de lectura y escritura. Si va a migrar una base de datos local a AWS, debe determinar el pico de disco que I/O utiliza la base de datos. Puede utilizar los siguientes métodos para estimar el disco de la base de I/O datos de destino: • Sección de perfil de carga del informe AWR • Sección de estadísticas de actividad de instancia s del informe AWR (utilice esta sección para Oracle Database 12c o versiones posteriores) • Sección de perfiles de E/S del informe AWR (utilice esta sección para las versiones de Oracle Database anteriores a la 12c) • Vistas AWR	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Estos cuatro métodos se describen en los siguientes pasos.	

Tarea	Descripción	Habilidades requeridas
Opción 1: utilice el perfil de carga.	La siguiente tabla muestra un ejemplo de la sección Perfil de carga del informe AWR. **Important** Para obtener información más precisa, le recomendamos que utilice la opción 2 (perfiles de E/S) o la opción 3 (estadísticas de actividad de la instancia) en lugar del perfil de carga. Por segu / Tran ón / Por ejecu / Por llamac Tiem s de base de datos: 26.6 / 0.2 / 0,00 / 0,02 CPU de base de datos: 18,0 / 0.1 / 0,00 / 0.01	Administrador de base de datos

Tarea	Descripción				Habilidades requeridas
	CPU de fond	0.2	0.0	0,00	0,00	
	Tam de Redo (byte	2.45 ,9	17.0			
	Lectu lógic (bloq :	3.37 ,5	23.4			
	Cam en bloqu	21.6	150,5			
	Lectu física bloqu	13.5	94,4			
	Escri física (bloq :	3.46	24,1			
	Leer las solici es de E/ S:	3.58	24,9			
	Solic es	574,	4.0			

Tarea	Descripción	Habilidades requeridas
	de escri IO: Leer E/ S (MB) 106. Escri E/ S (MB) 27,1 0.2 Filas de esca de mens a insta ea: 0.0 0.0 Mens a insta ea de lectu lógic de sesió User calls 1.24 8.7	

Tarea	Descripción	Habilidades requeridas
	Anál (SQL 4.62 32,2 Anál duro (SQL 8.9 0.1 Área de traba de SQL (MB) 824,9 5.7 Inicio de sesió 1.7 0.0 Ejecu (SQL 136.6 950,4 Reve : 22.9 0.2 Tran ones 143.8 En función de esta informaci ón, puede calcular IOPs y procesar de la siguiente manera: IOPS = solicitudes de lectura: + I/O Solicitudes de escritura = I/O 3.586,8 + 574,7 = 4134,5	

Tarea	Descripción	Habilidades requeridas
	Rendimiento = lectura física (bloques) + escritura física (bloques) = 13 575,1 + 3467,3 = 17 042,4 Como el tamaño del bloque en Oracle es de 8 KB, puede calcular el rendimiento total de la siguiente manera: El rendimiento total en MB es 17 042,4 * 8 * 1024 / 1024 / 1024 = 133,2 MB **Warning** No utilice el perfil de carga para estimar el tamaño de la instancia . No es tan preciso como las estadísti cas o los perfiles de actividad de las instancias. I/O	

Tarea	Descripción	Habilidades requeridas
Opción 2: utilizar estadísticas de actividad de instancia.	Si utiliza una versión de la base de datos de Oracle anterior a la 12c, puede utilizar la sección de estadísticas de actividad de las instancias del informe AWR para estimar las IOPS y el rendimiento. En la tabla siguiente se muestra un ejemplo de esta sección. Estadística / Total / Por segun / por Trans lectura física total de solicitudes de E/S / 2.547..217 / 3.610, / 25,11 bytes totales de lectura física / 80.776.124.928 / 114,48 26,26 / 796.149 8 escritura física, total de solicitudes / 534.19 08 / 757,1 / 5.27	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de E/S bytes totales de escritu física 25.517 8.849. 36.165 1,84 251.508 8 En función de esta informaci ón, puede calcular el total de IOPS y el rendimiento de la siguiente manera: TIOPS totales = 3610,28 + 757,11 = 4367 Mbps totales = 114 482 426,26 + 36 165 631,84 = 150 648 058,1 / 1024 / 1024 = 143 Mbps	

Tarea	Descripción	Habilidades requeridas
Opción 3: utilizar perfiles. I/O	En Oracle Database 12c, el informe AWR incluye una sección de I/O perfiles que presenta toda la información en una sola tabla y proporcio na datos más precisos sobre el rendimiento de la base de datos. En la tabla siguiente se muestra un ejemplo de esta sección. Lectur + escritu por segun Lectur por segun Escritur s por segundo Solicit es por segun 4.367, 3.610, 757,1 Solicit es de bases de datos: 4.161, 3.586, 574,7 Solicit es optimi as: 0.0 0.0 0.0	Administrador de base de datos

Tarea	Descripción				Habilidades requeridas
	Rehac solicitu es:	179,3	2.8	176,6	
	Total (MB):	143.7	109,2	34,5	
	Base de datos (MB):	133,1	106.1	27,1	
	Total optimi: o (MB):	0.0	0.0	0.0	
	Rehac (MB):	7.6	2.7	4.9	
	Base de datos (bloqu :	17.042	13.575	3.467,3	
	A través de Buffer Cache (bloqu :	5.898,	5.360,	537,6	

Tarea	Descripción	Habilidades requeridas
	Direct 11.143 8.214, 2.929,7 (bloqu : En esta tabla se proporcio nan los siguientes valores de rendimiento e IOPS totales: Rendimiento = 143 MBPS (desde la quinta fila, denominada Total, segunda columna) IOPS = 4367,4 (desde la primera fila, denominada Solicitudes totales, segunda columna)	

Tarea	Descripción	Habilidades requeridas
Opción 4: utilizar vistas AWR.	Puede ver la misma información de IOPS y rendimiento mediante las vistas de AWR. Para obtener esta información, utilice la siguiente consulta: `break on report compute sum of Value on report select METRIC_NAME,avg(AVERAGE) as "Value" from dba_hist_sysmetric_summary where METRIC_NAME in ('Physical Read Total IO Requests Per Sec','Physical Write Total IO Requests Per Sec') group by metric_name;`	Administrador de base de datos

Calcule los requisitos de CPU

Tarea	Descripción	Habilidades requeridas
Elija un método.	Puede estimar la CPU necesaria para la base de datos de destino de tres maneras: • Mediante el uso de los núcleos disponibles reales del procesador • Mediante el uso de los núcleos utilizados según	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	las estadísticas del sistema operativo • Mediante el uso de los núcleos utilizados según las estadísticas Si está analizando los núcleos utilizados, le recomendamos que utilice el método de métricas de la base de datos en lugar de las estadísticas del sistema operativo, ya que se basa en la CPU que utilizan únicamente las bases de datos que planea migrar. (Las estadísticas del sistema operativo también incluyen el uso de la CPU por parte de otros procesos). También debería consultar las recomendaciones relacionadas con la CPU en el informe de ADDM para mejorar el rendimiento tras la migración. También puede estimar los requisitos en función de la generación de CPU. Si utiliza distintas generaciones de CPU, puede estimar la CPU necesaria para la base de datos de destino siguiendo las instrucciones del documento técnico Desmitificando el número de v para lograr un	

Tarea	Descripción	Habilidades requeridas
	rendimiento óptimo de la carga de trabajo. CPUs	

Tarea	Descripción	Habilidades requeridas

Opción 1: calcule los requisitos en función de los núcleos disponibles.	En informes AWR:
	• CPUs consulte la lógica y la virtual. CPUs
	• Los núcleos son el número de procesadores de un chipset de CPU físico.
	• Un socket es un dispositivo físico que conecta un chip a una placa. Los procesadores multinúcleo tienen sockets con varios núcleos de CPU.
	
	Puede estimar los núcleos disponibles de dos maneras:
	• Mediante comandos utilizando el sistema operativo
	• Mediante el informe AWR
	
	Para estimar los núcleos disponibles mediante comandos del sistema operativo
	
	Utilice el siguiente comando para contar los núcleos del procesador.
	
	`$ cat /proc/cpuinfo | grep "cpu cores"|uniq`
	`cpu cores : 4`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`cat /proc/cpuinfo	egrep "core id|physical id"	tr -d "\n"	sed s/physical/\\nphysical/g	grep -v ^$	sort	uniq	wc -l`  Utilice el siguiente comando para contar los sockets del procesador.  `grep "physical id" /proc/cpuinfo	sort -u` `physical id : 0` `physical id : 1` **Note** No recomendamos utilizar comandos del sistema operativo , como nmon y sar, para extraer el uso de la CPU. Esto se debe a que esos cálculos incluyen el uso de la CPU por parte de otros procesos y es posible que no reflejen la CPU real que utiliza la base de datos. Para estimar los núcleos disponibles mediante el informe AWR	

Tarea	Descripción	Habilidades requeridas
	También puede deducir el uso de la CPU de la primera sección del informe de AWR. A continuación se muestra un extracto del informe. N DB Inst Inst Hor Rele RA d Id num de b inici d d X <DE XX) 1 05- 12.1 NO Sep 0 23:(Hos Plat CPU Núc Soc Mem Nar a (GB) <ho Linu 80 80 2 441,7 e> x86 64- bit En este ejemplo, el CPUs recuento es 80, lo que indica que son lógicos (virtuales). CPUs También puede ver que esta configuración tiene dos sockets, un procesador físico en cada socket (para un total de dos procesadores físicos) y 40 núcleos para cada socket o procesador físico.	

<table>
<tr><th>Tarea</th><th>Descripción</th><th>Habilidades requeridas</th></tr>
<tr><td>Opción 2: Calcule el uso de la CPU mediante las estadísticas del sistema operativo.</td><td>Puede comprobar las estadísticas de uso de la CPU del sistema operativo directamente en el sistema operativo (mediante sar u otra utilidad del sistema operativo host) o revisando los valores de IDLE/(IDLE+BUSY) de la sección de estadísticas del sistema operativo del informe AWR. Puede ver los segundos de CPU consumidos directamente desde v$osstat. Los informes AWR y Statspack también muestran estos datos en la sección de estadísticas del sistema operativo.

Si hay varias bases de datos en el mismo cuadro, todas tienen los mismos valores de v$osstat para BUSY_TIME.

<table><tr><th>Estadística</th><th>Valor</th><th>Valor final</th></tr><tr><td>FREE_MEMORY_BYT</td><td>6.810.67.248</td><td>12.280.799.232</td></tr><tr><td>INACTIVE_MEMORY_BYTES</td><td>175.627.33.632</td><td>160.380,653,568</td></tr><tr><td>SWAP_FREE_BYTES</td><td>17.145.64.336</td><td>17.145.872.384</td></tr></table></td><td>Administrador de base de datos</td></tr>
</table>

Tarea	Descripción		Habilidades requeridas
	BUSY_T	1.305.56 .937	
	IDLE_TI	4.312.71 .839	
	IOWAIT_ ME	53.417.1 4	
	NICE_TI	29.815	
	SYS_TIM	148.567. 70	
	USER_T	1.146.91 .783	
	LOAD	25	29
	VM_IN_E ES	593.920	
	VM_OUT TES	327.680	
	PHYSIC/ MEMOR TES	474.362. 17.152	
	NUM_CF	80	
	NUM_CF ORES	80	
	NUM_CF OCKETS	2	

Tarea	Descripción	Habilidades requeridas
	GLOBAL_SEND_SOCKET_BUFFER_MAX 4.194.304 GLOBAL_RECEIVE_SOCKET_BUFFER_MAX 2.097.152 TCP_RECEIVE_SIZE_DEFAULT 87.380 TCP_RECEIVE_SIZE_MAX 6.291.456 TCP_RECEIVE_SIZE_MIN 4.096 TCP_SEND_SIZE_DEFAULT 16.384 TCP_SEND_SIZE_MAX 4.194.304 TCP_SEND_SIZE_MIN 4.096 Si no hay otros consumidores importantes de CPU en el sistema, utilice la siguiente fórmula para calcular el porcentaje de uso de la CPU:	

Tarea	Descripción	Habilidades requeridas
	Utilización = tiempo de actividad / tiempo total Tiempo de actividad = requisitos = v$osstat.BUSY_TIME C = Tiempo total (actividad + inactivo) C = capacidad = v$ostat.BUSY_TIME + v$ostat.IDLE_TIME Utilización = BUSY_TIME / (BUSY_TIME + IDLE_TIME) = -1 305 569 937 / (1 305 569 937 + 4 312 718 839) = 23 % utilizado	

Tarea	Descripción	Habilidades requeridas
Opción 3: calcule el uso de la CPU mediante métricas de bases de datos.	Si hay varias bases de datos en ejecución en el sistema, puede utilizar las métricas de la base de datos que aparecen al principio del informe. Snap Id / Snap Time / Sesi / Curso sesión Inicia Snap: 1846 / 28-Sep-09:0(/ 1226 / 35,8 Final Snap: 1854 / 06-Oct-2 13:0(/ 1876 / 41,1 Tran ido: / 11 759,((minu Tiem de base de datos: / 312 625,4 (minu Para obtener las métricas de uso de la CPU, utilice esta fórmula: Uso de la CPU de la base de datos (% de la potencia de la CPU disponible) = tiempo	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de CPU / NUM_CPUS / tiempo transcurrido donde el uso de la CPU se describe mediante el tiempo de CPU y representa el tiempo dedicado a la CPU, no el tiempo de espera a la CPU. Este cálculo da como resultado: = 312 625,40 / 11 759,64/80 = Se está utilizando el 33 % de la CPU Número de núcleos (33 %) * 80 = 26,4 núcleos Núcleos totales = 26,4 * (120 %) = 31,68 núcleos Puede usar el mayor de estos dos valores para calcular la utilización de la CPU de la instancia de base de datos Amazon RDS o Aurora. **Note** En IBM AIX, la utilización calculada no coincide con los valores del sistema operativo o de la base de datos. Estos valores coinciden	

Tarea	Descripción	Habilidades requeridas
	en otros sistemas operativos.	

Calcule los requisitos de memoria

Tarea	Descripción	Habilidades requeridas
Calcule los requisitos de memoria mediante estadísticas de memoria.	Puede usar el informe AWR para calcular la memoria de la base de datos de origen y compararla con la base de datos de destino. También debe comprobar el rendimiento de la base de datos existente y reducir los requisitos de memoria para ahorrar costos o aumentar los requisitos para mejorar el rendimiento. Esto requiere un análisis detallado del tiempo de respuesta del AWR y del acuerdo de nivel de servicio (SLA) de la aplicación. Utilice la suma del uso del área global del sistema (SGA) y del área global del programa (PGA) de Oracle como uso de memoria estimado para Oracle. Añada un 20 por ciento adicional para que el sistema operativo determine un requisito de tamaño de memoria objetivo. En el caso de Oracle RAC, utilice la suma	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de la utilización de memoria estimada en todos los nodos RAC y reduzca la memoria total, ya que se almacena en bloques comunes. 1. Compruebe las métricas en la tabla de porcentajes de eficiencia de las instancias. La tabla utiliza los siguiente s términos: • El Porcentaje de aciertos en el búfer es el porcentaj e de veces que se ha encontrado un bloque concreto en la memoria caché del búfer en lugar de realizar una E/S física. Para mejorar el rendimien to, procure alcanzar el 100 por ciento. • El Porcentaje de espera de búfer debe estar cerca del 100 por ciento. • El porcentaje de aciertos de bloqueo debe estar cerca del 100 por ciento. • El porcentaje de CPU que no se analiza es el porcentaje de tiempo de CPU que se dedica a actividades no relaciona das con el análisis. Este	

Tarea	Descripción	Habilidades requeridas
	valor debe estar cerca del 100 por ciento. Porcentaje de eficiencia de las instancias (objetivo: 100 %) % de esper de búfer: 99,99 NoWa % de rehac 100,00 % de aciert del búfer: 99,84 % de clasifi ción en memo 100,00 % de aciert de biblio as: 748,7 % de anális suave 99,81 % de ejecu para analiz 96,61 % de aciert de cierre 100,00 Analiz CPU para 72.73 % de CPU 99,21	

Tarea	Descripción	Habilidades requeridas
	analiz no analiz % e: transc ido: % 0,00 de aciert de caché flash: En este ejemplo, todas las métricas son correctas, por lo que puede utilizar el SGA y el PGA para la base de datos existente como requisito de planificación de la capacidad. 2. Compruebe la sección de estadísticas de la memoria y calcule el SGA/PGA. Inicio Final Memoria 452.387 452.387,3 del host (MB): Uso 220 220 de 544,0 544,0 SGA (MB):	

Tarea	Descripción	Habilidades requeridas
	Uso de PGA (MB): 36.874,9 45.270,0 Memoria total de la instancia en uso = SGA + PGA = 220 GB + 45 GB = 265 GB Añada un 20 por ciento de búfer: Memoria total de la instancia = 1,2 * 265 GB = 318 GB Dado que SGA y PGA representan el 70 por ciento de la memoria del host, el requisito total de memoria es: Memoria total del host = 318/0,7 = 464 GB **Note** Al migrar a Amazon RDS para Oracle, el PGA y el SGA se calculan previamente en función de una fórmula predefinida. Asegúrese de que los valores precalculados	

Tarea	Descripción	Habilidades requeridas
	se acerquen a sus estimaciones.	

Determine el tipo de instancia de base de datos de la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Determine el tipo de instancia de base de datos en función de las estimaciones de E/S, CPU y memoria del disco.	Según las estimaciones de los pasos anteriores, la capacidad de la base de datos Amazon RDS o Aurora de destino debería ser: • 68 núcleos de CPU • 143 MBPS de rendimiento • 4367 IOPS para E/S de disco • 464 GB de memoria En la base de datos Amazon RDS o Aurora de destino, puede asignar estos valores al tipo de instancia db.r5.16x large, que tiene una capacidad de 32 núcleos, 512 GB de RAM y 13 600 Mbps de rendimiento. Para obtener más información, consulte la publicación del blog de AWS en el Tamaño adecuado de instancias de Amazon RDS a escala en función de las	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	métricas de rendimiento de Oracle.	

Recursos relacionados

- Clase de instancia de base de datos Aurora (documentación de Amazon Aurora)
- Almacenamiento de instancias de base de datos de Amazon RDS (documentación de Amazon RDS)
- Herramienta AWS Miner (GitHub repositorio)

Exporte tablas de Amazon RDS for SQL Server a un bucket de S3 mediante AWS DMS

Subhani Shaik, Amazon Web Services

Resumen

Amazon Relational Database Service (Amazon RDS) para SQL Server no admite la carga de datos en otros servidores vinculados a motores de bases de datos (DB) en la nube de Amazon Web Services AWS(). En su lugar, puede utilizar AWS Database Migration Service (AWS DMS) para exportar tablas de Amazon RDS for SQL Server a un bucket de Amazon Simple Storage Service (Amazon S3), donde los datos estén disponibles para otros motores de bases de datos.

AWS DMS le ayuda a migrar bases de datos de forma AWS rápida y segura. La base de datos de origen permanece en pleno funcionamiento durante la migración, lo que minimiza el tiempo de inactividad de las aplicaciones que dependen de la base de datos. AWS DMS puede migrar sus datos hacia y desde las bases de datos comerciales y de código abierto más utilizadas.

Este patrón se utiliza AWS Secrets Manager al configurar los puntos AWS DMS finales. Secrets Manager le ayuda a proteger los secretos necesarios para acceder a sus aplicaciones, servicios y recursos de TI. Puede utilizar el servicio para rotar, administrar y recuperar credenciales de bases de datos, claves de API y otros secretos durante todo su ciclo de vida. Los usuarios y las aplicaciones recuperan los secretos con una llamada a Secrets Manager, lo que reduce la necesidad de codificar información confidencial. Secrets Manager ofrece la rotación de secretos con una integración integrada para Amazon RDS, Amazon Redshift y Amazon DocumentDB (con compatibilidad con MongoDB). Además, el servicio se puede extender a otros tipos de secretos, incluidas las claves de API y los tokens de OAuth. Con Secrets Manager, puede controlar el acceso a los secretos mediante permisos detallados y auditar la rotación de secretos de forma centralizada para los recursos en la AWS nube, los servicios de terceros y las instalaciones.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Un bucket de Amazon S3
- Una nube privada virtual (VPC)
- Una subred de base de datos

- Amazon RDS para SQL Server
- Un rol AWS Identity and Access Management (IAM) con acceso (lista, obtención y colocación de objetos) al bucket de S3 en nombre de la instancia de Amazon RDS
- Secrets Manager para almacenar las credenciales de la instancia de Amazon RDS

Arquitectura

Pila de tecnología

- Amazon RDS para SQL Server
- AWS DMS
- Amazon S3
- AWS Secrets Manager

Arquitectura de destino

El siguiente diagrama muestra la arquitectura para exportar datos de la instancia de Amazon RDS al bucket de Amazon S3 con la ayuda de AWS DMS.

1. La tarea de AWS DMS migración que se conecta a la instancia de Amazon RDS de origen a través del punto de enlace de origen
2. Copiar datos de la instancia de Amazon RDS de origen
3. La tarea de AWS DMS migración que se conecta al bucket de Amazon S3 de destino a través del punto final de destino
4. Exportación de datos copiados al bucket de Amazon S3 en formato de valores separados por comas (CSV)

Tools (Herramientas)

Servicios de AWS

- AWS Database Migration Service (AWS DMS) le ayuda a migrar los almacenes de datos a la AWS nube o entre combinaciones de configuraciones locales y en la nube.
- AWS Identity and Access Management (IAM) le ayuda a gestionar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.

- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, operar y escalar una base de datos relacional en la nube. AWS
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Secrets Manager lo ayuda a reemplazar las credenciales codificadas en su código, incluidas contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.

Otras herramientas

- Microsoft SQL Server Management Studio (SSMS) es una herramienta para administrar SQL Server, que incluye el acceso, la configuración y la administración de los componentes de SQL Server.

Prácticas recomendadas

- Realice una prueba de concepto con un subconjunto de tablas antes de la migración completa para comparar el rendimiento e identificar los problemas.
- Evite ejecutar AWS DMS tareas durante las horas de mayor actividad de la base de datos para reducir la carga en la instancia de Amazon RDS de origen.
- Siga las prácticas recomendadas para AWS DMS.
- Siga las prácticas recomendadas de seguridad de Amazon S3.

Epics

Configuración de la instancia de Amazon RDS para SQL Server

Tarea	Descripción	Habilidades requeridas
Cree la instancia de Amazon RDS para SQL Server.	1. Abra Consola de administración de AWS, elija RDS y utilice la opción de creación estándar para crear una instancia de Amazon RDS con la edición requerida,	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	como SQL Server Express Edition, SQL Server Standard Edition o SQL Server Enterprise Edition. Para la versión, elija 2016 o posterior. 2. En Plantillas, elija. Dev/Test	
Configure las credenciales para la instancia.	1. Escriba el nombre de la instancia. 2. Proporcione un nombre de usuario y una contraseñ a para la instancia de Amazon RDS.	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
Configure la clase de instancia , el almacenamiento, el escalado automático y la disponibilidad.	1. Seleccione la clase de instancia de base de datos de la lista: clases Estándar, Optimizada para memoria y Ampliable. Elija el tipo de instancia de base de datos que asigne la capacidad computacional, de red y de memoria necesaria para las cargas de trabajo planifica das para esta instancia de base de datos. Para obtener más información, consulte la Documentación de AWS. 2. Seleccione el tipo de almacenamiento de la lista: SSD de uso general, SSD con IOPS aprovisionadas o magnético. Asigne el tamaño de almacenamiento predeterminado según sea necesario. 3. Seleccione Habilitar el escalado automático del almacenamiento para aumentar el almacenam iento de Amazon RDS en función de su planificación de capacidad. 4. Un Multi-AZ despliegu e con una instancia de replicación es compatible con. AWS DMS En caso	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	de que se produzca una interrupción en la zona de disponibilidad, el hardware interno o la red AWS DMS crearán una instancia en espera y proporcionarán alta disponibilidad (HA) mediante una conmutaci ón por error automática a las réplicas en espera. En función del tamaño de la importación, seleccione la opción adecuada.	
Especifique la VPC, el grupo de subredes, el acceso público y el grupo de seguridad.	Seleccione la VPC, los grupos de subredes de base de datos y el grupo de seguridad de VPC según sea necesario para crear la instancia de Amazon RDS. Siga las prácticas recomendadas, por ejemplo: • No habilite el acceso público a la instancia de Amazon RDS. • No utilice el CIDR 0.0.0. 0/0 en los grupos de seguridad. • Utilice únicamente la dirección IP y los detalles del puerto necesarios para acceder a la instancia de Amazon RDS.	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
Configure la supervisión, el respaldo y el mantenimiento.	1. Especifique las opciones de copia de seguridad que desea. De forma predeterminada, las copias de seguridad están habilitadas con un periodo de retención de 7 días. 2. Elija la configuración adecuada de la ventana de actualización automática de la versión secundaria y de mantenimiento para aplicar las modificaciones o el mantenimiento pendientes a la base de datos por parte de Amazon RDS. 3. Seleccione Crear base de datos.	DBA, ingeniero DevOps

Configure la base de datos y los datos de ejemplo

Tarea	Descripción	Habilidades requeridas
Cree una tabla y cargue los datos del ejemplo.	En la nueva base de datos, cree una tabla. Utilice el código de ejemplo de la sección Información adicional para cargar los datos en la tabla.	DBA, ingeniero DevOps

Configuración de credenciales

Tarea	Descripción	Habilidades requeridas
Cree el secreto.	1. En la consola, seleccion a Secrets Manager y, a continuación, selecciona Guardar un secreto nuevo. 2. Introduzca un nombre de usuario y una contraseña para la base de datos de Amazon RDS para SQL Server. Este secreto se usará para el punto final AWS DMS de origen.	DBA, ingeniero DevOps

Configure el acceso entre la base de datos y el bucket de Amazon S3

Tarea	Descripción	Habilidades requeridas
Para crear un rol de IAM para acceder a Amazon RDS.	1. En la consola, elija IAM y cree un rol de IAM que dé read/write acceso a un bucket de S3 a Amazon RDS. 2. En Característica, seleccion e Integración con S3.	DBA, ingeniero DevOps

Cree el bucket de Amazon S3

Tarea	Descripción	Habilidades requeridas
Cree el bucket de Amazon S3.	Para guardar los datos de Amazon RDS para SQL Server, en la consola, elija S3 y, a continuación, elija Crear bucket. Asegúrese de que el bucket de Amazon S3 no esté disponible públicamente.	DBA, ingeniero DevOps

Configure el acceso entre AWS DMS y el bucket de Amazon S3

Tarea	Descripción	Habilidades requeridas
Cree un rol de IAM para acceder AWS DMS a Amazon S3.	Cree un rol de IAM que permita AWS DMS enumerar, obtener y colocar objetos del bucket de Amazon S3.	DBA, ingeniero DevOps

Configuración AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree el punto final AWS DMS de origen.	1. En la consola, elija Database Migration Service y elija Puntos de conexión. Cree el Punto de conexión de origen y active la casilla de verificación Seleccionar instancia de base de datos de RDS.	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	2. Para el motor Origen, seleccione Microsoft SQL Server. 3. En Acceso a la base de datos del punto final AWS Secrets Manager, elija e introduzca el secreto y el rol de IAM que creó anteriormente, así como el nombre de la base de datos. 4. Pruebe el punto de conexión de origen.	
Cree el punto final AWS DMS de destino.	Cree el Punto de conexión de destino y seleccione Amazon S3 como Motor de destino. Proporcione el nombre del bucket de Amazon S3 y el nombre de la carpeta para el rol de IAM que creó anteriormente.	DBA, ingeniero DevOps
Cree la instancia de AWS DMS replicación.	En la misma VPC, subred y grupo de seguridad, cree la AWS DMS instancia de replicación. Para obtener más información sobre cómo elegir una clase de instancia, consulta la AWS documentación.	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
Cree la tarea de AWS DMS migración.	Para exportar los datos de Amazon RDS for SQL Server al bucket de Amazon S3, cree una tarea de migración de base de datos. En tipo de migración, seleccione migrar datos existentes. Seleccion e los AWS DMS puntos de enlace y la instancia de replicación que creó.	DBA, ingeniero DevOps

Exporte los datos al bucket de Amazon S3

Tarea	Descripción	Habilidades requeridas
Ejecute la tarea de migración de bases de datos de.	Para exportar los datos de la tabla de SQL Server, inicie la tarea de migración de la base de datos. La tarea exportará los datos de Amazon RDS for SQL Server al bucket de Amazon S3 en formato CSV.	DBA, ingeniero DevOps

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Elimine los recursos.	Para evitar incurrir en costos adicionales, utilice la consola para eliminar los recursos en el siguiente orden: 1. Tarea de migración 2. Instancia de replicación	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	3. Puntos de conexión 4. Bucket de Amazon S3 5. Instancia de base de datos	

Resolución de problemas

Problema	Solución
Solución de problemas con Microsoft SQL Server	Para obtener más información sobre cómo resolver problemas con Microsoft SQL Server durante el uso AWS DMS, consulte Solución de problemas con Microsoft SQL Server.
Solución de problemas de tareas de migración	Para obtener más información sobre cómo resolver los problemas de migración durante el uso AWS DMS, consulte Solución de problemas de migración en AWS Database Migration Service.

Recursos relacionados

- AWS DMS
- Amazon S3
- Amazon RDS para SQL Server
- Integración de Amazon S3
- Uso de una base de datos de Microsoft SQL Server como fuente para AWS DMS
- Uso de Amazon S3 como objetivo para AWS DMS

Información adicional

Para crear la base de datos y la tabla y cargar los datos de ejemplo, utilice el siguiente código:

```
--Step1: Database creation in RDS SQL Server
```

```
CREATE DATABASE [Test_DB]
 ON  PRIMARY
( NAME = N'Test_DB', FILENAME = N'D:\rdsdbdata\DATA\Test_DB.mdf' , SIZE = 5120KB ,
 FILEGROWTH = 10%)
 LOG ON
( NAME = N'Test_DB_log', FILENAME = N'D:\rdsdbdata\DATA\Test_DB_log.ldf' , SIZE =
 1024KB , FILEGROWTH = 10%)
GO

--Step2: Create Table
USE Test_DB
GO
Create Table Test_Table(ID int, Company Varchar(30), Location Varchar(20))

--Step3: Load sample data.
USE Test_DB
GO
Insert into Test_Table values(1,'AnyCompany','India')
Insert into Test_Table values(2,'AnyCompany','USA')
Insert into Test_Table values(3,'AnyCompany','UK')
Insert into Test_Table values(4,'AnyCompany','Hyderabad')
Insert into Test_Table values(5,'AnyCompany','Banglore')
```

Gestionar bloques anónimos en instrucciones SQL dinámicas en Aurora PostgreSQL

anuradha chintha, Amazon Web Services

Resumen

Nota: Amazon Cloud Directory ya no está abierto a nuevos clientes. Para obtener alternativas a Cloud Directory, explore Amazon DynamoDB y Amazon Neptune. Si necesita ayuda para elegir la alternativa adecuada para su caso de uso o si tiene alguna otra pregunta, póngase en contacto con nosotros. AWS Support

Este patrón le muestra cómo evitar el error que se produce al gestionar bloques anónimos en instrucciones SQL dinámicas. Recibirá un mensaje de error cuando use la herramienta de conversión de esquemas de AWS para convertir una base de datos de Oracle en una base de datos Aurora compatible con PostgreSQL. Para evitar el error, debe conocer el valor de una variable de enlace OUT, pero no podrá conocer el valor de una variable de enlace OUT hasta que ejecute la instrucción SQL. Este error se debe a que la herramienta de conversión de esquemas de AWS (AWS SCT) no entiende la lógica de la instrucción SQL dinámica. AWS SCT no puede convertir la sentencia SQL dinámica en PL/SQL código (es decir, funciones, procedimientos y paquetes).

Requisitos previos y limitaciones

Requisitos previos

- Cuenta de AWS activa
- Instancia de base de datos (DB) de Aurora PostgreSQL
- Amazon Relational Database Service (Amazon RDS) para la instancia de base de datos de Oracle
- Terminal interactiva de PostgreSQL (psql)
- SQL *Plus
- Esquema de `AWS_ORACLE_EXT` (parte del paquete de extensión AWS SCT) en la base de datos de destino
- Versión más reciente de la herramienta de conversión de esquemas de AWS (AWS SCT) y los controladores necesarios

Arquitectura

Pila de tecnología de origen

- Oracle Database 10g en las instalaciones y versiones posteriores

Pila de tecnología de destino

- PostgreSQL de Amazon Aurora
- Amazon RDS para PostgreSQL
- Herramienta de conversión de esquemas de AWS (AWS SCT)

Arquitectura de migración

El siguiente diagrama muestra cómo usar las variables de enlace 0UT de AWS SCT y Oracle para escanear el código de la aplicación en busca de instrucciones SQL integradas y convertir el código a un formato compatible que pueda usar una base de datos de Aurora.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Genere un informe de AWS SCT para la base de datos de origen usando Aurora PostgreSQL como base de datos de destino.
2. Identifique el bloque anónimo en el bloque de código SQL dinámico (por el que AWS SCT generó el error).
3. Convierta el bloque de código manualmente e impleméntelo en una base de datos de destino.

Tools (Herramientas)

Servicios de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.
- Amazon Relational Database Service (Amazon RDS) para Oracle le ayuda a configurar, utilizar y escalar una base de datos relacional de Oracle en la nube de AWS.

- La Herramienta de conversión de esquemas de AWS (AWS SCT) le ayuda a hacer previsibles las migraciones de bases de datos heterogéneas convirtiendo automáticamente el esquema de la base de datos de origen y la mayoría de los objetos de código de la base de datos a un formato compatible con la base de datos de destino.

Otras herramientas

- pgAdmin le permite conectarse e interactuar con su servidor de base de datos.
- Oracle SQL Developer es un entorno de desarrollo integrado que puede usar para desarrollar y gestionar bases de datos en Oracle Database. Puede usar SQL *Plus u Oracle SQL Developer para este patrón.

Epics

Configurar la base de datos de orgien de Oracle

Tarea	Descripción	Habilidades requeridas
Cree una instancia de Oracle en Amazon RDS o Amazon EC2.	Para crear una instancia de base de datos de Oracle en Amazon RDS, consulte Crear una instancia de base de datos de Oracle y conectarse a una base de datos en una instancia de base de datos en Oracle en la documentación de Amazon RDS. Para crear una instancia de base de datos de Oracle en Amazon Elastic Compute Cloud (Amazon EC2), consulte Amazon EC2 for Oracle en la documentación de AWS Prescriptive Guidance.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree un esquema de base de datos y objetos para la migración.	Puede usar Amazon Cloud Directory para crear un esquema de base de datos. Para más información, consulte Crear un esquema en la documentación de Cloud Directory.	Administrador de base de datos
Configure grupos de seguridad entrantes y salientes.	Para crear y configurar grupos de seguridad, consulte Controlar el acceso con grupos de seguridad en la documentación de Amazon RDS.	Administrador de base de datos
Confirme que la base de datos se está ejecutando.	Para comprobar el estado de su base de datos, consulte Visualizar los eventos de Amazon RDS en la documentación de Amazon RDS.	Administrador de base de datos

Configure la base de datos Aurora PostgreSQL de destino

Tarea	Descripción	Habilidades requeridas
Cree una instancia de Aurora PostgreSQL en Amazon RDS.	Para crear una instancia de Aurora PostgreSQL, consulte Crear un clúster de base de datos y conectarse a una base de datos en un clúster de base de datos de Aurora PostgreSQL en la documentación de Amazon RDS.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Configure un grupo de seguridad entrante y saliente.	Para crear y configurar grupos de seguridad, consulte Proporcionar acceso al clúster de base de datos en la VPC creando un grupo de seguridad en la documentación de Aurora.	Administrador de base de datos
Confirme que la base de datos Aurora PostgreSQL se está ejecutando.	Para comprobar el estado de su base de datos, consulte Visualizar los eventos de Amazon RDS en la documentación de Aurora.	Administrador de base de datos

Configure AWS SCT

Tarea	Descripción	Habilidades requeridas
Conectar AWS SCT a la base de datos de origen.	Para conectar AWS SCT a su base de datos de origen, consulte Conectar a PostgreSQL como fuente en la documentación de AWS SCT.	Administrador de base de datos
Conectar AWS SCT a la base de datos de destino.	Para conectar AWS SCT a su base de datos de destino, consulte ¿Qué es la la Herramienta de conversión de esquemas de AWS (AWS SCT)? en la Guía del usuario de la la Herramienta de conversión de esquemas de AWS (AWS SCT).	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Convierta el esquema de la base de datos en AWS SCT y guarde el código convertid o automáticamente como archivo SQL.	Para guardar los archivos convertidos de AWS SCT, consulte Guardar y aplicar el esquema convertido en AWS SCT la Guía del usuario de la la Herramienta de conversión de esquemas de AWS (AWS SCT).	Administrador de base de datos

Migración del código

Tarea	Descripción	Habilidades requeridas
Obtenga el archivo SQL para la conversión manual.	En el archivo convertido de AWS SCT, extraiga el archivo SQL que requiere la conversió n manual.	Administrador de base de datos
Actualice el script.	Actualice manualmente el archivo SQL.	Administrador de base de datos

Recursos relacionados

- Amazon RDS
- Características de Amazon Aurora

Información adicional

En el siguiente ejemplo de código se muestra cómo configurar la base de datos de origen de Oracle:

```
CREATE or replace PROCEDURE calc_stats_new1 (
  a NUMBER,
  b NUMBER,
  result out NUMBER)
```

```
IS
BEGIN
result:=a+b;
END;
/
```

```
set serveroutput on ;

DECLARE
  a NUMBER := 4;
  b NUMBER := 7;
  plsql_block VARCHAR2(100);
  output number;
BEGIN
  plsql_block := 'BEGIN calc_stats_new1(:a, :b,:output); END;';
  EXECUTE IMMEDIATE plsql_block USING a, b,out output;
  DBMS_OUTPUT.PUT_LINE('output:'||output);

END;
```

En el siguiente ejemplo de código se muestra cómo configurar la base de datos de Aurora PostgreSQL de destino:

```
 w integer,
 x integer)
RETURNS integer
AS
$BODY$
DECLARE
begin
return w + x ;
end;
$BODY$
LANGUAGE  plpgsql;


CREATE OR REPLACE FUNCTION test_pg.init()
RETURNS void
AS
$BODY$
BEGIN
if aws_oracle_ext.is_package_initialized
      ('test_pg' ) then
```

```
      return;
    end if;
    perform aws_oracle_ext.set_package_initialized
      ('test_pg' );

PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_output', NULL::INTEGER);
PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_status', NULL::text);
END;
$BODY$
LANGUAGE  plpgsql;


DO $$
declare
v_sql text;
v_output_loc int;
a integer :=1;
b integer :=2;
BEGIN
perform  test_pg.init();
--raise notice 'v_sql %',v_sql;
execute 'do $a$ declare v_output_l int; begin select * from test_pg.calc_stats_new1('||
a||','||b||') into v_output_l;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_output'', v_output_l) ;
 end; $a$'  ;
v_output_loc := aws_oracle_ext.get_package_variable('test_pg', 'v_output');
raise notice 'v_output_loc %',v_output_loc;
END ;
$$
```

Ayudar a reforzar el etiquetado en DynamoDB

Mansi Suratwala, Amazon Web Services

Resumen

Este patrón configura notificaciones automáticas cuando falta o se elimina una etiqueta predefinida de Amazon DynamoDB de un recurso de DynamoDB en la nube de Amazon Web Services (AWS).

DynamoDB es un servicio de bases de datos NoSQL totalmente administrado que proporciona un rendimiento rápido y predecible así como escalabilidad. DynamoDB le permite liberarse de la carga administrativa que supone operar y escalar una base de datos distribuida. Cuando utiliza DynamoDB, no tiene que preocuparse del aprovisionamiento, la instalación ni la configuración del hardware, ni tampoco de las tareas de replicación, aplicación de parches de software o escalado de clústeres.

El patrón utiliza una CloudFormation plantilla de AWS, que crea un evento de Amazon CloudWatch Events y una función de AWS Lambda. El evento busca cualquier información de etiquetado de DynamoDB nueva o existente mediante AWS. CloudTrail Si falta o se elimina una etiqueta predefinida, CloudWatch activa una función Lambda, que le envía una notificación del Amazon Simple Notification Service (Amazon SNS) informándole de la infracción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un bucket de Amazon Simple Storage Service (Amazon S3) para el archivo .zip de Lambda que contiene el script de Python para ejecutar la función de Lambda

Limitaciones

- La solución solo funciona cuando se producen los `UntagResource` CloudTrail eventos `TagResource` or. No crea notificaciones para ningún otro evento.

Arquitectura

Pila de tecnología de destino

- Amazon DynamoDB

- AWS CloudTrail
- Amazon CloudWatch
- AWS Lambda
- Amazon S3
- Amazon SNS

Arquitectura de destino

Automatización y escala

Puede utilizar la CloudFormation plantilla de AWS varias veces para distintas regiones y cuentas de AWS. Debe ejecutar la plantilla solo una vez en cada región o cuenta.

Herramientas

Herramientas

- Amazon DynamoDB: DynamoDB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido y predecible, así como escalabilidad.
- AWS CloudTrail: CloudTrail es un servicio de AWS que le ayuda con la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de su cuenta de AWS. Las acciones realizadas por un usuario, un rol o un servicio de AWS se registran como eventos en CloudTrail.
- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece un flujo casi en tiempo real de eventos del sistema que describen los cambios en los recursos de AWS.
- AWS Lambda: Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable que se puede utilizar para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio web que permite a las aplicaciones, los usuarios finales y los dispositivos enviar y recibir al instante notificaciones desde la nube.

Codigo

- El archivo .zip del proyecto está disponible como adjunto.

Epics

Cómo definir el bucket de S3

Tarea	Descripción	Habilidades requeridas
Defina el bucket de S3.	En la consola de Amazon S3, seleccione o cree un bucket de S3 con un nombre único que no contenga barras diagonales iniciales . Este bucket de S3 alojará el archivo .zip de código de Lambda. El bucket de S3 debe estar en la misma región de AWS que el recurso de DynamoDB que se está monitoreando.	Arquitecto de la nube

Cómo cargar el código de Lambda en el bucket de S3

Tarea	Descripción	Habilidades requeridas
Cargue el código de Lambda en el bucket de S3.	Cargue el archivo .zip de código de Lambda que se proporciona en la sección Adjuntos en el bucket de S3. El bucket de S3 debe estar en la misma región de que el recurso de DynamoDB que se está supervisando.	Arquitecto de la nube

Implemente la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla de AWS.	En la CloudFormation consola de AWS, implemente la CloudFormation plantilla de AWS que se proporciona en la sección de adjuntos. En la Epic siguiente, proporcione valores para los parámetros.	Arquitecto de la nube

Complete los parámetros de la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Ponga nombre al bucket de S3.	Escriba el nombre de bucket de S3 que ha creado o elegido en la primera Epic.	Arquitecto de la nube
Proporcione la clave de Amazon S3.	Proporcione la ubicación del archivo .zip del código de Lambda en su bucket de S3, sin barras diagonales iniciales (por ejemplo, `<folder>/<file-name>.zip`).	Arquitecto de la nube
Facilitar una dirección de correo electrónico	Proporcione una dirección de correo electrónico activa en la que desea recibir las notificac iones de Amazon SNS.	Arquitecto de la nube
Defina el nivel de registro.	Defina el nivel y la frecuenci a de registro de la función de Lambda. `Info` designa mensajes informativos detallados sobre el progreso	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	de la aplicación. `Error` designa los eventos de error que aún podrían permitir que la aplicación siguiera ejecutándose. `Warning` designa situaciones potencial mente dañinas.	
Introduzca las claves de etiquetas de DynamoDB requeridas.	Asegúrese de que las etiquetas estén separadas por comas, sin espacios entre ellas (por ejemplo, `ApplicationId,Crea tedBy,Environment, Organization`). El evento CloudWatch Events busca estas etiquetas y envía una notificación si no las encuentra .	Arquitecto de la nube

Confirme la suscripción.

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la plantilla se implementa correctamente, envía un correo electrónico de suscripción a la dirección de correo electrónico que proporcionaste. Para recibir notificaciones de infracciones, debes confirmar esta suscripci ón de correo electrónico.	Arquitecto de la nube

Recursos relacionados

- Crear un bucket de S3
- Carga de archivos en un bucket de S3
- Recursos de etiquetado en DynamoDB
- Crear una regla de CloudWatch eventos que se active en una llamada a la API de AWS mediante AWS CloudTrail

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Implemente recuperación de desastres entre regiones con AWS DMS y Amazon Aurora

Mark Hudson, Amazon Web Services

Resumen

Los desastres naturales o provocados por el hombre pueden suceder en cualquier momento y afectar a la disponibilidad de los servicios y cargas de trabajo que se ejecutan en una determinada región de AWS. Para mitigar estos riesgos, debe desarrollar un plan de recuperación de desastres (DR) que incorpore las capacidades integradas entre regiones de los servicios de AWS. En el caso de servicios de AWS que no proporcionan funcionalidad entre regiones de forma inherente, el plan de DR también debe proporcionar una solución para gestionar la conmutación por error entre regiones de AWS.

Este patrón le guía a través de una configuración de recuperación de desastres que incluye dos clústeres de bases de datos de Amazon Aurora compatibles con MySQL en una única región. Para satisfacer los requisitos de DR, los clústeres de bases de datos están configurados para usar la característica de base de datos global de Amazon Aurora, con una única base de datos que abarca múltiples regiones de AWS. Una tarea de AWS Database Migration Service (AWS DMS) replica datos entre los clústeres de la región local. No obstante, actualmente AWS DMS no es compatible con la conmutación por error de tareas entre regiones. Este patrón incluye los pasos necesarios para evitar esa limitación y configurar AWS DMS de forma independiente en ambas regiones.

Requisitos previos y limitaciones

Requisitos previos

- Regiones de AWS principales y secundarias seleccionadas, compatibles con bases de datos globales de Amazon Aurora.
- Dos clústeres de bases de datos independientes de Amazon Aurora compatible con MySQL en una sola cuenta en la región principal.
- Clase de instancia de base de datos db.r5 o superior (recomendada).
- Una tarea de AWS DMS en la región principal que realice una replicación continua entre los clústeres de bases de datos existentes.
- Recursos regionales de DR disponibles para satisfacer los requisitos de creación de instancias de bases de datos. Para obtener más información, consulte Uso de una instancia de base de datos en una VPC.

Limitaciones

- Para ver la lista completa de limitaciones de las bases de datos globales de Amazon Aurora, consulte Limitaciones de las bases de datos globales de Amazon Aurora.

Versiones de producto

- Amazon Aurora compatible con MySQL edición 5.7 o 8.0. Para obtener más información, consulte versiones de Amazon Aurora.

Arquitectura

Pila de tecnología de destino

- Clúster de base de datos global de Amazon Aurora compatible con MySQL
- AWS DMS

Arquitectura de destino

En el siguiente diagrama se muestra una base de datos global para dos regiones de AWS, una con las bases de datos principal y de informes primarias y la replicación de AWS DMS, y otra con las bases de datos principal y de informes secundarias.

Automatización y escala

Puede usar AWS CloudFormation para crear la infraestructura necesaria en la región secundaria, como la nube privada virtual (VPC), las subredes y los grupos de parámetros. También puede usar AWS CloudFormation para crear los clústeres secundarios en la región DR y añadirlos a la base de datos global. Si utilizó CloudFormation plantillas para crear los clústeres de bases de datos en la región principal, puede actualizarlas o ampliarlas con una plantilla adicional para crear el recurso de base de datos global. Para obtener más información, consulte Crear un clúster de base de datos de Amazon Aurora con dos instancias de base de datos y Crear un clúster de base de datos global para Aurora MySQL.

Por último, puede crear las tareas de AWS DMS en las regiones principal y secundaria utilizándolas CloudFormation después de que se produzcan los eventos de conmutación por error y devolución. Para obtener más información, consulte AWS::DMS::ReplicationTask.

Tools (Herramientas)

- Amazon Aurora es un motor de base de datos relacional completamente administrado compatible con MySQL y PostgreSQL. Este patrón utiliza la edición de Amazon Aurora compatible con MySQL.
- Las Bases de datos globales de Amazon Aurora están diseñadas para aplicaciones distribuidas por todo el mundo. Una única base de datos global de Amazon Aurora puede abarcar varias regiones de AWS. Replica sus datos sin afectar al rendimiento de la base de datos. También facilita las lecturas locales rápidas con baja latencia en cada región, y proporciona recuperación de desastres en caso de interrupciones en toda la región.
- AWS DMS ofrece migración puntual o replicación continua. La tarea de replicación continua mantiene sincronizadas las bases de datos de origen y destino. Una vez configurada, la tarea de replicación continua aplica de forma constante los cambios del origen al destino con una latencia mínima. Todas las funciones de AWS DMS, como la validación y las transformaciones de datos, están disponibles para cualquier tarea de replicación.

Epics

Prepare los clústeres de bases de datos existentes en la región principal

Tarea	Descripción	Habilidades requeridas
Modifique el grupo de parámetros del clúster de bases de datos.	En el grupo de parámetros del clúster de base de datos existente, active el registro binario a nivel de fila configurando el parámetro `binlog_format` en el valor de fila. AWS DMS requiere el registro binario a nivel de fila para las bases de datos compatibles con MySQL al realizar replicación continua o captura de datos de cambios (CDC). Para obtener más información, consulte Usar una base de	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	datos compatible con MySQL gestionada por AWS como origen de AWS DMS.	

Tarea	Descripción	Habilidades requeridas

Actualice el período de retención del registro binario de la base de datos.	Con un cliente MySQL instalado en el dispositivo del usuario final o una instancia de Amazon Elastic Compute Cloud (Amazon EC2), ejecute el siguiente procedimiento almacenado proporcionado por Amazon Relational Database Service (Amazon RDS) en el nodo de escritura del clúster de base de datos principal, que es el número de horas XX que se conservan los registros.
	`call mysql.rds_set_configuration('binlog retention hours', XX)`
	Confirme la configuración ejecutando el siguiente comando.
	`call mysql.rds_show_configuration;`
	Las bases de datos compatibles con MySQL administradas por AWS purgan los registros binarios lo antes posible. Por lo tanto, el período de retención debe ser lo suficientemente prolongado como para garantizar que los registros no se purguen antes de
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	ejecutar la tarea de AWS DMS. Un valor de 24 horas suele ser suficiente, pero deberá basarse en el tiempo necesario para configurar la tarea de AWS DMS en la región de DR.	

Actualice la tarea de AWS DMS existente en la región principal

Tarea	Descripción	Habilidades requeridas

Registre el ARN de la tarea de AWS DMS.	Use el nombre de recurso de Amazon (ARN) para obtener el nombre de tarea de AWS DMS. Lo usará posterior mente. Para recuperar el ARN de la tarea de AWS DMS, visualice la tarea en la consola o ejecute el siguiente comando.
	`aws dms describe-replication-tasks`
	Un registro de ARN tiene el siguiente aspecto.
	`arn:aws:dms:us-east-1:<accountid>:task:AN6HFFMPM246XOZVEUHCNSOVF7MQCLTOZUIRAMY`
		Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	Los caracteres que aparecen tras los últimos dos puntos corresponden al nombre de la tarea que se usará en un paso posterior.	
Modifique la tarea de AWS DMS existente para registrar el punto de control.	El punto de comprobación que AWS DMS crea contiene información para que el motor de replicación sepa el punto de recuperación del flujo de cambios. Para registrar la información del punto de control, siga estos pasos en la consola: 1. Detenga las tareas de AWS DMS. 2. Utilice el editor JSON en la tarea para establecer el TaskRecoveryTableEnabled parámetro en true. 3. Inicie las tareas de AWS DMS.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Valide la información del punto de control.	Con un cliente MySQL conectado al punto de conexión de escritura del clúster, consulte la nueva tabla de metadatos en el clúster secundario de base de datos para comprobar que existe y contiene la información del estado de la replicación. Ejecute el comando siguiente. `select * from awsdms_control.awsdms_txn_state;` El nombre de la tarea de ARN se encuentra en la columna `Task_Name` de esta tabla.	Administrador de base de datos

Amplíe ambos clústeres de Amazon Aurora a una región de DR

Tarea	Descripción	Habilidades requeridas
Cree una infraestructura base en la región de DR.	Cree los componentes básicos necesarios para la creación y acceso a los clústeres de Amazon Aurora: • Virtual Private Cloud (VPC) (Nube virtual privada [VPC]) • Subredes • Security group (Grupo de seguridad)	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	• Listas de control de acceso a la red • Grupo de subredes • DB Parameter Group (Grupo de parámetros de base de datos) • Grupo de parámetros de clúster de base de datos Asegúrese de que la configuración de ambos grupos de parámetros coincida con la configuración de la región principal.	
Agregue la región de DR a ambos clústeres de Amazon Aurora.	Agregue una región secundaria (la región de DR) a los clústeres principales y secundarios de Amazon Aurora. Para mayor información, consulte Cómo agregar una región AWS a una base de datos global de Amazon Aurora.	Administrador de AWS

Realice una conmutación por error

Tarea	Descripción	Habilidades requeridas
Detenga las tareas de AWS DMS.	La tarea de AWS DMS en la región principal no funcionará correctamente tras la conmutación por error, y	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	deberá detenerla para evitar errores.	
Realice una conmutación por error gestionada.	Realice una conmutación por error gestionada del clúster de base de datos principal a la región de DR. Para instrucciones, consulte Ejecución de la conmutación por error planificada administrada para bases de datos globales de Amazon Aurora. Una vez finalizada la conmutación por error en el clúster de base de datos principal, realice la misma operación en el clúster de base de datos secundaria.	Administrador de AWS, administrador de base de datos
Cargue los datos en la base de datos principal.	Inserte los datos de prueba en el nodo de escritura de la base de datos principal del clúster de base de datos de DR. Estos datos se usarán para validar el correcto funcionamiento de la replicación.	Administrador de base de datos
Cree una instancia de replicación de AWS DMS.	Para crear la instancia de replicación de AWS DMS en la región de DR, consulte Crear una instancia de replicación.	Administrador de AWS, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree los puntos de conexión de AWS DMS de origen y de destino.	Para crear los puntos de conexión de origen y destino de AWS DMS en la región de DR, consulte Crear puntos de conexión de origen y destino. El origen debe apuntar a la instancia de escritura del clúster de la base de datos principal. El origen debe apuntar a la instancia de escritura del clúster de la base de datos principal.	Administrador de AWS, administrador de base de datos
Obtenga el punto de control de replicación.	Para obtener el punto de control de replicación, consulte la tabla de metadatos con un cliente MySQL ejecutando la siguiente operación en el nodo de escritura del clúster de base de datos secundaria de la región de DR. `select * from awsdms_control.awsdms_txn_state;` En la tabla, busque el valor task_name que corresponde al ARN de la tarea de AWS DMS en la región principal que obtuvo en la segunda épica.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree una tarea de AWS DMS.	Desde la consola, cree una tarea de AWS DMS en la región de DR. En la tarea, especifique un método de migración para replicar únicamente los cambios de datos. Para obtener más información, consulte Crear una tarea. 1. En la configuración de la tarea, use el asistente para especificar lo siguiente: • Modo de inicio de CDC para transacciones de origen: habilite el modo de inicio de CDC personalizado • Punto de inicio de CDC personalizado para transacciones de origen: especifique un punto de control de recuperación 2. En la casilla Punto de control de recuperación, introduzca en la tabla `awsdms_txn_state` el valor del punto de control de replicación obtenido previamente mediante la consulta a la base de datos. 3. En la sección de configura ción de la tarea, selecciona	Administrador de AWS, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	el editor JSON y establece el TaskRecoveryTableEnabledparámetro en true. Establezca la configuración Iniciar tarea de migración de la tarea de AWS DMS en Automáticamente al crear.	
Registre el ARN de la tarea de AWS DMS.	Utilice el ARN para obtener el nombre de la tarea tarea de AWS DMS para uso posterior . Para recuperar el ARN de la tarea de AWS DMS, ejecute el siguiente comando. `aws dms describe-replication-tasks`	Administrador de AWS, administrador de base de datos
Valide los datos replicados.	Consulte el clúster de base de datos secundaria en la región de DR para confirmar que los datos de prueba que cargó en el clúster de base de datos principal se han replicado.	Administrador de base de datos

Realice una conmutación por recuperación

Tarea	Descripción	Habilidades requeridas
Detenga las tareas de AWS DMS.	La tarea de AWS DMS en la región DR no funcionará correctamente tras la conmutación por error, y	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	deberá detenerla para evitar errores.	
Realice una conmutación por error gestionada.	Realice una conmutación por error el clúster de base de datos principal de la región principal. Para instrucciones, consulte Ejecución de la conmutación por error planificada administrada para bases de datos globales de Amazon Aurora. Una vez finalizada la conmutación por error en el clúster de la base de datos principal, realice la misma operación en el clúster de base de datos.	Administrador de AWS, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Obtenga el punto de control de replicación.	Para obtener el punto de control de replicación, consulte la tabla de metadatos con un cliente MySQL ejecutando la siguiente operación en el nodo de escritura del clúster de base de datos secundaria de la región de DR. `select * from awsdms_control.awsdms_txn_state;` En la tabla, busque el valor `task_name` que corresponde al ARN de la tarea de AWS DMS en la región DR que obtuvo en la cuarta épica.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Actualice los puntos de conexión de origen y de destino de AWS DMS.	Una vez conmutados por error los clústeres de bases de datos, compruebe los clústeres de la región principal para determinar qué nodos son las instancias de escritura . A continuación, compruebe que los puntos de conexión de origen y destino de AWS DMS existentes en la región principal apunten a las instancias de escritura. Si no es así, actualice los puntos de conexión con los nombres del sistema de nombres de dominio (DNS) de la instancia de escritura.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Cree una tarea de AWS DMS.	Utilizando la consola, cree una tarea de AWS DMS en la región principal. En la tarea, especifique un método de migración para replicar únicamente los cambios de datos. Para obtener más información, consulte Crear una tarea. 1. En la configuración de tareas, use el asistente para especificar lo siguiente : • Modo de inicio de CDC para transacciones de origen: habilite el modo de inicio de CDC personalizado • Punto de inicio de CDC personalizado para transacciones de origen: especifique un punto de control de recuperación 2. En la casilla Punto de control de recuperación, introduzca en la tabla `awsdms_txn_state` el valor del punto de control de replicación obtenido previamente mediante la consulta a la base de datos.	Administrador de AWS, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	3. También en la sección de configuración de tareas, selecciona el editor JSON y establece el TaskRecoveryTableEnabledparámetro en true. 4. Finalmente, establezca la tarea de AWS DMS Iniciar tarea de migración a Crear automáticamente.	
Registre el nombre de recurso de Amazon (ARN) de la tarea AWS DMS.	Utilice el ARN para obtener el nombre de la tarea tarea de AWS DMS para uso posterior . Para recuperar el ARN de tarea de AWS DMS, ejecute el siguiente comando: `aws dms describe-replication-tasks` Necesitará el nombre de la tarea cuando realice otra conmutación por error gestionada o en un escenario de DR.	Administrador de AWS, administrador de base de datos
Elimine las tareas de AWS DMS.	Elimine la tarea de AWS DMS original (actualmente detenida) en la región principal y la tarea de AWS DMS existente (actualmente detenida) en la región secundaria.	Administrador de AWS

Recursos relacionados

- Configuración de su clúster de base de datos de Amazon Aurora
- Uso de bases de datos globales de Amazon Aurora
- Trabajar con Amazon Aurora MySQL
- Trabajar con una instancia de replicación de AWS DMS
- Trabajar con puntos de conexión de AWS DMS
- Trabajar con tareas de AWS DMS
- ¿Qué es AWS CloudFormation?

Información adicional

En este ejemplo de DR se usan bases de datos globales de Amazon Aurora, ya que proporcionan un objetivo de tiempo de recuperación (RTO) efectivo de 1 segundo y un objetivo de punto de recuperación (RPO) de menos de 1 minuto, ambos inferiores a los de las soluciones replicadas tradicionales e ideales para escenarios de DR.

Las bases de datos globales de Amazon Aurora ofrecen muchas otras ventajas, entre las que se incluyen las siguientes:

- Lecturas globales con latencia local: los consumidores globales pueden acceder a la información en una región local y con latencia local.
- Clústeres de base de datos Amazon Aurora secundarios escalables: los clústeres secundarios se pueden escalar de forma independiente, y es posible añadir hasta 16 réplicas de solo lectura.
- Replicación rápida de clústeres de base de datos Aurora primarios a secundarios – La replicación realizada tiene poco impacto en el clúster principal. Se produce en la capa de almacenamiento, con latencias típicas de replicación entre regiones de menos de 1 segundo.

Este patrón también emplea AWS DMS para la replicación. Las bases de datos de Amazon Aurora ofrecen la posibilidad de crear réplicas de lectura, lo que puede simplificar el proceso de replicación y la configuración de DR. AWS DMS suele usarse para replicar cuando es necesario transformar los datos, o cuando la base de datos de destino requiere índices adicionales que la base de datos de origen no contiene.

Migración de funciones y procedimientos de Oracle con más de 100 argumentos a PostgreSQL

Srinivas Potlachervoo, Amazon Web Services

Resumen

Este patrón muestra cómo migrar funciones y procedimientos de Oracle Database que tienen más de 100 argumentos a PostgreSQL. Por ejemplo, puede usar este patrón para migrar funciones y procedimientos de Oracle a uno de los siguientes servicios de bases de datos de AWS compatibles con PostgreSQL:

- Amazon Relational Database Service (Amazon RDS) para PostgreSQL
- Edición de Amazon Aurora compatible con PostgreSQL

PostgreSQL no admite funciones o procedimientos que tengan más de 100 argumentos. Como solución alternativa, puede definir un nuevo tipo de datos cuyos campos de tipo coincidan con los argumentos de la función de origen. A continuación, puede crear y ejecutar una PL/pgSQL función que utilice el tipo de datos personalizado como argumento.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una instancia de base de datos (DB) Oracle de Amazon RDS
- Una instancia de base de datos Amazon RDS para PostgreSQL o una instancia de base de datos Aurora compatible con PostgreSQL

Versiones de producto

- Instancia de base de datos de Oracle de Amazon RDS, versión 10.2 y posteriores
- Instancia de base de datos Amazon RDS PostgreSQL, versión 9.4 y posteriores, o instancia de base de datos Aurora compatible con PostgreSQL, versión 9.4 y posteriores
- Oracle SQL Developer versión 18 y posteriores
- pgAdmin versión 4 y posteriores

Arquitectura

Pila de tecnología de origen

- Instancia de base de datos de Oracle de Amazon RDS, versión 10.2 y posteriores

Pila de tecnología de destino

- Instancia de base de datos Amazon RDS PostgreSQL, versión 9.4 y posteriores, o instancia de base de datos Aurora compatible con PostgreSQL, versión 9.4 y posteriores

Tools (Herramientas)

Servicios de AWS

- Amazon Relational Database Service (Amazon RDS) para PostgreSQL le ayuda a configurar, utilizar y escalar una base de datos relacional de PostgreSQL en la nube de AWS.
- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.

Otros servicios

- Oracle SQL Developer es un entorno de desarrollo integrado que simplifica el desarrollo y la administración de bases de datos de Oracle, tanto en implementaciones tradicionales como en implementaciones basadas en la nube.
- pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.

Prácticas recomendadas

Asegúrese de que el tipo de datos creado coincida con los campos de tipos que se incluyen en la función o procedimiento de Oracle de origen.

Epics

Ejecute una función o procedimiento de Oracle con más de 100 argumentos

Tarea	Descripción	Habilidades requeridas
Cree o identifique una Oracle/PLSQL función o procedimiento existente que tenga más de 100 argumentos.	Cree una Oracle/PLSQL función o un procedimiento que tenga más de 100 argumentos. -o bien- Identifique una Oracle/PLSQL función o un procedimiento existente que tenga más de 100 argumentos. Para obtener más información, consulte las secciones 14.7 Instrucción CREATE FUNCTION y 14.11 Instrucción CREATE PROCEDURE de la documentación de bases de datos de Oracle.	Conocimientos de Oracle/PL/SQL
Compila la Oracle/PLSQL función o el procedimiento.	Compila la Oracle/PLSQL función o el procedimiento. Para más información, consulte Compilación de una función en la documentación de la base de datos de Oracle.	Conocimientos de Oracle/PL/SQL
Ejecute la Oracle/PLSQL función.	Ejecute la Oracle/PLSQL función o el procedimiento. A continuación, guarde el resultado.	Conocimientos de Oracle/PL/SQL

Defina un nuevo tipo de datos que coincida con los argumentos de la función o procedimiento de origen

Tarea	Descripción	Habilidades requeridas
Defina un nuevo tipo de datos en PostgreSQL.	Defina un nuevo tipo de datos en PostgreSQL que incluya todos los campos que aparecen en los argumentos de la función o procedimiento de Oracle de origen. Para obtener más información, consulte CREATE TYPE en la documentación de PostgreSQL.	Conocimientos de PostgreSQL PL/pgSQL

Cree una función de PostgreSQL que incluya el nuevo argumento TYPE

Tarea	Descripción	Habilidades requeridas
Cree una función de PostgreSQL que incluya el nuevo tipo de datos.	Crear una función de PostgreSQL que incluya el nuevo argumento `TYPE`. Para ver un ejemplo de función, consulte la sección de Información adicional de este patrón.	Conocimientos de PostgreSQL PL/pgSQL
Compile la función PostgreSQL.	Compile la función en PostgreSQL. Si los campos del nuevo tipo de datos coinciden con los argumentos de la función o procedimiento de origen, la función se compilará correctamente.	Conocimientos de PostgreSQL PL/pgSQL

Tarea	Descripción	Habilidades requeridas
Ejecute la función de PostgreSQL.	Ejecute la función de PostgreSQL.	Conocimientos de PostgreSQL PL/pgSQL

Resolución de problemas

Problema	Solución
La función devuelve el siguiente error: ERROR: syntax error near "<statement>"	Asegúrese de que todas las instrucciones de la función terminen con punto y coma (`;`).
La función devuelve el siguiente error: ERROR: "<variable>" is not a known variable	Asegúrese de que la variable empleada en el cuerpo de la función aparezca en la sección `DECLARE` de la función.

Recursos relacionados

- Uso de Amazon Aurora PostgreSQL (Guía del usuario de Amazon Aurora para Aurora)
- CREATE TYPE (documentación de PostgreSQL)

Información adicional

Ejemplo de función PostgreSQL que incluye un argumento TYPE

```
CREATE OR REPLACE FUNCTION test_proc_new
(
    IN p_rec type_test_proc_args
)
RETURNS void
AS
$BODY$
BEGIN

    /*
    **************
    The body would contain code to process the input values.
```

```
    For our testing, we will display couple of values.
    ***************
    */
    RAISE NOTICE USING MESSAGE = CONCAT_WS('', 'p_acct_id: ', p_rec.p_acct_id);
    RAISE NOTICE USING MESSAGE = CONCAT_WS('', 'p_ord_id: ', p_rec.p_ord_id);
    RAISE NOTICE USING MESSAGE = CONCAT_WS('', 'p_ord_date: ', p_rec.p_ord_date);

END;
$BODY$
LANGUAGE plpgsql
COST 100;
```

Migre una base de datos de Oracle a Amazon RDS mediante la importación directa de Oracle Data Pump a través de un enlace de base de datos

Rizwan Wangde, Amazon Web Services

Resumen

Numerosos patrones cubren la migración de bases de datos de Oracle en las instalaciones a Amazon Relational Database Service (Amazon RDS) para Oracle mediante Oracle Data Pump, una utilidad nativa de Oracle que es la forma preferida de migrar grandes cargas de trabajo de Oracle. Estos patrones suelen implicar la exportación de tablas o esquemas de aplicaciones a archivos de volcado, la transferencia de los archivos de volcado a un directorio de base de datos en Amazon RDS para Oracle y, a continuación, la importación de los esquemas de aplicación y los datos de los archivos de volcado.

Con este enfoque, la migración puede tardar más en función del tamaño de los datos y del tiempo que se tarde en transferir los archivos de volcado a la instancia de Amazon RDS. Además, los archivos de volcado residen en el volumen Amazon Elastic Block Store (Amazon EBS) de la instancia de Amazon RDS, que debe ser lo suficientemente grande para la base de datos y los archivos de volcado. Si los archivos volcados se eliminan tras la importación, no se puede recuperar el espacio vacío, por lo que tendrá que pagar por el espacio no utilizado.

Este patrón mitiga estos problemas al realizar una importación directa en la instancia de Amazon RDS mediante la API de Oracle Data Pump (`DBMS_DATAPUMP`) a través de un enlace de base de datos. El patrón inicia una canalización de exportación e importación simultánea entre las bases de datos de origen y destino. Este patrón no requiere ajustar el tamaño de un volumen de EBS para los archivos de volcado porque no se crea ni almacena ningún archivo de volcado en el volumen. Este enfoque ahorra el costo mensual del espacio en disco no utilizado.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa.
- Una nube privada virtual (VPC) configurada con subredes privadas en al menos dos zonas de disponibilidad, para proporcionar la infraestructura de red para la instancia de Amazon RDS.
- Una base de datos de Oracle en un centro de datos en las instalaciones o autoadministrada en Amazon Elastic Compute Cloud (Amazon EC2).

- Una instancia de Amazon RDS para Oracle en una única zona de disponibilidad. El uso de una única zona de disponibilidad mejora el rendimiento de escritura durante la migración. Se puede habilitar una implementación Multi-AZ entre 24 y 48 horas antes de la transición.

  Esta solución también puede utilizar Amazon RDS Custom para Oracle como destino.
- AWS Direct Connect (recomendado para bases de datos de gran tamaño).
- La conectividad de red y las reglas de firewall locales están configuradas para permitir una conexión entrante desde la instancia de Amazon RDS a la base de datos de Oracle en las instalaciones.

Limitaciones

- El límite de tamaño de la base de datos en Amazon RDS para Oracle es de 64 tebibytes (TiB) en diciembre de 2022.
- El tamaño máximo de un solo archivo en las instancias de base de datos de Amazon RDS para Oracle es de 16 TiB. Es importante saberlo porque es posible que tenga que distribuir las tablas en varios espacios de tablas.

Versiones de producto

- Base de datos de origen: base de datos de Oracle 10g, versión 1 y posteriores.
- Base de datos de destino: para obtener la lista más reciente de versiones y ediciones compatibles en Amazon RDS, consulte Amazon RDS para Oracle en la documentación de AWS.

Arquitectura

Pila de tecnología de origen

- Base de datos de Oracle autoadministrada en las instalaciones o en la nube

Pila de tecnología de destino

- Amazon RDS para Oracle o Amazon RDS Custom para Oracle

Arquitectura de destino

El siguiente diagrama muestra la arquitectura para migrar de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle en un entorno Single-AZ. Las direcciones de las flechas representan el flujo de datos en la arquitectura. El diagrama no muestra qué componente está iniciando la conexión.

1. La instancia de Amazon RDS para Oracle se conecta a la base de datos de Oracle de origen en las instalaciones para realizar una migración a plena carga a través del enlace de la base de datos.
2. AWS Database Migration Service (AWS DMS) se conecta a la base de datos Oracle de origen local para realizar una replicación continua mediante la captura de datos de cambios (CDC).
3. Los cambios de los CDC se aplican a la base de datos de Amazon RDS para Oracle.

Tools (Herramientas)

Servicios de AWS

- AWS Database Migration Service (AWS DMS) le ayuda a migrar los almacenes de datos a una combinación de configuraciones locales y en la nube Nube de AWS o entre ellas. Este patrón usa CDC y la configuración Replicar solo cambios de datos.
- AWS Direct Connectconecta su red interna a una Direct Connect ubicación a través de un cable Ethernet de fibra óptica estándar. Con esta conexión, puede crear interfaces virtuales directamente con las públicas y, al Servicios de AWS mismo tiempo, omitir a los proveedores de servicios de Internet en su ruta de red.
- Amazon Relational Database Service le ayuda a configurar, operar y escalar una base de datos relacional de Oracle en. Nube de AWS

Otras herramientas

- Oracle Data Pump le ayuda a trasladar datos y metadatos de una base de datos a otra a altas velocidades.
- Se utilizan herramientas de cliente como Oracle Instant Client o SQL Developer para conectar y ejecutar consultas SQL en la base de datos.

Prácticas recomendadas

Aunque Direct Connect utiliza conexiones de red privadas y dedicadas entre la red local AWS, tenga en cuenta las siguientes opciones para aumentar la seguridad y el cifrado de los datos en tránsito:

- Una red privada virtual (VPN) que utilice AWS Site-to-Site VPN o una conexión IPsec VPN desde la red local a la red AWS
- El cifrado de red nativo de la base de datos de Oracle configurado en la base de datos de Oracle en las instalaciones
- Cifrado con TLS

Epics

Prepare la base de datos en las instalaciones de origen

Tarea	Descripción	Habilidades requeridas
Configurar la conectividad de red desde la base de datos de destino a la base de datos de origen.	Configure el firewall y la red en las instalaciones para permitir la conexión entrante desde la instancia de Amazon RDS de destino a la base de datos de Oracle de origen en las instalaciones.	Administrador de redes, ingeniero de seguridad

Crear un usuario de base de datos con los privilegios adecuados.	Cree un usuario de base de datos en la base de datos de Oracle de origen en las instalaciones con privilegios para migrar datos entre el origen y el destino mediante Oracle Data Pump:
	`GRANT CONNECT to <migration_user>;`
	`GRANT DATAPUMP_EXP_FULL_DATABASE to <migration_user>;`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`GRANT SELECT ANY TABLE to <migration_user>;`	

Prepare la base de datos fuente local para la migración a AWS DMS los CDC.	(Opcional) Prepare la base de datos Oracle de origen local para la migración a AWS DMS los CDC después de completar la carga completa de Oracle Data Pump:
	1. Configure los privilegios adicionales necesarios para administrar FLASHBACK durante la migración a Oracle Data Pump:
	`GRANT FLASHBACK ANY TABLE to <migration_user>;`
	`GRANT FLASHBACK ARCHIVE ADMINISTER to <migration_user>;`
	2. Para configurar los privilegios de las cuentas de usuario necesarios en una fuente de Oracle autogestionada AWS DMS, consulte la AWS DMS documentación.
	3. Para preparar una base de datos fuente autogestionada de Oracle para su uso por los CDC AWS DMS, consulte la AWS DMS documentación.
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Instalar y configurar SQL Developer.	Instale y configure SQL Developer para conectar y ejecutar consultas SQL en las bases de datos de origen y destino.	Administrador de base de datos, ingeniero de migracion es
Generar un script para crear los espacios de tabla.	Utilice el siguiente ejemplo de consulta SQL para generar el script en la base de datos de origen: `SELECT 'CREATE TABLESPACE ' tablespace_name ' DATAFILE SIZE 1G AUTOEXTEND ON MAXSIZE UNLIMITED;' from dba_tablespaces where tablespace_name not in ('SYSTEM', 'SYSAUX','TEMP','UNDOTBS1') order by 1;` El script se aplicará en la base de datos de destino.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Generar un script para crear usuarios, perfiles, roles y privilegios.	Para generar un script para crear los usuarios, perfiles, funciones y privilegios de la base de datos, utilice los scripts del documento de Oracle Support Cómo extraer DDL para usuario, incluidos los privilegios y roles mediante dbms_metadata.get_ddl (ID de documento 2739952.1) (se requiere una cuenta de Oracle). El script se aplicará en la base de datos de destino.	Administrador de base de datos

Preparación de la instancia de Amazon RDS para Oracle

Tarea	Descripción	Habilidades requeridas
Crear un enlace de base de datos a la base de datos origen y verificar la conectividad.	Para crear un enlace de base de datos a la base de datos en las instalaciones de origen, puede usar el comando de ejemplo siguiente: `CREATE DATABASE LINK link2src CONNECT TO <migration_user_account> IDENTIFIED BY <password> USING '(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=<dns`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	or ip address of remote db>) (PORT=<listener port>))(CONNECT_DATA=(SID=<remote SID>)))'; Para comprobar la conectividad, ejecute el comando de SQL siguiente: select * from dual@link2src; La conectividad es correcta si la respuesta es X.	
Ejecute los scripts para preparar la instancia de destino.	Ejecute los scripts generados anteriormente para preparar la instancia de Amazon RDS para Oracle: 1. Espacios de tabla 2. Profiles 3. Roles Esto ayuda a garantizar que la migración de Oracle Data Pump pueda crear los esquemas y sus objetos.	Administrador de base de datos, ingeniero de migraciones

Realizar una migración a plena carga mediante Oracle Data Pump Import a través de un enlace de base de datos

Tarea	Descripción	Habilidades requeridas
Migre los esquemas necesarios.	Para migrar los esquemas necesarios de la base de datos en las instalaciones de origen a la instancia de Amazon RDS de destino, utilice el código de la sección de información adicional: • Para migrar un único esquema, ejecute el código 1 desde la sección de información adicional. • Para migrar múltiples esquemas, ejecute el código 2 desde la sección de información adicional. Para ajustar el rendimiento de la migración, puede ajustar el número de procesos paralelos mediante la ejecución del siguiente comando: `DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);`	Administrador de base de datos
Recopile estadísticas de esquema para mejorar el rendimiento.	El comando Recopilar estadísticas del esquema devuelve las estadísticas del optimizador de consultas de Oracle recopiladas para	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	los objetos de la base de datos. Con esta informaci ón, el optimizador puede seleccionar el mejor plan de ejecución para cualquier consulta relacionada con estos objetos: `EXECUTE DBMS_STAT S.GATHER_SCHEMA_ST ATS(ownname => '<schema_name>');`	

Realice una migración completa y una replicación de los CDC mediante Oracle Data Pump y AWS DMS

Tarea	Descripción	Habilidades requeridas
Capturar el SCN en la base de datos en las instalaciones de origen de Oracle.	Capture el número de cambio del sistema (SCN) en la base de datos de Oracle en las instalaciones de origen. Debe utilizar el SCN para la importación a plena carga y como punto de partida para la replicación de los CDC. Para generar el SCN actual de la base de datos de origen, ejecute la siguiente instrucción SQL: `SELECT current_scn FROM V$DATABASE;`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Realizar la migración a plena carga de los esquemas.	Para migrar los esquemas necesarios (`FULL LOAD`) de la base de datos en las instalaciones de origen a la instancia de Amazon RDS de destino, haga lo siguiente: • Para migrar un único esquema, ejecute el código 3 desde la sección de información adicional. • Para migrar múltiples esquemas, ejecute el código 4 desde la sección de información adicional. En el código, sustituya `<CURRENT_SCN_VALUE _IN_SOURCE_DATABAS E>` por el SCN que capturó de la base de datos de origen: `DBMS_DATAPUMP.SET_ PARAMETER (handle => v_hdnl, name => 'FLASHBACK_SCN', value => <CURRENT_SCN_VALUE _IN_SOURCE_DATABAS E>);` Para ajustar el rendimiento de la migración, puede configurar el número de procesos paralelos mediante	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	la ejecución del siguiente comando: `DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);`	
Deshabilitar los desencadenadores en los esquemas migrados.	Antes de comenzar la tarea AWS DMS exclusiva de los CDC, desactive la opción situada `TRIGGERS` debajo de los esquemas migrados.	Administrador de base de datos
Recopile estadísticas de esquema para mejorar el rendimiento.	El comando Recopilar estadísticas del esquema devuelve las estadísticas del optimizador de consultas de Oracle recopiladas para los objetos de la base de datos: `EXECUTE DBMS_STATS.GATHER_SCHEMA_STATS(ownname => '<schema_name>');` Con esta información, el optimizador puede seleccionar el mejor plan de ejecución para cualquier consulta relacionada con estos objetos.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Se utiliza AWS DMS para realizar una replicación continua desde el origen hasta el destino.	Se utiliza AWS DMS para realizar una replicación continua desde la base de datos de Oracle de origen a la instancia de Amazon RDS for Oracle de destino. Para obtener más informaci ón, consulte Creating tasks for ongoing replication using AWS DMS y la entrada en el blog How to work with native CDC support in AWS DMS.	Administrador de base de datos, ingeniero de migracion es

Cómo hacer la transición a Amazon RDS para Oracle

Tarea	Descripción	Habilidades requeridas
Habilitar la opción Multi-AZ en la instancia 48 horas antes de la transición.	Si se trata de una instancia de producción, recomendamos habilitar la implementación Multi-AZ en la instancia de Amazon RDS para ofrecer las ventajas de la alta disponibi lidad (HA) y la recuperación de desastres (DR).	Administrador de base de datos, ingeniero de migracion es
Detenga la tarea AWS DMS exclusiva de CDC (si CDC estaba activada).	1. Asegúrese de que la latencia de origen y la latencia de destino en las CloudWatch métricas de Amazon de la AWS DMS tarea muestren 0 segundos.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	2. Detenga la tarea AWS DMS exclusiva de los CDC.	
Habilitar los desencade nadores.	Active los `TRIGGERS` que desactivó antes de crear la tarea de CDC.	Administrador de base de datos

Recursos relacionados

AWS

- Preparar una base de datos fuente autogestionada de Oracle para los CDC mediante AWS DMS
- Creación de tareas para una replicación continua mediante AWS DMS
- Implementaciones Multi-AZ para alta disponibilidad
- How to work with native CDC support in AWS DMS (entrada en el blog)

Documentación de Oracle

- DBMS_DATAPUMP

Información adicional

Código 1: migración solo de carga completa, esquema de aplicación única

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE( handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''<schema_name>'')');  --
 To migrate one selected schema
    DBMS_DATAPUMP.METADATA_FILTER (hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')'); --
 To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
```

```
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Código 2: migración solo de carga completa, esquemas de aplicación múltiples

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE( handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'SCHEMA_LIST',
 '''<SCHEMA_1>'',''<SCHEMA_2>'', ''<SCHEMA_3>'''); -- To migrate multiple schemas
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')');
 -- To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Código 3: migración de carga completa antes de una tarea solo de CDC, esquema de aplicación única

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE( handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''<schema_name>'')');  --
 To migrate one selected schema
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')');
 -- To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARAMETER (handle => v_hdnl, name => 'FLASHBACK_SCN', value =>
 <CURRENT_SCN_VALUE_IN_SOURCE_DATABASE>); -- SCN required for AWS DMS CDC only task.
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
```

```
/
```

Código 4: migración de carga completa antes de una tarea solo de CDC, esquemas de aplicación múltiples

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN (operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE (handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'SCHEMA_LIST',
 '''<SCHEMA_1>'',''<SCHEMA_2>'', ''<SCHEMA_3>'''); -- To migrate multiple schemas
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')');
 -- To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARAMETER (handle => v_hdnl, name => 'FLASHBACK_SCN', value =>
 <CURRENT_SCN_VALUE_IN_SOURCE_DATABASE>); -- SCN required for AWS DMS CDC only task.
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Escenario en el que un enfoque de migración mixto puede funcionar mejor

En raras ocasiones, en las que la base de datos de origen contiene tablas con millones de filas y columnas LOBSEGMENT de gran tamaño, este patrón ralentizará la migración. Oracle migra a LOBSEGMENTs través del enlace de red de uno en uno. Extrae una sola fila (junto con los datos de la columna LOB) de la tabla de origen e inserta la fila en la tabla de destino, repitiendo el proceso hasta que se migren todas las filas. Oracle Data Pump a través del enlace de la base de datos no admite los mecanismos de carga masiva o de carga por LOBSEGMENTs ruta directa.

En las siguientes situaciones, se recomienda:

- Para omitir las tablas identificadas durante la migración de Oracle Data Pump, agregue el siguiente filtro de metadatos:

```
dbms_datapump.metadata_filter(handle =>h1, name=>'NAME_EXPR', value => 'NOT IN
 (''TABLE_1'',''TABLE_2'')');
```

- Utilice una AWS DMS tarea (migración a carga completa, con replicación de CDC si es necesaria) para migrar las tablas identificadas. AWS DMS extraerá varias filas de la base de datos Oracle de origen y las insertará en un lote en la instancia de Amazon RDS de destino, lo que mejora el rendimiento.

Migración de las cargas de trabajo de Redis a Redis Enterprise Cloud en AWS

Antony Prasad Thevaraj, Amazon Web Services

Srinivas Pendyala, Redis

Resumen

Este patrón analiza el proceso de alto nivel para migrar las cargas de trabajo de Redis a Redis Enterprise Cloud en Amazon Web Services (AWS). Describe los pasos de la migración, proporciona información sobre la selección de herramientas disponibles y analiza las ventajas, desventajas y pasos para usar cada herramienta. Si lo desea, si necesita ayuda adicional para migrar cargas de trabajo desde Redis, puede contratar los servicios profesionales de Redis.

Si utiliza Redis OSS o Redis Enterprise Software de forma en las instalaciones, estará familiarizado con los importantes gastos administrativos y la complejidad operativa que supone mantener las bases de datos de Redis en el centro de datos. Al migrar sus cargas de trabajo a la nube, puede reducir significativamente esta carga operativa y aprovechar Redis Enterprise Cloud, que es una oferta de base de datos como servicio (DBaaS) totalmente alojada de Redis. Esta migración ayuda a aumentar la agilidad empresarial, mejora la fiabilidad de las aplicaciones y reduce los costos generales, al tiempo que obtiene acceso a las funciones más recientes de Redis Enterprise Cloud en AWS, como la disponibilidad del 99,999 %, la simplicidad de la arquitectura y la escalabilidad.

Redis Enterprise Cloud tiene posibles aplicaciones en los sectores de los servicios financieros, el comercio minorista, la sanidad y los juegos, así como en casos de uso que requieren soluciones para la detección del fraude, el inventario en tiempo real, el procesamiento de reclamaciones y la gestión de sesiones. Puede usar Redis Enterprise Cloud para conectarse a sus recursos de AWS, por ejemplo, a un servidor de aplicaciones que se ejecute en instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a un microservicio que se implemente como un servicio de AWS Lambda.

Requisitos previos y limitaciones

Supuestos

- Actualmente utiliza un sistema de base de datos en las instalaciones que desea migrar a la nube.
- Ha identificado los requisitos de migración para sus cargas de trabajo, entre los que se incluyen:
  - Requisitos de consistencia de datos
  - Requisitos del entorno de infraestructura y sistema

  - Requisitos de mapeo y transformación de datos
  - Requisitos de pruebas funcionales
  - Requisitos de pruebas de rendimiento
  - Requisitos de validación
  - Estrategia de transición definida
- Ha evaluado los plazos y las estimaciones de costos necesarios para la migración.
- Sus requisitos tienen en cuenta el alcance del trabajo y los sistemas y bases de datos que haya identificado como parte de la migración.
- Ha identificado a las partes interesadas junto con sus funciones y responsabilidades en una matriz responsable, consultada e informada (RACI).
- Ha recibido el acuerdo y las aprobaciones necesarios de todas las partes interesadas.

Costo

En función de las especificaciones técnicas de la base de datos fuente existente (por ejemplo, el tamaño de la memoria, el rendimiento y el tamaño total de los datos), un arquitecto de soluciones de Redis puede dimensionar el sistema de destino en Redis Enterprise Cloud. Para obtener información general sobre los precios, consulte los Precios de Redis en el sitio web de Redis.

Personas y habilidades

El proceso de migración implica las siguientes funciones y responsabilidades.

Rol	Description (Descripción)	Habilidades requeridas
Arquitecto de soluciones de migración	Arquitecto técnico con experiencia en la definición, planificación e implementación de estrategias de migración	Comprensión técnica y a nivel de aplicación de los sistemas de origen y destino; experienc ia en la migración de cargas de trabajo a la nube
Arquitecto de datos	Arquitecto técnico con amplia experiencia en la definición, implementación y entrega de soluciones de datos para una	Modelado de datos para datos estructurados y no estructur ados, con amplios conocimie ntos y experiencia en la

	amplia variedad de bases de datos	implementación de bases de datos para una empresa
Arquitecto de soluciones de Redis	Un arquitecto técnico que puede ayudar a diseñar un clúster Redis de tamaño óptimo para el caso de uso adecuado	Experiencia en el diseño e implementación de solucione s de Redis para una amplia variedad de casos de uso
Arquitecto de soluciones en la nube	Un arquitecto técnico con un conocimiento más profundo de las soluciones en la nube, especialmente en AWS	Experiencia en la creación de soluciones para la nube; experiencia en migración de cargas de trabajo y moderniza ción de aplicaciones
Arquitecto empresarial	Un arquitecto técnico que tenga un conocimiento completo del panorama técnico de su organizac ión, que tenga una visión compartida de la hoja de ruta del futuro y que practique y establezca las prácticas recomendadas de arquitectura estandarizadas en todos los equipos de su organización	Certificaciones de arquitectura de software, como el TOGAF, conocimientos básicos de ingeniería de software y experiencia en arquitectura de soluciones y arquitectura empresarial
Ingeniero o de TI DevOps	Un ingeniero responsable de crear y mantener la infraestr uctura, incluida la supervisi ón de la infraestructura para detectar problemas, realizar tareas de mantenimiento y realizar las actualizaciones necesarias.	Amplio conocimiento de diversas tecnologías, incluidos los sistemas operativos, las redes y la computación en la nube; familiaridad con lenguajes de programación como Python, Bash y Ruby, así como con herramientas como Docker, Kubernetes y Ansible

Arquitectura

Opciones de migración

En el siguiente diagrama, se muestran las opciones para migrar los orígenes de datos en las instalaciones (basadas en Redis u otras) a AWS. Muestra varias herramientas de migración entre las que puede elegir, como la exportación de archivos de Redis Database (RDB) a Amazon Simple Storage Service (Amazon S3), el uso de la característica de replicación de Redis o el uso de AWS DMS.

1. Orígenes de datos en las instalaciones: bases de datos que no están basadas en Redis, como MySQL, PostgreSQL, Oracle, SQL Server o MariaDB.
2. Orígenes de datos en las instalaciones: bases de datos basadas en el protocolo de Redis, como Redis OSS y Redis Enterprise Software.
3. La forma más sencilla de migrar datos de bases de datos basadas en Redis es exportar archivos RDB e importarlos a la nube empresarial de Redis de destino en AWS.
4. Como alternativa, puede migrar los datos del origen al destino mediante la función de replicación (`ReplicaOf`) de Redis.
5. Si sus requisitos de migración de datos incluyen la transformación de los datos, puede emplear Redis Input/Output Tools (RIOT) para migrar los datos.
6. Como alternativa, puede utilizar AWS Data Migration Service (AWS DMS) para migrar los datos desde bases de datos basadas en SQL.
7. Debe utilizar la interconexión de nube privada virtual (VPC) para AWS DMS a fin de migrar los datos correctamente a la nube empresarial de Redis de destino en AWS.

Arquitectura de destino

El siguiente diagrama muestra una arquitectura de implementación típica de Redis Enterprise Cloud en AWS e ilustra cómo se puede usar con los principales servicios de AWS.

1. Puede conectarse a las aplicaciones empresariales respaldadas por Redis Enterprise Cloud en AWS.
2. Puede ejecutar aplicaciones empresariales en su propia cuenta de AWS, en una VPC dentro de esa cuenta.

3. Puede utilizar los puntos de conexión de la base de datos de Redis Enterprise Cloud para conectarse a sus aplicaciones. Los ejemplos incluyen un servidor de aplicaciones que se ejecuta en EC2 instancias, un microservicio implementado como un servicio de AWS Lambda, una aplicación de Amazon Elastic Container Service (Amazon ECS) o una aplicación de Amazon Elastic Kubernetes Service (Amazon EKS).
4. Las aplicaciones empresariales que se ejecutan en su VPC requieren una conexión de emparejamiento de VPC a la VPC de Redis Enterprise Cloud. Esto permite que las aplicaciones empresariales se conecten de forma segura a través de puntos de conexión privados.
5. Redis Enterprise Cloud en AWS es una plataforma de base de datos NoSQL en memoria que se implementa como una S DBaa en AWS y está totalmente gestionada por Redis.
6. Redis Enterprise Cloud se implementa dentro de una VPC en una cuenta de AWS estándar creada por Redis.
7. Por motivos de seguridad, Redis Enterprise Cloud se implementa en una subred privada a la que se puede acceder desde puntos de conexión públicos y privados. Le recomendamos que conecte las aplicaciones de cliente a Redis en puntos de conexión privados. Si planea utilizar un punto de conexión público, le recomendamos encarecidamente que habilite TLS para cifrar los datos entre sus aplicaciones cliente y Redis Enterprise Cloud.

La metodología de migración de Redis se alinea con la metodología de migración de AWS, que se ilustra en Movilice su organización para acelerar las migraciones a gran escala en el sitio web AWS Prescriptive Guidance.

Automatizar y escalar

Las tareas de configuración del entorno para la migración se pueden automatizar mediante AWS Landing Zone y plantillas de infraestructura como código (IaC) para la automatización y la escalabilidad. Estas cuestiones se analizan en la sección Epics de este patrón.

Tools (Herramientas)

En función de sus requisitos de migración de datos, puede elegir entre una selección de opciones tecnológicas para migrar sus datos a Redis Enterprise Cloud en AWS. En la tabla siguiente se describen estos parámetros.

Herramienta	Description (Descripción)	Ventajas	Desventajas

Exportación e importación de RDB	Los datos de la base de datos de origen (por ejemplo, Redis OSS o Redis Enterprise Software) se exportan en forma de archivos RDB. Si la base de datos se proporciona a través de un clúster de OSS de Redis, exporta cada partición maestro a una RDB. A continuación, importe todos los archivos RDB en un solo paso. Si la base de datos de origen se basa en un clúster de OSS, pero la base de datos de destino no utiliza la API de clúster de OSS, debe cambiar el código fuente de la aplicación para utilizar una biblioteca cliente de Redis estándar. Los requisitos de transformación de datos o las fusiones de bases de datos lógicas requieren un proceso más complejo, que se	• Sencillo. • Funciona con cualquier solución basada en Redis que pueda exportar datos en formato RDB como fuente (incluidos Redis OSS y Redis Enterprise Software). • Logra la coherencia de datos con un proceso sencillo.	• No responde a los requisitos de transformación de datos ni admite las fusiones lógicas de bases de datos. • Consume mucho tiempo para conjuntos de datos más grandes. • La falta de soporte para la migración delta puede provocar un tiempo de inactividad más prolongado.

explica en Fusión lógica de bases de datos más adelante en esta tabla.

Función de replicación de Redis (activa-pasiva)	Puede replicar continuamente los datos de una base de datos de Redis OSS, Enterprise Software o Enterprise Cloud a una base de datos de Redis Enterprise Cloud. Tras la sincronización inicial, la función de replicación de Redis (`ReplicaOf `) realiza una migración delta, lo que significa que prácticamente no se observa ningún tiempo de inactividad de las aplicaciones. La característica de replicación de Redis está diseñada para usarse de forma activa y pasiva. Se supone que el objetivo es pasivo y se vuelve a sincronizar por completo (se vacía y sincroniza desde la base de datos de origen). Por lo tanto, cambiar entre el origen y el destino es algo más complicado.	• Admite la replicación continua (carga de datos inicial seguida de deltas). • Prácticamente no hay tiempo de inactividad (depende del retraso de la replicación). • Logra la coherencia de datos.	• Se prevé que solo un sitio esté activo, por lo que cambiar de un sitio a otro es más complicado. • Admite un máximo de 32 particiones maestras al migrar desde un clúster de OSS.

	Es posible replicar desde un clúster de OSS de Redis a una base de datos estándar de Redis Enterprise Cloud agrupada en clústeres especificando todas las particion es maestras del clúster de OSS como fuentes. Sin embargo, la función de replicaci ón de Redis permite un máximo de 32 bases de datos de origen.		
AWS DMS	Puede usar AWS DMS para migrar datos de cualquier base de datos de origen compatible a un almacén de datos de Redis de destino con un tiempo de inactividad mínimo. Para obtener más información, consulte Uso de Redis como objetivo para AWS DMS en la documenta ción de AWS DMS.	• Soporta la migración de orígenes de datos NoSQL y SQL. • Funciona bien con otros servicios de AWS. • Admite casos de uso de la captura de datos de cambio y migración en tiempo real (CDC, change data capture).	• Los valores clave de Redis no pueden contener caracteres especiales como%. • No admite la migración de datos que contengan caracteres especiales en las filas o en los nombres de los campos. • No es compatibl e con el modo de objetos binarios completamente grandes (LOB).

Combinación lógica de bases de datos	Los requisitos especiales de combinación de bases de datos pueden requerir una solución de migración de datos personalizada. Por ejemplo, es posible que tenga cuatro bases de datos lógicas (`SELECT 0..3`) en Redis OSS, pero tal vez desee utilizar un único punto de conexión de base de datos en lugar de mover los datos a varias bases de datos de Redis Enterprise Cloud. Redis Enterprise no admite bases de datos lógicas seleccionables, por lo que tendría que transformar el modelo de datos físicos de la base de datos de origen. Por ejemplo, puede asignar cada índice de base de datos a un prefijo (`0` a `usr`, `1` a `cmp`, etc.) y, a continuación, utilizar un script de migración o una herramienta de extracción, transform	• Control detallado de la configuración de los datos durante la migración al sistema de destino mediante scripts personalizados.	• Si decide no completar la migración, la reversión puede ser muy difícil, especialmente si los datos más recientes deben devolverse a los sistemas de origen. • El costo de creación puede ser elevado si el objetivo es crear una solución única para una migración única. • Los costos de mantenimiento del código, la infraestructura, el tiempo de desarrollo y otras áreas pueden ser altos si los requisitos de migración cambian con frecuencia.

	ación y carga (ETL) para generar un archivo RDB que, a continuación, podrá importar a la base de datos de destino.

Además, puede utilizar las siguientes herramientas y servicios de AWS.

Herramienta de evaluación y descubrimiento:

- Evaluador de migración

Herramientas de migración de aplicaciones y servidores:

- AWS Application Migration Service

Herramientas de migración de bases de datos:

- Herramienta de conversión de esquemas de AWS (AWS SCT)
- AWS Database Migration Service (AWS DMS)

Herramientas de migración de datos:

- AWS Storage Gateway
- AWS DataSync
- AWS Direct Connect
- AWS Snowball
- Amazon Data Firehose

Soluciones de socios de AWS:

- Socios con competencias en migración de AWS

Epics

Complete las tareas de descubrimiento y evaluación

Tarea	Descripción	Habilidades requeridas
Identifique cargas de trabajo.	Identifique las cargas de trabajo candidatas adecuadas que desea migrar. Tenga en cuenta lo siguiente antes de elegir una carga de trabajo para la migración: • ¿Cuál es el valor empresarial de migrar o no migrar esta carga de trabajo? • ¿Existe un plan de contingencia si esta carga de trabajo no se migra correctamente al sistema de destino? Lo ideal es elegir una carga de trabajo que tenga el máximo impacto empresarial con el mínimo de riesgos involucrados. Mantenga el proceso general iterativo y migre en pequeños incrementos.	Arquitecto de datos, promotor empresarial y patrocinador de proyectos de migración
Identifique los orígenes y los requisitos de datos; diseñe un modelo de datos.	Redis organiza un taller para acelerar el descubrimiento y definir la planificación de la migración para el proyecto. Como parte de este taller, los equipos de Redis identifican los orígenes de datos y los	Arquitecto de soluciones de Redis

Tarea	Descripción	Habilidades requeridas
	requisitos del modelo de datos fuente, y analizan cómo se pueden remodelar en Redis Enterprise Cloud. El equipo de migración de Redis (servicios profesionales) realiza un ejercicio detallado de diseño del modelo de datos con su organización. Como parte de este ejercicio, el equipo de Redis: • Identifica las estructuras de datos de Redis objetivo. • Define la estrategia de mapeo de datos. • Documenta el enfoque y las recomendaciones de migración. • Revisa y finaliza el modelo de datos con las partes interesadas.	

Tarea	Descripción	Habilidades requeridas
Identificar las características de la base de datos de origen.	Identifique el producto de Redis que se utiliza en los entornos de origen y destino. Por ejemplo: • ¿La base de datos de origen es una base de datos de clúster de OSS, una base de datos de Redis independiente o una base de datos de Redis Enterprise? • ¿La base de datos de destino será una base de datos estándar de Redis Enterprise o una base de datos compatible con OSS Cluster? • ¿Cuáles son las implicaciones relacionadas con el código fuente de la aplicación?	Arquitecto de datos
Recopile el SLA actual del sistema y otras métricas de tamaño.	Determine los acuerdos de nivel de servicio (SLAs) actuales expresados en términos de rendimiento (operaciones por segundo), latencia, tamaño total de memoria por base de datos y requisitos de alta disponibilidad (HA).	Arquitecto de datos

Tarea	Descripción	Habilidades requeridas
Identifique las características del sistema de destino.	Determine las respuestas a estas preguntas: • ¿Cuántos datos se deben migrar? • ¿Cuánto tiempo demora migrar la cantidad de datos dada? • ¿Cuáles son los requisitos de tiempo de inactividad para la migración? ¿Es aceptable que su servicio o aplicación no estén disponibles durante un período específico? Si es así, ¿durante cuánto tiempo? • ¿Qué grado de coherencia deben tener los datos migrados? ¿Puede la base de datos de destino estar en un estado ligeramente incoherente (desactualizada)? • ¿Es necesario transformar los datos antes de cargarlos en la base de datos de destino? (Por ejemplo, es posible que desee convertir índices de base de datos seleccionables en prefijos antes de la migración). • ¿Se puede acceder a la base de datos de origen	Arquitecto de datos, arquitecto de soluciones de Redis (opcional)

Tarea	Descripción	Habilidades requeridas
	desde el host de la base de datos de destino (por ejemplo, desde una VPC homóloga o desde un punto de conexión público mediante cifrado)? • Realice un ejercicio de dimensionamiento de datos y tamaño de clústeres de Redis con un arquitecto técnico de Redis. • Identifique los requisito s de red, los requisito s de infraestructura, las versiones de software y las licencias de software, y adquiera cualquier componente antes de la migración. • ¿Hay algún problema de seguridad relacionado con la transferencia de estos datos?	

Tarea	Descripción	Habilidades requeridas
Identifique las dependencias.	Identifique las dependencias ascendentes y descendentes del sistema actual que se va a migrar. Asegúrese de que el trabajo de migración esté alineado con otras migracion es de sistemas dependientes. Por ejemplo, si planea migrar otras aplicaciones empresari ales de las instalaciones a la nube de AWS, identifique estas aplicaciones y alinéelas en función de los objetivos, los plazos y las partes interesad as del proyecto.	Arquitecto de datos, arquitecto empresarial

Tarea	Descripción	Habilidades requeridas
Identifique las herramientas de migración.	En función de sus requisitos de migración de datos (como los datos de origen o los requisitos de tiempo de inactividad), puede utilizar cualquiera de las herramientas descritas anteriormente en la sección Herramientas. Además, puede utilizar: • Replicación bidireccional (activa-activa) mediante la implementación de CRDB. • Secuencias de export/import comandos personalizadas (por ejemplo, mediante `DUMP/RESTORE` comandos). • export/import Herramientas adicionales y herramientas de ayuda ECstats2, como RIOT o ETL. • Herramientas de IaC como Terraform o plantillas de AWS CloudFormation .	Arquitecto de soluciones de migración, arquitecto de soluciones de Redis
Cree un plan de contingencia.	Establezca un plan de contingencia para dar marcha atrás en caso de que surjan problemas durante la migración.	Gestión de proyectos, equipos técnicos, incluido el arquitecto

Complete las tareas de seguridad y cumplimiento

Tarea	Descripción	Habilidades requeridas
Proteja la consola de administración de Redis.	Para proteger la consola de administración, siga las instrucciones de la documentación de Redis.	Administrador de la infraestructura de TI
Proteja la base de datos de Redis.	Consulte las siguientes páginas de la documentación de Redis para: • Definir control de acceso basado en roles • Defina la seguridad de la red. • Habilite TLS.	
Proteja la nube de Redis. APIs	Al habilitar la API, puede administrar las claves de API de todos los propietarios de su cuenta de Redis Cloud. Para obtener una descripción general de las funciones de seguridad de la API, consulte la documentación de autenticación de la API en el sitio web de Redis.	Administrador de la infraestructura de TI

Configurar el nuevo entorno de

Tarea	Descripción	Habilidades requeridas
Configure un nuevo entorno en AWS.	Esta tarea incluye:	¿Informático o ingeniero DevOps

Tarea	Descripción	Habilidades requeridas

	• Actividades de configuración de AWS Landing Zone. La zona de aterrizaje admite:
	  • Implementaciones con varias cuentas
	  • Base de seguridad mínima
	  • Una forma automatizada de aprovisionar nuevas cuentas con una base de seguridad y requisitos previos de ISV (redes, configuración de seguridad, etc.)
	  • Notificaciones, registro centralizado y supervisión
	• Actividades de configuración del software ISV. Esto incluye las configuraciones que deben incluirse en la migración, como la configuración y los cambios de los productos y las cargas de trabajo.
	• Actividades de IaC, como configurar o personalizar las plantillas de AWS CloudFormation o Terraform.	

Tarea	Descripción	Habilidades requeridas
Implemente la arquitectura de migración.	1. Configure Redis Enterprise Cloud en AWS. 2. Instale herramientas de migración como RIOT o AWS DMS. Consulte la sección Herramientas para ver una lista de las herramientas disponibles. 3. Establezca la conectividad entre las capas de aplicación, migración y base de datos. 4. Cree una carga de trabajo de muestra que pueda fluir por cada capa y migrar un conjunto pequeño de datos de muestra. Ahora está preparado para ejecutar los procesos de migración de datos reales y probarlos.	¿Informático o DevOps ingeniero

Configurar redes

Tarea	Descripción	Habilidades requeridas
Establezca la conectividad.	Establezca la conectividad entre la infraestructura en las instalaciones y los recursos de la nube de AWS. Utilice los grupos de seguridad, AWS Direct Connect y otros	¿Informático o DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	recursos para lograr esta funcionalidad. Para obtener más información, consulte Conectar su centro de datos a AWS en el sitio web de AWS.	
Configure las interconexiones con VPC.	Establezca una interconexión de VPC entre la VPC VPCs que ejecuta las aplicaciones empresariales (o las EC2 instancias que ejecutan las herramientas de migración o el servidor de replicación de AWS DMS) y la VPC que ejecuta Redis Enterprise Cloud. Para obtener instrucciones, consulte Comenzar con Amazon VPC en la documentación de Amazon VPC y Habilitar el emparejamiento de VPC en la documentación de Redis.	¿Ingeniero o de TI DevOps

Migración de datos

Tarea	Descripción	Habilidades requeridas
Elija una herramienta de migración de datos.	Consulte la tabla de la sección Herramientas para ver las descripciones, ventajas y desventajas de estas herramientas: • Exportación e importación de RDS	Arquitecto de soluciones de migración

Tarea	Descripción	Habilidades requeridas
	• Función de replicación de Redis (`ReplicaOf `) • AWS DMS • Combinación lógica de bases de datos Las filas siguientes describen las tareas de migración de datos asociadas a cada herramienta.	

Tarea	Descripción	Habilidades requeridas
Opción 1: utilice la exportación e importación de RDB.	1. Desconectar la fuente: detenga el tráfico en la base de datos de origen (por ejemplo, desconect ando las aplicaciones empresariales). 2. Exportar: exporte los datos de la base de datos de origen como un archivo RDB. 3. Etapa: cargue los datos en una ubicación a la que puedan acceder las instancias de Redis Enterprise Cloud en AWS (por ejemplo, puede cargarlos en un bucket de S3 o en un servidor FTP). 4. Importación: importe los archivos RDB (enumerán dolos todos en un solo paso de importación) a su base de datos de destino de Redis Enterprise Cloud. 5. Transición: vaya a la base de datos de destino (por ejemplo, conectando su aplicación, conéctese a ella). Para obtener más información, consulte la documentación de Redsis.	Arquitecto de soluciones de migración, arquitecto de soluciones de Redis

Tarea	Descripción	Habilidades requeridas
Opción 2: utilice la caracterí stica de replicación de Redis (activa-pasiva).	1. Conectar base de datos: establezca un enlace de `ReplicaOf` entre las bases de datos de origen y destino. 2. Ejecute una sincronización inicial: espere hasta que se complete la sincronización inicial entre las bases de datos de origen y destino. 3. Desconectar la fuente: detenga el tráfico en la base de datos de origen (por ejemplo, desconect ando la aplicación). 4. Ejecute la replicación delta: espere hasta que la replicación delta se replique en la base de datos de destino. 5. Transición: vaya a la base de datos de destino (por ejemplo, conectando su aplicación a ella). 6. Eliminar: elimine el enlace de `ReplicaOf` entre las bases de datos de origen y destino. Para obtener más información, consulte la documentación de Redsis.	Arquitecto de soluciones de migración, arquitecto de soluciones de Redis

Tarea	Descripción	Habilidades requeridas
Opción 3: utilice AWS DMS.	1. Configurar una instancia de replicación de AWS DMS: esta instancia realiza todos los procesos de migración. Para obtener instrucciones: Trabajar con una instancia de replicación de AWS DMS en la documentación de AWS DMS. 2. Defina la base de datos de origen: defina el punto de conexión de origen. Pruebe la conectividad entre el punto de conexión de origen y el servidor de replicación de AWS DMS. Para obtener instrucciones: Cómo crear puntos de enlace de origen y destino en la documentación de AWS DMS. 3. Configurar la base de datos de destino: configure Redis Enterprise Cloud en AWS y configure la base de datos a la que se va a migrar. 4. Defina la base de datos de destino: defina el punto de conexión de destino. Asegúrese de que la Interconexión de VPC esté establecida entre la VPC en la que se ejecuta AWS DMS y la VPC que aloja	Arquitecto de soluciones de migración, arquitecto de soluciones de Redis

Tarea	Descripción	Habilidades requeridas
	Redis Enterprise Cloud en AWS. Pruebe la conectividad entre el servidor de replicación de AWS DMS y la base de datos de destino. 5. Cree una tarea de AWS DMS: cree una tarea o un conjunto de tareas para definir las tablas y los procesos de replicación que desee utilizar para migrar los datos. Para obtener instrucciones: Trabajar con las tareas de AWS DMS en la documentación de AWS DMS. 6. Migrar: migre los datos ejecutando la tarea de AWS DMS. 7. Transición: vaya a la base de datos de destino (por ejemplo, conectando su aplicación a ella).	
Opción 4: utilice la combinación lógica de bases de datos.	Esta opción implica el uso de un script de migración o una herramienta ETL que pueda transformar el modelo de datos físicos de la base de datos de origen y generar un archivo RDB. Los servicios profesionales de Redis pueden ayudar con este paso, si es necesario.	Arquitecto de soluciones de migración, arquitecto de soluciones de Redis

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Alinee los plazos y los objetivos de la gestión de proyectos.	Alinee los objetivos, hitos y plazos del proyecto de migración de la capa de aplicación con los del proyecto de migración de datos de Redis.	Administración de proyectos
Alinee las actividades de prueba.	Después de migrar y modernizar la capa de aplicaciones en la nube de AWS, dirija la capa de aplicaciones a la recién migrada Redis Enterprise Cloud en AWS para realizar pruebas.	Testeo

Test

Tarea	Descripción	Habilidades requeridas
Implemente planes de pruebas.	Ejecute las rutinas de migración de datos y los scripts que se desarrollaron durante la fase de implement ación en un entorno de pruebas, según los requisitos de las pruebas, en su sitio.	Testeo
Prueba de calidad de datos de prueba.	Prueba de la calidad de los datos después de migrarlos.	Testeo
Pruebe la funcionalidad.	Pruebe las consultas de datos y la capa de aplicación para	Testeo

Tarea	Descripción	Habilidades requeridas
	asegurarse de que la aplicación funciona al mismo nivel que en el sistema de origen.	

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Tome la decisión de transición.	Una vez finalizadas todas las pruebas a nivel de aplicación y base de datos, el equipo de liderazgo ejecutivo y las partes interesadas toman la decisión final sobre si pasarán al nuevo entorno de AWS en función de los resultados finales confirmados por los equipos de pruebas.	La gestión de proyectos, campeona del mundo empresarial
Transición a la nube de AWS.	Cuando haya confirmado que todo está en su lugar, dirija la capa de aplicación a los datos recién migrados y dirija los clientes a la nueva capa de aplicaciones que se está ejecutando en función del nuevo sistema Redis Enterprise Cloud en AWS.	DevOps Ingeniero o informático, arquitecto de datos, arquitecto de soluciones de migración, arquitecto de soluciones de Redis

Recursos relacionados

Recursos de Redis

- Documentación de Redis Enterprise Cloud

- Herramienta RIOT (GitHub repositorio)
- Terraform Provider (descargar)

Recursos de AWS

- Migraciones de demostración
- Soluciones de socios de AWS
- Documentación
- Publicaciones de blog
- Libros blancos
- Tutoriales y videos
- Migración de datos a la nube de AWS
- Recomendaciones de AWS

Información adicional

Para conocer los requisitos de seguridad estándar para la migración de cargas de trabajo de Redis a la nube de AWS, consulte Best Practices for Security, Identity, and Compliance en el sitio web de AWS y Redis Trust Center en el sitio web de Redis.

Migración de SAP HANA a AWS mediante SAP HSR con el mismo nombre de host

Pradeep Puliyampatta, Amazon Web Services

Resumen

Las migraciones de SAP HANA a Amazon Web Services (AWS) pueden llevarse a cabo de múltiples maneras, como copia de seguridad y restauración, exportación e importación y replicación del sistema SAP HANA (HSR). La selección de una opción concreta dependerá de la conectividad de red entre las bases de datos SAP HANA de origen y destino, el tamaño de la base de datos de origen, las consideraciones de tiempo de inactividad y otros factores.

La opción HSR de SAP para migrar las cargas de trabajo de SAP HANA a AWS funciona adecuadamente cuando hay una red estable entre los sistemas de origen y destino, y cuando toda la base de datos (instantánea de replicación de la base de datos de SAP HANA) se puede replicar por completo en 1 día, según lo estipulado por SAP en los requisitos de rendimiento de la red para SAP HSR. Los requisitos de tiempo de inactividad de este enfoque se limitan a realizar la adquisición en el AWS entorno de destino, el respaldo de la base de datos de SAP HANA y las tareas posteriores a la migración.

SAP HSR admite el uso de diferentes nombres de host (nombres de host asignados a diferentes direcciones IP) para el tráfico de replicación entre los sistemas principal o de origen y secundario o de destino. Puede hacerlo definiendo esos conjuntos específicos de nombres de host en la sección `[system_replication_hostname_resolution]`, en `global.ini`. En esta sección, todos los hosts de los sitios principal y secundario deben estar definidos en cada host. Para ver los pasos de configuración detallados, consulte la documentación de SAP.

Una conclusión clave de esta configuración es que los nombres de host del sistema principal deben ser diferentes de los nombres de host del sistema secundario. De lo contrario, se pueden producir los siguientes errores.

- `"each site must have a unique set of logical hostnames"`
- `"remoteHost does not match with any host of the source site. All hosts of source and target site must be able to resolve all hostnames of both sites correctly"`

Sin embargo, la cantidad de pasos posteriores a la migración se puede reducir utilizando el mismo nombre de host de SAP HANA DB en el entorno de destino. AWS

Este patrón proporciona una solución alternativa para usar el mismo nombre de host en los entornos de origen y destino cuando se emplea la opción SAP HSR. Con este patrón, puede usar la opción de cambio de nombre de host de SAP HANA. Debe asignar un nombre de host temporal a la base de datos de SAP HANA de destino para facilitar la exclusividad del nombre de host de SAP HSR. Una vez que la migración complete la adquisición del entorno SAP HANA de destino, puede volver a convertir el nombre de host del sistema de destino en el nombre de host del sistema de origen.

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- Una nube privada virtual (VPC) con un punto de conexión de red privada virtual (VPN) o router.
- AWS Client VPN o AWS Direct Connect configurado para transferir archivos del origen al destino.
- Bases de datos de SAP HANA, tanto en el entorno de origen como en el de destino. El nivel de parche de la base de datos SAP HANA de destino debe ser igual o superior al nivel de parche de la base de datos SAP HANA de origen, dentro de la misma edición de la plataforma SAP HANA. Por ejemplo, no es posible configurar la replicación entre los sistemas HANA 1.0 y HANA 2.0. Para obtener más información, consulte la pregunta 15 en la nota de SAP: 1999880 — Preguntas frecuentes: replicación del sistema SAP HANA.
- Servidores de aplicaciones SAP en el entorno de destino.
- Volúmenes de Amazon Elastic Block Store (Amazon EBS) en el entorno de destino.

Limitaciones

En la siguiente lista de documentos de SAP se describen los problemas conocidos relacionados con esta solución alternativa, incluidas las limitaciones de la organización dinámica por niveles y las migraciones de escala horizontal de SAP HANA:

- 2956397 – Fallo al cambiar el nombre del sistema de base de datos SAP HANA
- 2222694 – Al intentar cambiar el nombre del sistema HANA, aparece el siguiente error: “Los archivos de origen no pertenecen al usuario sidadm original (uid = xxxx)”
- 2607227 – hdblcm: register_rename_system: No se pudo cambiar el nombre de la instancia de SAP HANA

- 2630562 – Error al cambiar el nombre de host de HANA, HANA no se inicia
- 2935639 – sr_register no usa el nombre de host especificado en system_replication_hostname_resolution en la sección global.ini
- 2710211 – Error: el sistema de origen y el sistema de destino tienen nombres de host lógicos superpuestos
- 2693441 – No se pudo cambiar el nombre de un sistema SAP HANA debido a un error
- 2519672 – HANA principal y secundario tienen sistemas diferentes (PKI, SSFS, datos y claves) o no se pueden comprobar
- 2457129 – No está permitido cambiar el nombre del host del sistema SAP HANA cuando la estratificación dinámica forma parte del entorno
- 2473002 – Uso de la replicación del sistema HANA para migrar un sistema de escala horizontal (SAP no impone restricciones a la hora de usar este enfoque de cambio de nombre de host para sistemas SAP HANA con capacidad de ampliación. Sin embargo, el procedimiento debe repetirse en cada host individual. Este enfoque también tiene otras limitaciones de migración de escala horizontal).

Versiones de producto

- Esta solución se aplica a las ediciones 1.0 y 2.0 de la plataforma de base de datos SAP HANA.

Arquitectura

Configuración de origen

Base de datos SAP HANA instalada en el entorno de origen. Todas las conexiones del servidor de aplicaciones e interfaces de base de datos de SAP usan el mismo nombre de host para las conexiones de los clientes. El siguiente diagrama muestra el ejemplo del nombre de host de origen `hdbhost` y su dirección IP correspondiente.

Configuración de destino

El entorno de Nube de AWS destino utiliza el mismo nombre de host para ejecutar una base de datos de SAP HANA. El entorno de destino en AWS incluye lo siguiente:

- Base de datos SAP HANA

- Servidores de aplicaciones SAP
- Volúmenes de EBS

Configuración intermedia

En el siguiente diagrama, el nombre de host del entorno de AWS destino se renombra temporalmente `temp-host` para que los nombres de host del origen y el de destino sean únicos. Una vez que la migración complete la adquisición en el entorno de destino, se cambia el nombre de host virtual del sistema de destino por el nombre original, `hdbhost`.

La configuración intermedia incluye una de las siguientes opciones:

- AWS Client VPN con un punto final Client VPN
- Direct Connect conectándose a un router

Los servidores de aplicaciones SAP en el entorno de AWS destino se pueden instalar antes de la configuración de la replicación o después de la adquisición. Sin embargo, instalar los servidores de aplicaciones antes de configurar la replicación puede ayudar a reducir el tiempo de inactividad durante la instalación, configurar la alta disponibilidad y realizar copias de seguridad.

Tools (Herramientas)

Servicios de AWS

- AWS Client VPNes un servicio de VPN gestionado y basado en clientes que le permite acceder de forma segura a AWS los recursos y recursos de su red local.
- AWS Direct Connectconecta su red interna a una Direct Connect ubicación a través de un cable Ethernet de fibra óptica estándar. Con esta conexión, puede crear interfaces virtuales directamente con las públicas Servicios de AWS, sin tener en cuenta a los proveedores de servicios de Internet en su ruta de red.
- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento a nivel de bloque para utilizarlos con instancias de Amazon Elastic Compute Cloud (Amazon EC2). Los volúmenes de EBS se comportan como dispositivos de bloques sin formatear. Puede montar estos volúmenes como dispositivos en sus instancias.

Otras herramientas

- Servidores de aplicaciones SAP: los servidores de aplicaciones SAP proporcionan a los programadores una forma de expresar la lógica empresarial. El servidor de aplicaciones SAP realiza el procesamiento de datos en función de la lógica empresarial. Los datos reales se almacenan en una base de datos, que es un componente independiente.
- SAP HANA cockpit y SAP HANA Studio: tanto SAP HANA cockpit como SAP HANA Studio proporcionan una interfaz administrativa para la base de datos de SAP HANA. En SAP HANA Studio, la consola de administración de SAP HANA es la vista del sistema que proporciona el contenido relevante para administrar la base de datos de SAP HANA.
- Replicación del sistema SAP HANA: la replicación del sistema SAP HANA (SAP HSR) es el procedimiento estándar que proporciona SAP para replicar las bases de datos de SAP HANA. Los ejecutables necesarios para SAP HSR forman parte del propio kernel del servidor SAP HANA.

Epics

Prepare el entorno de origen y destino

Tarea	Descripción	Habilidades requeridas
Instale y configure las bases de datos de SAP HANA.	En los entornos de origen y destino, asegúrese de que la base de datos de SAP HANA esté instalada y configurada de acuerdo con las prácticas recomendadas de SAP HANA. Para obtener más información, consulte SAP HANA en AWS.	Administrador de SAP Basis
Mapee la dirección IP.	En el entorno de destino, asegúrese de que el nombre de host temporal esté asignado a una dirección IP interna. 1. Para asignar una IPv4 dirección secundaria a la	Administración de AWS

Tarea	Descripción	Habilidades requeridas
	EC2 instancia en la consola de administración de AWS, vaya a Instancia EC2, Acciones, Redes, Administrar dirección IP y Asignar nueva dirección IP. 2. Para asignar la misma dirección al adaptador de EC2 red (NIC) del sistema operativo que al usuario root, ejecute el comando y `ip addr add <IP>/32 dev eth0` `<IP>` sustitúyalo por la dirección IP del paso 1.	
Resuelva los nombres de host de destino.	En la base de datos secundaria de SAP HANA, confirme que ambos nombres de host (`hdbhost` y `temp-host`) están resueltos para las redes de replicación de SAP HANA actualizando los nombres de host correspondientes en el archivo `/etc/hosts` .	Administración de Linux
Realice copias de seguridad de las bases de datos SAP HANA de destino.	Use SAP HANA Studio o SAP HANA cockpit para realizar copias de seguridad en las bases de datos de SAP HANA.	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
Intercambie los certificados de PKI del sistema.	(Solo se aplica a SAP HANA 2.0 y versiones posteriores) Intercambie los certificados en el almacén seguro de infraestructura de clave pública (PKI) del sistema, en el almacén del sistema de archivos (SSFS) entre las bases de datos principal y secundaria. Para obtener más información, consulte la nota 2369981 de SAP: Pasos de configuración necesarios para la autenticación con la replicación del sistema SAP HANA.	Administrador de SAP Basis

Cambie el nombre de la base de datos SAP HANA de destino

Tarea	Descripción	Habilidades requeridas
Detenga las conexiones con los clientes de destino.	En el entorno de destino, apague los servidores de aplicaciones de SAP y otras conexiones de clientes.	Administrador de SAP Basis
Cambie el nombre de la base de datos de SAP HANA de destino por el nombre de host temporal.	1. Como usuario raíz, cambie el nombre del host de la base de datos SAP HANA de destino por el nombre de host temporal usando el `hdblcm` residente. `root $> cd /hana/shared/<SID/hdblcm`	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	`root $> ./hdblcm` 2. Seleccione Opciones 9 `| rename_system | Rename the SAP HANA Database System`. 3. Proporcione el nombre nuevo: `temp-host` . 4. Puede validar otras opciones según sea necesario. Sin embargo, asegúrese de no confundir el cambio de nombre del host con un cambio de SID (Nota de SAP 2598814: hdblcm: error al cambiar el nombre del SID). La detención y el inicio de la base de datos de SAP HANA se controlarán mediante `hdblcm`.	
Asigne redes de replicación.	En el archivo `global.ini` del sistema de origen, bajo el encabezado `[system_replication_hostname_resolution]` , proporcione los detalles de la red de replicación de origen y destino. A continuación, copie las entradas en el archivo `global.ini` del sistema de destino.	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
Habilite la replicación en el servidor principal.	Para habilitar la replicación en la base de datos de SAP HANA de origen, ejecute el siguiente comando. `hdbnsutil -sr_enable --name=siteA`	Administrador de SAP Basis

Registre la base de datos de SAP HANA de destino como sistema secundario.	Para registrar la base de datos de SAP HANA de destino como sistema secundario de origen para SAP HSR, elija la replicación asíncrona.
	`(sid)adm $> HDB stop`
	`(sid)adm $> hdbnsutil -sr_register –name=siteB –remotehost=hdbhost /`
	`--remoteInstance=00 –replicationMode=async –operationMode=logreplay`
	`(sid)adm $> HDB start`
	También puede seleccionar la opción de registro `–online`. En ese caso, no necesita detener e iniciar la base de datos de SAP HANA.
		Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas

Valide la sincronización.	En la base de datos de SAP HANA de origen, compruebe que todos los registros se apliquen al sistema de destino (ya que se trata de una replicación asíncrona).
	
	Para verificar la replicaci ón, ejecute los siguientes comandos en el entorno de origen.
	
	`(sid)adm $> cdpy`
	`(sidadm $> python systemReplicationStatus.py`
		Administrador de SAP Basis

Cierre la aplicación SAP de origen y la base de datos de SAP HANA.	Durante la transición a la migración, apague el sistema de origen (la aplicación SAP y la base de datos SAP HANA).	Administrador de SAP Basis
Realice la adquisición del destino.	Para realizar la adquisición del destino en AWS, ejecute el comando `hdbnsutil -sr_takeover` .	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
En la base de datos de SAP HANA de destino, desactive la replicación.	Para borrar los metadatos de la replicación, detenga la replicación en el sistema de destino ejecutando el comando `hdbnsutil -sr_disable` . **Note** Según la Nota de SAP 2693441: No se pudo cambiar el nombre de un sistema SAP HANA debido a un error.	Administrador de SAP Basis
Realice una copia de seguridad de la base de datos SAP HANA de destino.	Una vez que la adquisición se haya realizado correctamente, recomendamos realizar una copia de seguridad completa de la base de datos de SAP HANA.	Administrador de SAP Basis

Revierta al nombre de host original en el sistema de destino

Tarea	Descripción	Habilidades requeridas
Revierta al nombre de host original el nombre de host de SAP HANA DB.	1. Para revertir el nombre de host de la base de datos de SAP HANA de destino al nombre de host virtual original, use `hdblcm` residente.	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas

	`root $> cd /hana/shared/<SID>/hdblcm`
	`root $> ./hdblcm`
	2. Seleccione Opciones 9 `| rename_system | Rename the SAP HANA Database System`.
	3. Proporcione el nombre nuevo: `hdbhost`.
	
	Puede validar otras opciones según sea necesario. Sin embargo, asegúrese de no confundir el cambio de nombre del host con un cambio de SID (Nota de SAP 2598814: hdblcm: error al cambiar el nombre del SID).	

Ajuste hdbuserstore.	Adapte los detalles de `hdbuserstore` apuntando a los detalles de la fuente `schema/user` . Para ver los pasos detallados, consulte la documentación de SAP. Para validar este paso, ejecute el comando `R3trans -d`. El resultado debe reflejar una conexión correcta a la base de datos de SAP HANA.	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
Inicie las conexiones con los clientes.	En el entorno de destino, inicie los servidores de aplicaciones de SAP y otras conexiones de clientes.	Administrador de SAP Basis

Recursos relacionados

Referencias de SAP

SAP actualiza con frecuencia las referencias de documentación de SAP. Para mantenerse al día, consulte la Nota de SAP 2407186: Guías prácticas y documentos técnicos sobre la alta disponibilidad de SAP HANA.

Notas adicionales de SAP

- 2550327 – Cómo cambiar el nombre de un sistema SAP HANA
- 1999880 – Preguntas frecuentes: replicación del sistema SAP HANA
- 2078425 – Nota de solución de problemas para la herramienta de gestión del ciclo de vida de la plataforma SAP HANA hdblcm
- 2592227 – Cambio del sufijo FQDN en sistemas HANA
- 2048681 – Realización de tareas de administración de ciclo de vida de la plataforma SAP HANA en sistemas con varios hosts sin credenciales de SSH o root

Documentos de SAP

- System Replication Network Connection
- Resolución del nombre de host para la replicación del sistema

AWS referencias

- Migración de SAP HANA de otras plataformas a AWS

Información adicional

Los cambios realizados por `hdblcm` como parte de la actividad de cambio de nombre de host se consolidan en el siguiente registro detallado.

Migre el grupo de disponibilidad Always On de Microsoft SQL Server mediante AWS Transform MGN

Sreenivas Nettem, Bharath Kumar Pammi Ramesh, Anantharaman Seshadri y Gireesh Sreekantan, Amazon Web Services

Resumen

AWS Transform MGN (AWS MGN) es la herramienta preferida para realojar los entornos existentes en el sistema Nube de AWS, lo que permite a los clientes alejarse de los centros de datos locales. Este patrón describe el proceso de uso de AWS MGN para migrar clústeres de Windows con grupos de disponibilidad Always On de Microsoft SQL Server.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.
- Un papel AWS Identity and Access Management (IAM) en la orquestación de AWS MGN.
- Acceso a servidores de bases de datos de origen (grupo de disponibilidad de SQL Server Always On).
- Active Directory en una AWS landing zone para conservar los nombres DNS.
- Una subred provisional con comunicación de red cerrada con Active Directory.
- Subredes de destino que pueden comunicarse con Active Directory.
- Dos direcciones IP reservadas para el clúster de Windows en una subred de destino (una en cada zona de disponibilidad).
- Dos direcciones IP reservadas para el oyente de SQL Always On en una subred de destino (una en cada zona de disponibilidad).

Versiones de producto

- Windows Server 2012 o posterior
- SQL Server 2012 o posterior

Arquitectura

Pila de tecnología de origen

Grupo de disponibilidad de Microsoft SQL Server Always On del clúster de Microsoft Windows (máquina virtual o física en las instalaciones)

Pila de tecnología de destino

Instancia de Windows de Amazon EC2

Arquitectura de destino

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- AWS Transform MGNle ayuda a realojar (levantar y trasladar) las aplicaciones a una ubicación Nube de AWS sin cambios y con un tiempo de inactividad mínimo.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.

Otras herramientas

- Microsoft SQL Server Management Studio (SSMS) es una herramienta para administrar SQL Server, que incluye el acceso, la configuración y la administración de los componentes de SQL Server.

Prácticas recomendadas

Para AWS MGN, consulte las prácticas recomendadas para. AWS Transform MGN

Epics

Preparación de la cuenta de destino

Tarea	Descripción	Habilidades requeridas
Inicialice MGN AWS .	Inicialice AWS MGN en el objetivo. Región de AWS De este modo, se crean las políticas y los roles de IAM necesarios. Para obtener más información, consulte Inicializar MGN con la consola.	Administrador de la nube
Cree plantillas de replicación y lanzamiento.	Configure las plantillas de replicación y lanzamiento para usarlas con AWS MGN. Para obtener más información, consulte Configuración de las plantillas en la AWS documentación.	Administrador de la nube
Permita los puertos de comunicación.	Para habilitar las comunicaciones de red para AWS MGN, permita el tráfico a través de los puertos TCP 443 y 1500. Para obtener más información, consulte los requisitos de red para MGN en la AWS documentación.	Administrador de red, administrador de la nube

Preparación del servidor de origen

Tarea	Descripción	Habilidades requeridas
Compruebe los requisitos AWS previos de MGN.	Compruebe que los servidores de origen cumplen los	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	requisitos previos para la instalación del agente AWS MGN. Para obtener más información, consulte los requisitos de instalación en la AWS documentación.	
Instale el agente AWS MGN.	Instale el agente AWS MGN en los servidores de origen. Durante la instalación, elija el Región de AWS lugar al que se migrarán los servidores. Tras la instalación, el agente se comunica con el servicio e inicia la replicación. Para obtener más información, consulte Instalación del agente de AWS replicación en servidores Windows.	Ingeniero de migraciones
Compruebe el estado del servidor de origen.	En la consola AWS MGN, compruebe el estado de los servidores de origen. Cuando comience la replicación, los servidores muestran Listo para la prueba. Si encuentra algún error, consulte Solución de errores de comunicación en la documentación de AWS MGN.	Administrador de la nube, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Optimice la configuración de replicación.	Los clústeres de SQL Always On utilizan una alta replicación I/O sincrónica del servidor principal al servidor secundario. Para optimizar la replicación y evitar retrasos, utilice un servidor de replicación dedicado para cada servidor de SQL Always On. Si la base de datos tiene un tamaño superior a 5 TB, considere la posibilidad de elegir un tamaño de instancia de servidor de replicación superior, como m5.large, en lugar de la opción t3.small predeterminada.	Administrador de la nube, ingeniero de migraciones
Actualice la plantilla de lanzamiento.	Actualice la configuración de lanzamiento y elija subredes para los servidores de SQL Always On. Los servidores de clúster SQL Always On están repartidos en diferentes ubicaciones Zonas de disponibilidad de AWS para ofrecer una alta disponibilidad.	Ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
Actualice la configuración de lanzamiento.	En función de sus requisitos de tamaño y rendimiento, actualice el tipo de instancia y input/output las operaciones por segundo (IOPS) en la configuración de lanzamiento. (Opcional) Elija una interfaz de red elástica existente en la configuración de lanzamiento.	Ingeniero de migraciones, líder de migración

Prueba de la transición

Tarea	Descripción	Habilidades requeridas
Verifique los servidores de origen.	En la consola AWS MGN, verifica que el estado del servidor de origen sea Listo para la prueba.	Administrador de la nube, ingeniero de migraciones
Lance las instancias de prueba.	1. Lance las instancias de prueba y verifique en la consola de Amazon EC2 que se superen las comprobaciones automatizadas. 2. Seleccione y lance las instancias de prueba para el servidor de testigo. 3. Compruebe que puede iniciar sesión en los servidores a través de la consola AWS MGN.	Administrador de la nube, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	4. Seleccione los servidores de clúster de SQL Always On y lance las instancias de prueba juntas.	
Pruebe la conectividad y la integridad de la base de datos.	Pruebe la conectividad y la integridad de la base de datos de las instancias de prueba. A continuación, marque los servidores de origen como Listos para la transición en la AWS consola MGN.	Administrador de la nube, ingeniero de migraciones

Pre-migration tareas

Tarea	Descripción	Habilidades requeridas
Pruebe la integridad de la base de datos.	Esto ayuda a garantizar que no haya problemas de integridad de la base de datos en el origen antes de la migración. Ejecute `DBCC CHECKDB` y especifique `WITH_PHYSICAL_ONLY` . Si se ejecuta esta comprobación sin `WITH_PHYSICAL_ONLY` , se pueden producir problemas de rendimiento en el origen. Para mantener la integridad de la base de datos, ejecute una comprobación completa semanal de la base de datos.	Ingeniero de datos, Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Estos comandos comprueban la integridad física y lógica de la base de datos mediante la detección de posibles problemas de corrupción. La comprobación verifica la estructura de la base de datos, como las páginas, las filas, los índices y las tablas del sistema.	
Pruebe las conexiones a los servidores vinculados.	Pruebe las conexiones entre todos los servidores existentes y documente su estado. Esto ayuda a garantizar que los servidores vinculados funcionen según lo previsto tras la migración.	Ingeniero de datos, Administrador de base de datos
Verifique las copias de seguridad.	Confirme la integridad de las copias de seguridad de origen.	Ingeniero de datos, Administrador de base de datos

AWS transición a MGN

Tarea	Descripción	Habilidades requeridas
Detenga los servicios de clúster y de SQL Server.	Detenga los servicios de clúster de SQL Server y Microsoft en todos los nodos de clústeres de SQL.	Administrador de base de datos, ingeniero de migraciones
Verifique los servidores.	En la consola AWS MGN, compruebe que el estado de los servidores de origen sea Preparado para la transición y	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	que el estado de la replicación de datos sea Correcto.	
Lance la transición.	1. Inicie la transición AWS MGN para el servidor testigo. 2. Inicie la transición a AWS MGN para las instancias del clúster SQL Always On. 3. Verifique que el estado cambie a Transición en curso. Para obtener más información, consulte Cómo lanzar una instancia transitada en la documentación de MGN. AWS	Ingeniero de migraciones
Pruebe los servidores lanzados.	Inicie sesión en las instancias de Amazon EC2 lanzadas y valide el estado del clúster. Compruebe que los servidores estén en las subredes correctas, que el tamaño de la instancia y la configuración de IOPS sean correctos y que se pueda acceder al servidor de testigo.	Administrador de base de datos, ingeniero de migraciones

Tareas posteriores a la transición de la base de datos

Tarea	Descripción	Habilidades requeridas
Actualice la dirección IP del clúster.	Actualice la dirección IP del clúster para el clúster de Windows mediante las dos direcciones IP reservadas de las subredes de destino. Para obtener más información, consulte Cambiar la dirección IP de una instancia de clúster de conmutación por error.	Administrador de base de datos, ingeniero de migraciones
Actualice las direcciones IP del oyente del grupo de disponibilidad Always On.	1. Abra el administrador de clústeres de conmutación por error. 2. Elija el rol del grupo de disponibilidad Always On. 3. Amplíe el nombre del oyente del grupo de disponibilidad. 4. En el menú contextual (clic con el botón derecho), elija Propiedades de dirección IP. 5. Actualice la dirección IP con la dirección reservada para el oyente en la subred de destino. 6. Conéctese a la instancia principal de SQL Server mediante SSMS y verifique que el oyente Always On utilice ambas IP de subred.	Administrador de base de datos, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Verifique la conexión.	Conéctese al oyente del grupo de disponibilidad Always On mediante SSMS y confirme que la conexión se lleve a cabo correctamente.	Administrador de base de datos, ingeniero de migracion es
Compruebe el estado del grupo de disponibilidad Always On.	1. Vaya a la carpeta Grupos de disponibilidad, abra el menú contextual (clic con el botón derecho) y elija Mostrar panel. 2. Para todas las réplicas, verifique que el estado de sincronización sea Sincronizado.	Administrador de base de datos, ingeniero de migracion es
Comprobación del registro de errores.	Abra el registro de errores y verifique los errores notificad os en la instancia de SQL Server. Asegúrese de que la recuperación se haya completado en todas las bases de datos.	Administrador de base de datos, ingeniero de migracion es
Pruebe los servidores vinculados.	Pruebe la conectividad de todos los servidores vinculado s. En caso de problemas de conectividad, asegúrese de que se pueda acceder al servidor y al puerto de destino.	Administrador de base de datos, ingeniero de migracion es

Finalización de la transición

Tarea	Descripción	Habilidades requeridas
Finalice la transición.	Tras validar los clústeres de SQL Always On de destino, finalice la transición a través de la consola MGN. AWS Esto detiene la replicación de datos de los servidores de origen y descarta los datos del servidor de replicación. También elimina el servidor de replicación y sus recursos asociados.	Administrador de la nube, ingeniero de migraciones

Resolución de problemas

Problema	Solución
AWS Solución de problemas de MGN	Para ver los problemas y las soluciones más comunes, consulte las secciones de solución de problemas y preguntas frecuentes de la documentación de AWS MGN.

Recursos relacionados

AWS resources

- Option-1 Realojar (-) AWS Transform MGNAWS
- ¿Qué es? AWS Transform MGN

Recursos de SQL Server

- What is SQL Server Management Studio (SSMS)?

Información adicional

Para conocer los requisitos de seguridad estándar para la migración de cargas de trabajo a Nube de AWS ella, consulte las prácticas recomendadas en materia de seguridad, identidad y cumplimiento en el AWS sitio web.

Migración de SQL Server a AWS mediante grupos de disponibilidad distribuidos

Praveen Marthala, Amazon Web Services

Resumen

Los grupos de disponibilidad Always On de Microsoft SQL Server proporcionan una solución de alta disponibilidad (HA) y recuperación de desastres (DR) para SQL Server. Un grupo de disponibilidad consta de una réplica principal que acepta read/write tráfico y hasta ocho réplicas secundarias que aceptan tráfico de lectura. Un grupo de disponibilidad se configura en un clúster de conmutación por error de Windows Server (WSFC) con dos o más nodos.

Los grupos de disponibilidad distribuida Always On de Microsoft SQL Server proporcionan una solución para configurar dos grupos de disponibilidad independientes entre dos grupos de disponibilidad independientes WFSCs. Los grupos de disponibilidad que forman parte del grupo de disponibilidad distribuida no tienen que estar en el mismo centro de datos. Un grupo de disponibilidad puede estar en las instalaciones y el otro grupo de disponibilidad puede estar en la nube de Amazon Web Services (AWS) en instancias de Amazon Elastic Compute Cloud (Amazon EC2) en un dominio diferente.

Este patrón describe los pasos para usar un grupo de disponibilidad distribuido para migrar bases de datos de SQL Server locales que forman parte de un grupo de disponibilidad existente a SQL Server con grupos de disponibilidad configurados en Amazon EC2. Si sigue este patrón, puede migrar las bases de datos a la nube de AWS con un tiempo de inactividad mínimo durante la transición. Las bases de datos están altamente disponibles en AWS inmediatamente después de la transición. También puede usar este patrón para cambiar el sistema operativo subyacente de local a AWS y, al mismo tiempo, mantener la misma versión de SQL Server.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- AWS Direct Connect o Site-to-Site VPN de AWS
- La misma versión de SQL Server instalada localmente y en los dos nodos de AWS

Versiones de producto

- SQL Server versión 2016 y posteriores
- SQL Server Enterprise Edition

Arquitectura

Pila de tecnología de origen

- Base de datos de Microsoft SQL Server con grupos de disponibilidad Always On en las instalaciones

Pila de tecnología de destino

- Base de datos de Microsoft SQL Server con grupos de disponibilidad Always On en Amazon EC2 en la nube de AWS

Arquitectura de migración

Terminología

- WSFC 1: WSFC en las instalaciones
- WSFC 2: WSFC en la nube de AWS
- AG 1: primer grupo de disponibilidad, que se encuentra en el WSFC 1
- AG 2: segundo grupo de disponibilidad, que se encuentra en el WSFC 2
- Réplica principal de SQL Server: nodo del AG 1 que se considera el principal global para todas las escrituras
- Reenviador de SQL Server: nodo de AG 2 que recibe datos de forma asíncrona desde la réplica principal de SQL Server
- Réplica secundaria de SQL Server: nodos en el AG 1 o el AG 2 que reciben datos de forma sincrónica desde la réplica principal o el reenviador

Tools (Herramientas)

- AWS Direct Connect: AWS Direct Connect se utiliza para vincular su red interna con una ubicación de AWS Direct Connect de a través de cable de fibra óptica Ethernet de fibra óptica. Con esta

conexión, puede crear interfaces virtuales directamente en servicios públicos de AWS, omitiendo a los proveedores de servicios de Internet en su ruta de acceso a la red.

- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede usar Amazon EC2 para lanzar tantos o tan pocos servidores virtuales como necesite, y puede ampliarlos de manera horizontal o horizontal.
- Site-to-SiteVPN de AWS: la Site-to-Site VPN de AWS permite crear una red privada site-to-site virtual (VPN). Puede configurar la VPN para que transmita el tráfico entre las instancias que lance en AWS y su propia red remota.
- Microsoft SQL Server Management Studio: Microsoft SQL Server Management Studio (SSMS) es un entorno integrado para administrar la infraestructura de SQL Server. Proporciona una interfaz de usuario y un grupo de herramientas con editores de scripts enriquecidos que interactúan con SQL Server.

Epics

Configurar un segundo grupo de disponibilidad en AWS

Tarea	Descripción	Habilidades requeridas
Crear un WSFC en AWS.	Cree WSFC 2 en EC2 instancias de Amazon con dos nodos para HA. Utilizará este clúster de conmutación por error para crear el segundo grupo de disponibilidad (AG 2) en AWS.	Administrador de sistemas, administrador SysOps
Cree el segundo grupo de disponibilidad en el WSFC 2.	Con SSMS, cree el AG 2 en dos nodos del WSFC 2. El primer nodo del WSFC 2 actuará como reenviador. El segundo nodo del WSFC 2 actuará como réplica secundaria del AG 2. En este momento, no hay bases de datos disponibles	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	en AG 2. Este es el punto de partida para configurar el grupo de disponibilidad distribuida.	
Crear bases de datos sin opción de recuperación en AG 2.	Realice copias de seguridad de las bases de datos en el grupo de disponibilidad local (AG 1). Restaurar las bases de datos tanto en el reenviador como en la réplica secundaria del AG 2 sin opción de recuperación. Al restaurar las bases de datos, especifique una ubicación con suficiente espacio en disco para los archivos de datos de la base de datos y los archivos de registro. En este momento, las bases de datos se encuentran en estado de restauración. No forman parte del AG 2 ni del grupo de disponibilidad distribuida y no se sincronizan.	Administrador de base de datos, desarrollador

Configurar el grupo de disponibilidad distribuida

Tarea	Descripción	Habilidades requeridas
Cree el grupo de disponibilidad distribuida en AG 1.	Para crear el grupo de disponibilidad distribuida en	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	el AG 1, utilice el `CREATE AVAILABILITY GROUP` con la `DISTRIBUTED` opción. 1. Utilice las direcciones de `LISTENER_URL` punto de conexión para el AG 1 y el AG 2. 2. Para `AVAILABILITY-MODE`, use `ASYNCHRONOUS_COMMIT` para evitar la latencia de la red, si la hubiera. Esto no afectará al rendimiento de la base de datos. 3. En `FAILOVER_MODE` , utilice `MANUAL`. Es el único modo de disponibilidad que funciona con grupos de disponibilidad distribuidos. 4. Para restaurar las bases de datos manualmente en AG 2 y tener más control en bases de datos más grandes, utilice `MANUAL` para `SEEDING_MODE` .	

Tarea	Descripción	Habilidades requeridas
Cree el grupo de disponibilidad distribuida en AG 2.	Para crear el grupo de disponibilidad distribuida en AG 2, utilice `ALTER AVAILABILITY GROUP` con la opción `DISTRIBUTED`. 1. Utilice las direcciones de `LISTENER_URL` punto de conexión para el AG 1 y el AG 2. 2. Para `AVAILABILITY-MODE`, use `ASYNCHRONOUS_COMMIT` para evitar la latencia de la red, si la hubiera. Esto no afectará al rendimiento de la base de datos. 3. En `FAILOVER_MODE`, utilice `MANUAL`. Es el único modo de disponibilidad que funciona con grupos de disponibilidad distribuidos. 4. Para restaurar las bases de datos manualmente en AG 2 y tener más control en bases de datos más grandes, utilice `MANUAL` para `SEEDING_MODE`. El grupo de disponibilidad distribuida se crea entre el AG 1 y el AG 2.	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	Las bases de datos del AG 2 aún no están configuradas para participar en el flujo de datos del AG 1 al AG 2.	
Añada bases de datos al reenviador y a la réplica secundaria en AG 2.	Agregue las bases de datos al grupo de disponibilidad distribuida utilizando `ALTER DATABASE` con la opción `SET HADR AVAILABILITY GROUP` tanto en el reenviador como en la réplica secundaria en el AG 2. Esto inicia un flujo de datos asíncrono entre las bases de datos de la AG 1 y la AG 2. La principal global realiza las escrituras, envía los datos de forma sincrónica a la réplica secundaria en la AG 1 y envía los datos de forma asíncrona al reenviador en la AG 2. El reenviador del AG 2 envía los datos de forma sincrónica a la réplica secundaria del AG 2.	Administrador de base de datos, desarrollador

Supervise el flujo de datos asíncrono entre AG 1 y AG 2

Tarea	Descripción	Habilidades requeridas
Registros DMVs de uso y de SQL Server.	Supervise el estado del flujo de datos entre dos grupos de disponibilidad mediante vistas	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	de administración dinámicas (DMVs) y registros de SQL Server. DMVs Entre los que son de interés para la supervisión se incluyen `sys.dm_hadr_availability_replica_states` y`sys.dm_hadr_automatic_seeding` . Para conocer el estado de la sincronización del reenviador, supervise el estado sincronizado en el registro de SQL Server del reenviador.	

Realice actividades de transición para la migración final

Tarea	Descripción	Habilidades requeridas
Detener todo el tráfico hacia la réplica principal.	Detenga el tráfico entrante a la réplica principal en la AG 1 para que no se produzca ninguna actividad de escritura en las bases de datos y las bases de datos estén listas para la migración.	Propietario de la aplicación, desarrollador
Cambie el modo de disponibilidad del grupo de disponibilidad distribuida en AG 1.	En la réplica principal, establezca el modo de disponibilidad del grupo de disponibilidad distribuido en sincrónico.	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	Tras cambiar el modo de disponibilidad a sincrónic o, los datos se envían de forma sincrónica desde la réplica principal de la AG 1 al reenviador de la AG 2.	
Compruebe LSNs los dos grupos de disponibilidad.	Compruebe los últimos números de secuencia logarítmica (LSNs) tanto en el AG 1 como en el AG 2. Como no se está realizando ninguna escritura en la réplica principal de AG 1, los datos se sincronizan y los últimos LSNs de ambos grupos de disponibi lidad deben coincidir.	Administrador de base de datos, desarrollador
Actualice AG 1 al rol secundari o.	Al actualizar el AG 1 al rol secundario, el AG 1 pierde el rol de réplica principal y no acepta escrituras, y el flujo de datos entre dos grupos de disponibilidad se detiene.	Administrador de base de datos, desarrollador

Conmutación por error al segundo grupo de disponibilidad

Tarea	Descripción	Habilidades requeridas
Conmutar por error manualmente a AG 2.	En el reenviador de AG 2, modifique el grupo de disponibilidad distribuida para permitir la pérdida de datos. Como ya ha comprobado y confirmado que los últimos	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	datos del AG 1 y LSNs el AG 2 coinciden, la pérdida de datos no es motivo de preocupación. Al permitir la pérdida de datos en el reenviador de AG 2, las funciones de AG 1 y AG 2 cambian: • AG 2 pasa a ser el grupo de disponibilidad con la réplica principal y la réplica secundaria. • El AG 1 pasa a ser el grupo de disponibilidad con el reenviador y la réplica secundaria.	
Cambie el modo de disponibilidad del grupo de disponibilidad distribuida en AG 2.	En la réplica principal de AG 2, cambie el modo de disponibilidad a asíncrono. Esto cambia el movimiento de datos del AG 2 al AG 1, de sincrónico a asíncrono. Este paso es necesario para evitar la latencia de la red entre el AG 2 y el AG 1, si existe, y no afectará al rendimiento de la base de datos.	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
Comience a enviar tráfico a la nueva réplica principal.	Actualice la cadena de conexión para utilizar el punto de conexión de la URL del oyente en la AG 2 para enviar el tráfico a las bases de datos. El AG 2 ahora acepta escritura s y envía datos al reenviador en el AG 1, además de enviar los datos a su propia réplica secundaria en el AG 2. Los datos se mueven de forma asíncrona del AG 2 al AG 1.	Propietario de la aplicación, desarrollador

Realice actividades posteriores a la transición

Tarea	Descripción	Habilidades requeridas
Elimine el grupo de disponibi lidad distribuida en AG 2.	Supervise la migración durante el tiempo planifica do. A continuación, coloque el grupo de disponibilidad distribuida en la AG 2 para eliminar la configuración del grupo de disponibilidad distribuida entre la AG 2 y la AG 1. Esto elimina la configuración del grupo de disponibilidad distribuida y se detiene el flujo de datos del AG 2 al AG 1. En este momento, AG 2 está altamente disponible en AWS, con una réplica principal que	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	realiza escrituras y una réplica secundaria en el mismo grupo de disponibilidad.	
Quite del servicio de los servidores en las instalaci ones.	Retire del servicio los servidores locales del WSFC 1 que forman parte del AG 1.	Administrador de sistemas, SysOps administrador

Recursos relacionados

- Grupos de disponibilidad distribuida
- SQL Docs: grupos de disponibilidad distribuida
- SQL Docs: grupos de disponibilidad Always On: una solución de alta disponibilidad y recuperación de desastres

Migrar una base de datos relacional a MongoDB Atlas en AWS

Battulga Purevragchaa e Igor Alekseev, Amazon Web Services

Babu Srinivasan, MongoDB

Resumen

En este patrón se describen los pasos para migrar de una base de datos relacional como SQL Server, MySQL o PostgreSQL a MongoDB Atlas en la Nube de AWS. Utilice MongoDB Relational Migrator para ayudar a acelerar la migración de datos desde bases de datos relacionales a MongoDB Atlas.

El patrón acompaña a la guía Migración a MongoDB Atlas que se encuentra en AWS el sitio web de orientación prescriptiva. AWS Proporciona los pasos de implementación para uno de los escenarios de migración que se analizan en esa guía. Para ver otros escenarios de migración, consulte los siguientes patrones en el sitio web de la Guía prescriptiva: AWS

- Migre un entorno MongoDB autohospedado a MongoDB Atlas en AWS
- Transmita datos desde IBM Db2, SAP, Sybase y otras bases de datos a MongoDB Atlas en AWS

El patrón está destinado a los socios y AWS usuarios de AWS System Integrator (SI).

Requisitos previos y limitaciones

Requisitos previos

- Una base de datos relacional de origen (Oracle Database, SQL Server, PostgreSQL, SAP/Sybase MySQL, ASE y otras) para migrar a MongoDB Atlas.
- Familiaridad con las bases de datos relacionales, MongoDB Atlas y. Servicios de AWS Este patrón explica algunos de los pasos de migración de forma general. Se agregarán detalles adicionales en futuras versiones.

Versiones de producto

- MongoDB versión 5.0 o posterior

Arquitectura

En el siguiente diagrama se muestra la migración de una base de datos de un sistema de administración de bases de datos relacionales (RDBMS) a MongoDB Atlas en AWS.

Para ver las arquitecturas de referencia de MongoDB Atlas que admiten diferentes escenarios de uso, consulte Migración a MongoDB Atlas en el sitio web de orientación prescriptiva. AWS AWS

Tools (Herramientas)

- MongoDB Atlas es una base de datos como servicio DBaa (S) totalmente gestionada para implementar y gestionar bases de datos MongoDB en la nube.
- MongoDB Relational Migrator proporciona una transición fluida de datos desde bases de datos relacionales tradicionales a MongoDB. Ayuda a automatizar el proceso de conversión y transforma el modelo de datos estructurados de las bases de datos relacionales en el formato de documento flexible proporcionado por MongoDB. Relational Migrator preserva las relaciones y la integridad de los datos para simplificar la migración. Las organizaciones pueden aprovechar las ventajas de escalabilidad, rendimiento y versatilidad que ofrece MongoDB y, al mismo tiempo, retener la familiaridad de sus datos existentes.

Prácticas recomendadas

Para conocer las mejores prácticas para usar MongoDB AWS en, consulte las publicaciones del blog de Partner Network AWS .

Epics

Descubrimiento y evaluación

Tarea	Descripción	Habilidades requeridas
Determine los parámetros y el tamaño de la base de datos relacional.	Para calcular el tamaño del conjunto de trabajo, utilice las recomendaciones de Relational Migrator y la información de `db.stats()` para el espacio total del	Administrador de base de datos, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	índice Presuponga que se accederá con frecuencia a un porcentaje de su espacio de datos. Esta tarea puede necesitar aproximadamente una semana. Para obtener más información y ejemplos de esta y otras historias de esta épica, consulte la sección Recursos relacionados.	

Tarea	Descripción	Habilidades requeridas
Calcule los requisitos de ancho de banda de la red.	Para calcular los requisitos de ancho de banda de la red, multiplique el tamaño medio de los documentos por el número de documentos servidos por segundo. Tenga en cuenta el tráfico máximo que soportará cualquier nodo del clúster como base. Para calcular las velocidades de transferencia de datos descendentes del clúster a las aplicaciones cliente, utilice la suma del total de documentos devueltos durante un período de tiempo. Si sus aplicaciones leen desde nodos secundarios, divida este número total de documentos por el número de nodos que pueden realizar operaciones de lectura. Para encontrar el tamaño medio de los documentos de una base de datos, utilice el comando `db.stats().avgObjSize` . Esta tarea suele necesitar un día.	Administrador de base de datos
Seleccione la capa de Atlas.	Siga las instrucciones de la documentación de MongoDB para seleccionar la capa del clúster de Atlas correcta.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Planifique la transición.	Planifique la transición de la aplicación.	Administrador de base de datos, propietario de la aplicación

Configure un nuevo entorno de MongoDB Atlas en AWS

Tarea	Descripción	Habilidades requeridas
Cree un nuevo clúster de MongoDB Atlas en. AWS	En MongoDB Atlas, elija Build a Cluster. En el cuadro de diálogo Crear nuevo clúster, seleccione AWS como proveedor de nube.	Administrador de base de datos
Seleccione Regiones de AWS una configuración de clúster global.	Seleccione una opción de la lista de disponibles Regiones de AWS para su clúster de Atlas. Configure clústeres globales si es necesario.	Administrador de base de datos
Seleccione la capa del clúster.	Seleccione la capa del clúster que prefiera. La selección de la capa determina factores como la memoria, el almacenamiento y las especificaciones de IOPS.	Administrador de base de datos
Configure los ajustes adicional es del clúster.	Configure los ajustes adicional es del clúster, como la versión de MongoDB, la copia de seguridad y las opciones de cifrado. Para obtener más información sobre estas	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	opciones, consulte la sección Recursos relacionados.	

Configure la seguridad y el cumplimiento

Tarea	Descripción	Habilidades requeridas
Configure la lista de acceso.	Para conectarse al clúster de Atlas, debe agregar una entrada a la lista de acceso del proyecto. Atlas TLS/SSL lo utiliza para cifrar las conexiones a la nube privada virtual (VPC) de su base de datos. Para configurar la lista de acceso al proyecto y obtener más información sobre las historias de esta epopeya, consulte la sección Recursos relacionados.	Administrador de base de datos
Autentique y autorice a los usuarios.	Debe crear y autenticar a los usuarios de la base de datos que accederán a los clústeres de MongoDB Atlas. Para acceder a los clústeres de un proyecto, los usuarios deben pertenecer a ese proyecto y pueden pertenecer a varios proyectos.	Administrador de base de datos
Cree roles personalizados.	(Opcional) Atlas admite la creación de roles personalizados en los casos en que los permisos de usuario integrado	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	s en la base de datos Atlas no cubran el conjunto de privilegi os deseado.	
Configure las interconexiones con VPC.	(Opcional) Atlas admite la interconexión de VPC con otras. VPCs AWS	Administrador de AWS
Configure un punto final AWS PrivateLink .	(Opcional) Puede configurar puntos de conexión privados AWS utilizando AWS PrivateLi nk. Para obtener más información, consulte la documentación de Amazon VPC.	Administrador de AWS
Habilitar la autenticación en dos pasos.	(Opcional) Atlas admite la autenticación en dos pasos (2FA) para ayudar a los usuarios a controlar el acceso a sus cuentas de Atlas.	Administrador de AWS
Configure la autenticación y la autorización de los usuarios con LDAP.	(Opcional) Atlas admite realizar la autenticación y autorización de los usuarios con el Protocolo ligero de acceso a directorios (LDAP).	Administrador de base de datos
Configure el AWS acceso unificado.	(Opcional) Algunas funciones de Atlas, como Atlas Data Lake y el cifrado en reposo mediante la gestión de claves del cliente, utilizan funciones AWS Identity and Access Management (IAM) para la autenticación.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure el cifrado en reposo utilizando AWS KMS.	(Opcional) Atlas admite el uso de AWS Key Managemen t Service (AWS KMS) para cifrar los motores de almacenamiento y las copias de seguridad de los proveedor es de servicios en la nube.	Administrador de AWS
Configure el cifrado en el nivel de campo del cliente.	(Opcional) Atlas admite el cifrado en el nivel de campo del cliente, incluido el cifrado automático de los campos.	Administrador de AWS

Migración de datos

Tarea	Descripción	Habilidades requeridas
Agregue MongoDB Relational Migrator a la lista de acceso.	Agregue Relational Migrator a la lista de acceso para la base de datos de origen. Esto ayuda a preparar el entorno de origen para conectarse al clúster de Atlas de destino.	Administrador de base de datos
Evalúe los objetos de la base de datos relacional.	Inicie MongoDB Relational Migrator y conéctese a la base de datos relacional. Inicie la evaluación.	Administrador de base de datos
Acepte los patrones de migración o elija si quiere modificarlos en función de las necesidades de la empresa.	Acepte los patrones de bases de datos recomendados por Relational Migrator en función de la evaluación inicial y los parámetros de rendimiento, u opte por modificarlos en	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	función de los requisitos de la empresa.	
Lance el conjunto de réplicas de destino en MongoDB Atlas.	Lance el conjunto de réplicas de destino en MongoDB Atlas. En Relational Migrator, elija I'm ready to migrate.	Administrador de base de datos

Configurar la integración operativa

Tarea	Descripción	Habilidades requeridas
Conéctese al clúster de MongoDB Atlas.	Asegúrese de que la conectividad del clúster de MongoDB Atlas funcione según lo esperado.	Propietario de la aplicación
Interactúe con los datos del clúster.	Verifique los datos del clúster.	Administrador de base de datos
Supervise los clústeres.	Compruebe que sus clústeres estén configurados correctamente.	Administrador de base de datos
Realice copias de seguridad y restaure los datos del clúster.	Programe las copias de seguridad con una cadencia regular para los datos del clúster.	Administrador de base de datos

Recursos relacionados

Todos los enlaces siguientes, a menos que se indique lo contrario, van a páginas web de la documentación de MongoDB.

Guía de migración

- Migración a MongoDB Atlas AWS en (Guía prescriptiva)AWS

Detectar y evaluar

- Memoria
- Ejemplo de dimensionamiento con conjuntos de datos de muestra de Atlas
- Ejemplo de dimensionamiento para aplicaciones móviles
- Tráfico de red
- Escalado automático de clústeres
- Plantilla de dimensionamiento de Atlas

Configure la seguridad y el cumplimiento

- Configurar entradas de la lista de acceso IP
- Configure Database Users
- Configure Access to the Atlas UI
- Configure Custom Database Roles
- Configure Database Users
- Configurar un emparejamiento de red
- Learn About Private Endpoints in Atlas
- Manage Your Multi-Factor Authentication Options
- Configurar la autenticación y la autorización de usuarios con LDAP
- Lago de datos Atlas
- Cifrado en reposo mediante la administración de claves de cliente
- Métodos para asumir un rol (documentación de IAM)
- Configurar el cifrado en el nivel de campo del cliente
- Automatic Encryption
- MongoDB Atlas Security Controls
- Centro de confianza de MongoDB
- Configure Security Features for Clusters

Configuración de un nuevo entorno de MongoDB Atlas en AWS

- Proveedores y regiones de la nube
- Manage Global Clusters
- Select Cluster Tier
- Configure Additional Settings
- Introducción a Atlas
- Configure Access to the Atlas UI

Migración de datos

- Migrate or Import Data

Monitorear clústeres

- Monitor Your Clusters

Integrar operaciones

- Conectarse a un clúster
- Interact with Your Data
- Monitor Your Clusters
- Back Up, Restore, and Archive Data

Migre un entorno MongoDB autohospedado a MongoDB Atlas en AWS

Battulga Purevragchaa e Igor Alekseev, Amazon Web Services

Babu Srinivasan, MongoDB

Resumen

Este patrón describe los pasos para migrar de un entorno de MongoDB autoadministrado (que incluye MongoDB Community Server, Enterprise Server, Enterprise Advanced, mLab o cualquier clúster de MongoDB administrado) a MongoDB Atlas en la Nube de AWS. Utiliza Atlas Live Migration Service para ayudar a acelerar la migración de los datos de MongoDB a MongoDB Atlas.

El patrón acompaña a la guía Migración a MongoDB Atlas que se encuentra en AWS el sitio web de orientación prescriptiva. AWS Proporciona los pasos de implementación para uno de los escenarios de migración que se analizan en esa guía. Para ver otros escenarios de migración, consulte los siguientes patrones en el sitio web de la Guía prescriptiva: AWS

- Migrar una base de datos relacional a MongoDB Atlas en AWS
- Transmita datos desde IBM Db2, SAP, Sybase y otras bases de datos a MongoDB Atlas en AWS

El patrón está destinado a socios y usuarios AWS de Systems Integrator (SI). AWS

Requisitos previos y limitaciones

Requisitos previos

- Un entorno de MongoDB Enterprise Advanced, Community Server u otro entorno de MongoDB autoadministrado de origen para migrar a MongoDB Atlas.
- Familiaridad con MongoDB, MongoDB Atlas y. Servicios de AWS Este patrón explica algunos de los pasos de migración de forma general. Se agregarán detalles adicionales en futuras versiones.

Versiones de producto

- MongoDB versión 6.0.13 o posterior

Arquitectura

En el siguiente diagrama se muestra Atlas Live Migration Service, que se utiliza para migrar datos de una base de datos de MongoDB Enterprise Advanced y una base de datos de MongoDB Community a MongoDB Atlas en AWS. Utilice este servicio cuando tenga que migrar bases de datos grandes y complejas a MongoDB Atlas con un tiempo de inactividad mínimo y una sincronización de datos continua. Este patrón utiliza Atlas Live Migration Service.

El siguiente diagrama muestra el servicio de réplica de MongoDB `mongomirror` () que también puede utilizar para migrar datos de una base de datos de MongoDB Enterprise Advanced y una base de datos de MongoDB Community a MongoDB Atlas a través de una conexión segura. AWS AWS PrivateLink Use `mongomirror` para la replicación de datos continua entre MongoDB en las instalaciones y MongoDB Atlas. Esta herramienta es ideal para la recuperación ante desastres o las migraciones por fases, pero queda fuera del alcance de este patrón.

Para obtener más arquitecturas de referencia de MongoDB Atlas que admiten diferentes escenarios de uso, consulte Migración a MongoDB Atlas en el sitio web de orientación prescriptiva. AWS AWS

Tools (Herramientas)

- MongoDB Atlas es una base de datos como servicio (DbaaS) completamente administrada para implementar y administrar bases de datos de MongoDB en la nube.
- Atlas Live Migration Service es un programa de utilidad gratuito de MongoDB que ayuda a migrar bases de datos a Atlas. Este servicio mantiene la base de datos de origen sincronizada con la base de datos de destino hasta la transición. Cuando esté todo a punto para realizar la transición, detenga las instancias de la aplicación, diríjalas al clúster Atlas de destino y reinícielas. Para acceder a este servicio, elija Opciones de base de datos en su clúster de MongoDB Atlas.
- mongomirror es una herramienta para migrar datos manualmente de un conjunto de réplicas de MongoDB existente a un conjunto de réplicas de MongoDB Atlas. `mongomirror` no requiere que cierre el conjunto de réplicas ni las aplicaciones existentes, no importa datos de usuarios ni roles ni copia la base de datos de configuración. Puede descargar `mongomirror` desde la documentación de MongoDB.

Prácticas recomendadas

Para conocer las mejores prácticas para usar MongoDB AWS en, consulte las publicaciones del blog de Partner Network AWS .

Epics

Descubrimiento y evaluación

Tarea	Descripción	Habilidades requeridas
Determine el tamaño del clúster.	Calcule el tamaño del conjunto de trabajo utilizando la información de `db.stats( )` para el espacio total del índice. Presuponga que se accederá con frecuencia a un porcentaje de su espacio de datos. O bien, puede estimar las necesidades de memoria en función de sus propias presuposiciones. Esta tarea puede necesitar aproximad amente una semana. Para obtener más información y ejemplos de esta y otras historias de esta épica, consulte la sección Recursos relacionados.	Administrador de base de datos, propietario de la aplicación
Calcule los requisitos de ancho de banda de la red.	Para calcular los requisito s de ancho de banda de la red, multiplique el tamaño medio de los documentos por el número de documentos servidos por segundo. Tenga en cuenta el tráfico máximo que soportará cualquier	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	nodo del clúster como base. Para calcular las velocidad es de transferencia de datos descendentes del clúster a las aplicaciones cliente, utilice la suma del total de documentos devueltos durante un período de tiempo. Si sus aplicaciones leen desde nodos secundari os, divida este número total de documentos por el número de nodos que pueden realizar operaciones de lectura. Para encontrar el tamaño medio de los documentos de una base de datos, utilice el comando `db.stats().avgObjS ize` . Esta tarea suele necesitar un día.	
Seleccione la capa de Atlas.	Siga las instrucciones de la documentación de MongoDB para seleccionar la capa del clúster de Atlas correcta.	Administrador de base de datos
Planifique la transición.	Planifique la transición de la aplicación.	Administrador de base de datos, propietario de la aplicación

Configurar un nuevo entorno de MongoDB Atlas en AWS

Tarea	Descripción	Habilidades requeridas
Cree un nuevo clúster de MongoDB Atlas en. AWS	Inicie sesión en Atlas y abra la página Información general	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de su proyecto. Seleccion e el botón Crear para crear un clúster. Para obtener más información, consulte la documentación de MongoDB.	
Seleccione una Regiones de AWS configuración de clúster global.	Seleccione una opción de la lista de disponibles Regiones de AWS para su clúster de Atlas. Configure clústeres globales si es necesario. Para obtener más información, consulte la documentación de MongoDB.	Administrador de base de datos
Seleccione la capa del clúster.	Seleccione la capa del clúster que prefiera. La selección de la capa determina factores como la memoria, el almacenamiento y las especificaciones de IOPS.	Administrador de base de datos
Configure los ajustes adicional es del clúster.	Configure los ajustes adicional es del clúster, como la versión de MongoDB, la copia de seguridad y las opciones de cifrado. Para obtener más información sobre estas opciones, consulte la sección Recursos relacionados.	Administrador de base de datos

Configure la seguridad y el cumplimiento

Tarea	Descripción	Habilidades requeridas
Autentique y autorice a los usuarios.	Debe crear y autenticar a los usuarios de la base de datos que accederán a los clústeres de MongoDB Atlas. Para acceder a los clústeres de un proyecto, los usuarios deben pertenecer a ese proyecto y pueden pertenecer a varios proyectos. Atlas también admite la autenticación basada en AWS Identity and Access Management (IAM). Para obtener más información, consulte la documentación de MongoDB.	Administrador de base de datos
Cree roles personalizados.	(Opcional) Atlas admite la creación de roles personalizados en los casos en que los permisos de usuario integrados en la base de datos Atlas no cubran el conjunto de privilegios deseado.	Administrador de base de datos
Configure las interconexiones con VPC.	(Opcional) Atlas admite el emparejamiento de nubes privadas virtuales (VPC) con otras. VPCs AWS	Administrador de AWS
Configure un punto final AWS PrivateLink .	(Opcional) Puede configurar puntos de conexión privados AWS utilizando AWS PrivateLink. Para obtener más información, consulte la	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	documentación de Amazon VPC.	
Habilitar la autenticación en dos pasos.	(Opcional) Atlas admite la autenticación en dos pasos (2FA) para ayudar a los usuarios a controlar el acceso a sus cuentas de Atlas.	Administrador de AWS
Configure la autenticación y la autorización de los usuarios con LDAP.	(Opcional) Atlas admite realizar la autenticación y autorización de los usuarios con el Protocolo ligero de acceso a directorios (LDAP).	Administrador de AWS
Configure el AWS acceso unificado.	(Opcional) Algunas caracterí sticas de Atlas, como Atlas Data Lake y el cifrado en reposo mediante la administr ación de claves de cliente, utilizan los roles de IAM para la autenticación.	Administrador de AWS
Configure el cifrado en reposo utilizando AWS KMS.	(Opcional) Atlas admite el uso de AWS Key Managemen t Service (AWS KMS) para cifrar los motores de almacenamiento y las copias de seguridad de los proveedor es de servicios en la nube.	Administrador de AWS
Configure el cifrado en el nivel de campo del cliente.	(Opcional) Atlas admite el cifrado en el nivel de campo del cliente, incluido el cifrado automático de los campos.	Administrador de AWS

Migración de datos

Tarea	Descripción	Habilidades requeridas
Seleccionar el conjunto de réplicas de destino en MongoDB Atlas.	Vaya al clúster de Atlas de destino y elija el botón de puntos suspensivos (…). En la lista de clústeres, este botón aparece debajo del nombre del clúster. En los detalles del clúster, el botón aparece a la derecha, junto a los botones Conectarse y Configuración. Para obtener más información, consulte la documentación de MongoDB.	Administrador de base de datos
Agregar Atlas Live Migration Service a la lista de acceso.	Añada el servicio Atlas Live Migration a la lista de acceso de su clúster AWS de origen. Esto ayuda a preparar el entorno de origen para conectarse al clúster de Atlas de destino.	Administrador de base de datos
Llevar a cabo la migración con Atlas Live Migration Service.	Elija Iniciar migración. Cuando el botón Preparación de la transición se ponga en verde, lleve a cabo la transició n. Revise las métricas de rendimiento de los clústeres de Atlas. Considere la posibilid ad de actualizar la conexión de la base de datos en todas las capas de la aplicación para que apunte a la nueva base de datos.	Administrador de base de datos

Configurar la integración operativa

Tarea	Descripción	Habilidades requeridas
Conéctese al clúster de MongoDB Atlas.	Asegúrese de que la conectividad del clúster de MongoDB Atlas funcione según lo esperado.	Propietario de la aplicación
Interactúe con los datos del clúster.	Pruebe los datos del clúster.	Administrador de base de datos
Supervise los clústeres.	Compruebe que sus clústeres estén configurados correctamente.	Administrador de base de datos
Realice copias de seguridad y restaure los datos del clúster.	Programe las copias de seguridad con una cadencia regular para los datos del clúster.	Administrador de base de datos

Resolución de problemas

Problema	Solución

Error: No se pudo alcanzar el origen especificado	• Asegúrese de haber agregado los rangos de subredes correctos a la lista de acceso de IP del clúster de origen. Puede encontrar los cuatro rangos de subredes necesarios en la ventana modal Migración en vivo.
	• Confirme que el nombre de host que especificó se resuelve en una dirección IP pública. En el símbolo del sistema, use uno de los siguientes comandos:
	`nslookup <hostname>`
	`ping <hostname>`

Problema	Solución
	• Asegúrese de no utilizar una conexión de emparejamiento de VPC, que no es compatible con la migración en vivo por extracción. Si la única opción es una conexión de emparejamiento de VPC, use `mongomirror` en su lugar.
Error: No se pudo resolver el nombre de host	No se encontró ninguna dirección IP para el nombre de host indicado. Confirme que el nombre de host indicado sea correcto y de acceso público.
Cualquier otro error	Si encuentra algún otro error, consulte Troubleshoot Live Migration (Pull) en la documentación de MongoDB.

Recursos relacionados

Todos los enlaces siguientes, a menos que se indique lo contrario, van a páginas web de la documentación de MongoDB.

Guía de migración

- Migración a MongoDB Atlas AWS en (Guía prescriptiva)AWS

Migración de versiones antiguas

- Migration of older versions of MongoDB

Detectar y evaluar

- Memoria
- Ejemplo de dimensionamiento con conjuntos de datos de muestra de Atlas
- Ejemplo de dimensionamiento para aplicaciones móviles
- Tráfico de red

- Escalado automático de clústeres
- Plantilla de dimensionamiento de Atlas

Configure la seguridad y el cumplimiento

- Configurar entradas de la lista de acceso IP
- Configure Database Users
- Configure Access to the Atlas UI
- Configure Custom Database Roles
- Configure Database Users
- Configurar un emparejamiento de red
- Learn About Private Endpoints in Atlas
- Manage Your Multi-Factor Authentication Options
- Configurar la autenticación y la autorización de usuarios con LDAP
- Lago de datos Atlas
- Cifrado en reposo mediante la administración de claves de cliente
- Métodos para asumir un rol (documentación de IAM)
- Configurar el cifrado en el nivel de campo del cliente
- Automatic Encryption
- MongoDB Atlas Security Controls
- Centro de confianza de MongoDB
- Configure Security Features for Clusters

Configuración de un nuevo entorno de MongoDB Atlas en AWS

- Proveedores y regiones de la nube
- Manage Global Clusters
- Select Cluster Tier
- Configure Additional Settings
- Introducción a Atlas
- Configure Access to the Atlas UI

Migración de datos

- Migrate or Import Data

Monitorización de clústeres

- Monitor Your Clusters

Integrar operaciones

- Conectarse a un clúster
- Interact with Your Data
- Monitor Your Clusters
- Back Up, Restore, and Archive Data

Entrenamiento

- Live Migration with MongoDB Atlas

Información adicional

Para obtener más información, consulte los siguientes temas en la documentación de MongoDB:

- Para mover datos a una instancia sin servidor, utilice Compass para exportar e importar datos, o migre los datos con herramientas autogestionadas. Para obtener más información, consulte Serverless Instance Limitations.
- Para cargar datos en un nuevo clúster de Atlas, consulte Load Data into Atlas.
- Para hacer una copia del clúster con fines de prueba, consulte Backup Methods for a Self-Managed Deployment.
- Si la aplicación que desea migrar requiere un tiempo de actividad casi continuo, póngase en contacto con el equipo de atención al cliente de MongoDB y comparta sus requisitos de tiempo de actividad y la configuración del clúster.
- Para obtener información adicional, consulte Migrate or Import Data.

Migración de una base de datos de Oracle a Amazon DynamoDB mediante AWS DMS

Rambabu Karnena, Amazon Web Services

Resumen

Este patrón le guía por los pasos para migrar una base de datos de Oracle a Amazon DynamoDB mediante AWS Database Migration Service (AWS DMS). Abarca tres tipos de bases de datos de origen:

- Bases de datos de Oracle en las instalaciones
- Bases de datos de Oracle en Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS) para instancias de bases de datos de Oracle

En esta prueba de concepto, este patrón se centra en la migración desde una instancia de BD de Amazon RDS para Oracle.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una aplicación que se conecta a una base de datos de Amazon RDS para Oracle
- Una tabla creada en la base de datos de Amazon RDS para Oracle de origen con una clave principal y datos de muestra

Limitaciones

- Los objetos de la base de datos de Oracle, como los procedimientos, las funciones, los paquetes y los desencadenadores, no se consideran para la migración porque Amazon DynamoDB no admite estos objetos de base de datos.

Versiones de producto

- Este patrón se aplica a todas las ediciones y versiones de las bases de datos de Oracle compatibles con AWS DMS. Para obtener más información, consulte el uso de una base de datos

de Oracle como origen para AWS DMS y el uso de una base de datos de Amazon DynamoDB como destino para AWS DMS. Le recomendamos utilizar las versiones más recientes de AWS DMS para obtener el soporte más completo de versiones y características.

Arquitectura

Pila de tecnología de origen

- Instancias de bases de datos Amazon RDS para Oracle, Oracle on EC2 Amazon o bases de datos Oracle locales

Pila de tecnología de destino

- Amazon DynamoDB

Arquitectura de migración de datos de AWS

Tools (Herramientas)

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS. Este patrón utiliza Amazon RDS para Oracle.

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	En su cuenta de AWS, cree una nube privada virtual (VPC) y una subred privada.	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Cree grupos de seguridad y listas de control de acceso a la red.	Para obtener más información, consulte la documentación de AWS.	Administrador de sistemas
Configure e inicie la instancia de BD de Amazon RDS para Oracle.	Para obtener más información, consulte la documentación de AWS.	Administrador de base de datos, administrador de sistemas

Migración de datos

Tarea	Descripción	Habilidades requeridas
Crear un rol de IAM para acceder a DynamoDB.	En la consola de AWS Identity and Access Management (IAM), cree el rol, adjunte la política `AmazonDynamoDBFullAccess to it` y seleccione AWS DMS como servicio.	Administrador de sistemas
Crear una instancia de replicación de AWS DMS para la migración.	La instancia de replicación debe estar en la misma zona de disponibilidad y VPC que la base de datos de origen.	Administrador de sistemas
Cree puntos de conexión de origen y destino en AWS DMS.	Para crear el punto de conexión de la base de datos de origen, tiene dos opciones: • En la consola de Amazon RDS, elija Bases de datos, Identificador de base BD, Conectividad y seguridad y elija el punto de conexión.	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	• En la consola de AWS DMS, elija Seleccionar instancia de RDS DB. Para crear el punto de conexión de la base de datos de destino, elija el rol de Nombre de recurso de Amazon (ARN) de la tarea anterior para acceder a DynamoDB.	
Cree una tarea de AWS DMS para cargar las tablas de base de datos de Oracle de origen en DynamoDB.	Elija los nombres de los puntos de conexión de origen y destino y la instancia de replicación en los pasos anteriores. El tipo puede ser de carga completa. Elija el esquema de Oracle y especifique % para seleccion ar todas las tablas.	Administrador de sistemas
Valide las tablas en DynamoDB.	Para ver los resultados de la migración, seleccione Tablas en el panel de navegación izquierdo de la consola de DynamoDB.	Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Cómo modificar el código de la aplicación	Para conectarse y recuperar datos de DynamoDB,	Administrador de base de datos, propietario de la

Tarea	Descripción	Habilidades requeridas
	actualice el código de la aplicación.	aplicación, administrador de sistemas

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Cambie los clientes de la aplicación para que usen DynamoDB.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cierre los recursos de AWS.	Por ejemplo, cierre la instancia de Amazon RDS para Oracle, DynamoDB y la instancia de replicación de AWS DMS.	Administrador de base de datos, administrador de sistemas
Recopile métricas.	Las métricas incluyen el tiempo de migración, los porcentajes de trabajo manual y realizado por la herramienta y el ahorro de costos.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Recursos relacionados

- AWS Database Migration Service (AWS DMS) y Amazon DynamoDB: lo que necesita saber (entrada del blog)
- Uso de una base de datos de Oracle como origen para AWS DMS

- Uso de una base de datos de Amazon DynamoDB como objetivo del servicio de migración de bases de datos de AWS
- Prácticas recomendadas para migrar de RDBMS a Amazon DynamoDB (documento técnico)

Migre de Oracle 8i o 9i a Amazon RDS para Oracle con AWS DMS SharePlex

Ramu Jagini, Amazon Web Services

Resumen

Este patrón describe cómo migrar una base de datos de Oracle 8i o 9i en las instalaciones a una base de datos de Amazon Relational Database Service (Amazon RDS) para Oracle. Puede utilizar este patrón para completar la migración con un tiempo de inactividad reducido si utiliza Quest para la replicación sincrónica. SharePlex

Debe usar una instancia de base de datos de Oracle intermedia para la migración, ya que AWS Database Migration Service (AWS DMS) no admite Oracle 8i o 9i como entorno de origen. Puede utilizar la versión SharePlex 7.6.3 para replicar desde versiones anteriores de bases de datos Oracle a versiones posteriores de bases de datos Oracle. La instancia de base de datos Oracle intermedia es compatible como destino para SharePlex 7.6.3 y se admite como fuente para AWS DMS o versiones más recientes de. SharePlex Esta compatibilidad permite la replicación posterior de los datos en el entorno de destino de Amazon RDS para Oracle.

Tenga en cuenta que varios tipos de datos y funciones obsoletos pueden afectar a una migración de Oracle 8i o 9i a la versión más reciente de Oracle Database. Para mitigar este impacto, este patrón emplea Oracle 11.2.0.4 como versión de base de datos intermedia para ayudar a optimizar el código del esquema antes de migrar al entorno de destino de Amazon RDS para Oracle.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de Oracle 8i o 9i de origen en un entorno en las instalaciones
- Oracle Database 12c versión 2 (12CR2) para almacenamiento en Amazon Elastic Compute Cloud (Amazon) EC2
- Quest SharePlex 7.6.3 (versión comercial)

Limitaciones

- Limitaciones de RDS para Oracle

Versiones de producto

- Oracle 8i o 9i para la base de datos de origen
- Oracle 12 CR2 para la base de datos provisional (debe coincidir con la versión Amazon RDS for Oracle)
- Oracle 12 CR2 o posterior para la base de datos de destino (Amazon RDS for Oracle)

Arquitectura

Pila de tecnología de origen

- Base de datos de Oracle 8i o 9i
- SharePlex

Pila de tecnología de destino

- Amazon RDS para Oracle

Arquitectura de migración

El siguiente diagrama muestra cómo migrar una base de datos de Oracle 8i o 9i de un entorno en las instalaciones a una instancia de base de datos de Amazon RDS para Oracle en la nube de AWS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Habilite la base de datos de origen de Oracle con modo de registro de archivos, registro forzado y registro suplementario.
2. Restaure la base de datos provisional de Oracle desde la base de datos de origen de Oracle mediante Recovery Manager (RMAN) point-in-time y FLASHBACK_SCN.
3. Configure SharePlex para leer los redo logs de la base de datos fuente de Oracle mediante (se utiliza `FLASHBACK_SCN` en RMAN).
4. Inicie SharePlex la replicación para sincronizar los datos de la base de datos de origen de Oracle con la base de datos provisional de Oracle.
5. Restaure la base de datos de destino de Amazon RDS para Oracle mediante EXPDP e IMPDP con `FLASHBACK_SCN`.

6. Configure AWS DMS y sus tareas de origen como base de datos transitoria de Oracle, y Amazon RDS para Oracle como base de datos de destino mediante `FLASHBACK_SCN` (se usa en EXPDP).
7. Inicie las tareas de AWS DMS para sincronizar los datos de la base de datos transitoria de Oracle con la base de datos de destino de Oracle.

Tools (Herramientas)

- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Quest SharePlex es una herramienta Oracle-to-Oracle de replicación de datos para mover datos con un tiempo de inactividad mínimo y sin pérdida de datos.
- Recovery Manager (RMAN) es un cliente de Oracle Database que realiza tareas de copia de seguridad y recuperación en sus bases de datos. Simplifica en gran medida las copias de seguridad, la restauración y la recuperación de los archivos de bases de datos.
- Data Pump Export le ayuda a cargar datos y metadatos en un conjunto de archivos del sistema operativo denominado conjunto de archivos de volcado. El conjunto de archivos de volcado solo se puede importar mediante la utilidad Data Pump Import o el paquete DBMS_DATAPUMP.

Epics

Configuración SharePlex y la base de datos provisional de Oracle en Amazon EC2

Tarea	Descripción	Habilidades requeridas
Cree una EC2 instancia.	1. Crea una EC2 instancia. 2. Instale Oracle 12 CR2 en la EC2 instancia para que sirva como base de datos provisional de Oracle.	Administración de Oracle
Prepare la base de datos transitoria.	Prepare la base de datos provisional de Oracle para restaurarla como una actualiza	Administración de Oracle

Tarea	Descripción	Habilidades requeridas
	ción en Oracle 12 CR2 realizando la copia de seguridad en RMAN del entorno de origen de la base de datos Oracle 8i o 9i. Para obtener más informaci ón, consulte la Guía del usuario de Oracle 9i Recovery Manager y la Guía del usuario de copia de seguridad y recuperación de bases de datos en la documentación de Oracle.	
Configure. SharePlex	Configure el SharePlex origen como una base de datos Oracle 8i o 9i local y configure el destino como la base de datos provisional de Oracle 12 CR2 alojada en Amazon. EC2	SharePlex, administración de Oracle

Configure Amazon RDS para Oracle como su entorno objetivo

Tarea	Descripción	Habilidades requeridas
Crear una instancia de base de datos de Oracle.	Cree una base de datos Amazon RDS for Oracle y, a continuación, conecte Oracle CR2 12 a la base de datos. Para más información, consulte Crear una instancia de base de datos de Oracle y conectarse a una base de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	datos en una instancia de base de datos en Oracle en la documentación de Amazon RDS.	
Restaure Amazon RDS para Oracle desde la base de datos transitoria.	1. Realice una copia de seguridad de EXPDP del servidor de base de datos transitorio de Oracle mediante `FLASHBACK_SCN` . 2. Restaure Amazon RDS para Oracle desde la base de datos transitoria. Para obtener más informaci ón, consulte 54 DBMS_DATA PUMP en la documentación de Oracle.	Administrador de base de datos

Configure AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree puntos de conexión para las bases de datos.	Cree un punto de conexión de origen para la base de datos transitoria de Oracle y un punto de conexión de destino para la base de datos Amazon RDS para Oracle. Para obtener más información, consulte ¿Cómo puedo crear puntos de conexión de origen	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	o de destino con AWS DMS? en el Centro de conocimientos de AWS.	
Cree una instancia de replicación.	Use AWS DMS para lanzar una instancia de replicación de la base de datos transitoria de Oracle en la base de datos Amazon RDS para Oracle. Para obtener más información, consulte el tema ¿Cómo crear una instancia de replicación de AWS DMS? en el Centro de conocimientos de AWS.	Administrador de base de datos
Crear e iniciar tareas de replicación.	Cree tareas de replicación de AWS DMS para la captura de datos de cambios (CDC) usando `FLASHBACK_SCN` de EXPDP (dado que la carga completa ya se ha realizado a través de EXPDP). Para obtener más información, consulte Crear una tarea en la documentación de AWS DMS.	Administrador de base de datos

Cómo hacer la transición a Amazon RDS para Oracle

Tarea	Descripción	Habilidades requeridas
Detenga la carga de trabajo de la aplicación.	Detenga los servidores de aplicaciones y sus aplicacio	Desarrollador de aplicaciones, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	nes durante el período de transición previsto.	
Valide la sincronización de la base de datos provisional de Oracle local con la instancia. EC2	Confirme que se hayan publicado todos los mensajes para las tareas de replicaci ón desde la instancia de SharePlex replicación a la base de datos provisional de Oracle en Amazon EC2 realizando algunos cambios de registro en la base de datos de origen local. Para obtener más información, consulte 6.4.2 Cómo cambiar un archivo de registro en la documentación de Oracle.	Administrador de base de datos
Valide la sincronización de la base de datos transitoria de Oracle con la base de datos Amazon RDS para Oracle.	Confirme que sus tareas de AWS DMS no presentan retrasos ni errores y, a continuación, compruebe el estado de validación de las tareas.	Administrador de base de datos
Detenga la replicación SharePlex de Amazon RDS.	Si tanto la replicación SharePlex de AWS DMS como la de AWS no muestran ningún error, detenga ambas replicaciones.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Reasigne la aplicación a Amazon RDS.	Comparta los detalles del punto de conexión de Amazon RDS para Oracle con el servidor de aplicaciones y sus aplicaciones y, a continuación, inicie la aplicación para reanudar las operaciones empresariales.	Desarrollador de aplicaciones, administrador de base de datos

Pruebe el entorno de destino de AWS

Tarea	Descripción	Habilidades requeridas
Pruebe el entorno de base de datos transitoria de Oracle en AWS.	1. Pruebe la SharePlex replicación y compruebe que no haya brechas de sincronización ni errores de replicación en la base de datos provisional de Oracle. 2. Verifique que la aplicación se comporta según lo esperado mediante los puntos de referencia definidos en el entorno en las instalaciones.	SharePlex, administración de Oracle
Pruebe el entorno de Amazon RDS.	1. Compruebe que todos los datos propagados a Amazon RDS después de la replicación estén libres de errores. 2. Apunte otra aplicación a la instancia de base de datos de Amazon RDS y,	Administración de Oracle

Tarea	Descripción	Habilidades requeridas
	a continuación, ejecute pruebas de rendimiento para verificar el comportam iento esperado. Para obtener más información, consulte Amazon RDS para Oracle en la documentación de Amazon RDS.	

Recursos relacionados

- Migración con confianza
- Amazon EC2
- Amazon RDS para Oracle
- AWS Database Migration Service (AWS DMS)
- Depuración de las migraciones a AWS DMS: qué hacer cuando las cosas van mal (parte 1)
- Depuración de las migraciones a AWS DMS: qué hacer cuando las cosas van mal (parte 2)
- Depuración de las migraciones a AWS DMS: ¿qué hacer cuando las cosas van mal? (Parte 3)
- SharePlex para la replicación de bases de datos
- SharePlex: replicación de bases de datos para cualquier entorno

Migración de una base de datos MySQL en las instalaciones a Amazon EC2

Lorenzo Mota, Amazon Web Services

Resumen

Este patrón proporciona orientación para migrar una base de datos MySQL en las instalaciones a una base de datos MySQL en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). El patrón analiza el uso de AWS Database Migration Service (AWS DMS) o herramientas nativas de MySQL, como mysqldump, para la migración. Se centra en la migración completa de la base de datos a una instancia de base de datos MySQL.

El patrón es principalmente para DBAs arquitectos de soluciones y arquitectos de soluciones. Se puede usar en proyectos pequeños o grandes, en una fase de prueba o de migración final. Se recomienda ejecutar al menos un ciclo de pruebas antes de utilizar este patrón en un entorno de producción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de MySQL de origen en un centro de datos en las instalaciones

Versiones de producto

- Versión 5.5 de MySQL o posterior
- Un sistema operativo de destino compatible con Amazon EC2; consulte Amazon EC2 FAQs

Arquitectura

Pila de tecnología de origen

- Una base de datos MySQL en las instalaciones

Pila de tecnología de destino

- Una instancia de base de datos de MySQL en Amazon EC2

Métodos de migración de datos de AWS

- AWS DMS
- Herramientas nativas de MySQL, como mysqldump, o herramientas de terceros, como Percona XtraBackup

Arquitectura de destino

En el siguiente diagrama se muestra la implementación de Amazon EC2 de destino tras la transición.

Arquitectura de migración de datos de AWS

Uso de AWS DMS:

El siguiente diagrama ilustra el flujo de trabajo de migración de datos en el que se basa el AWS DMS envío de cambios completos e incrementales a la base de datos MySQL de destino hasta la transición. La conexión de red local a otra AWS depende de los requisitos del cliente SQL y queda fuera del ámbito de este patrón.

Uso de otras herramientas de MySQL:

En el siguiente diagrama se ilustra el flujo de trabajo de migración de datos basado en el uso de herramientas de MySQL para generar archivos de volcado de exportación desde la base de datos en las instalaciones. Estos archivos se trasladan a Amazon Simple Storage Service (Amazon S3) y se importan a la base de datos MySQL de destino antes de la transición. La conexión de red local a otra AWS depende de los requisitos del cliente SQL y queda fuera del ámbito de este patrón.

Notas:

- En función del tiempo de inactividad y del tamaño de la base de datos para la transición final, puede utilizar AWS DMS otra herramienta de captura de datos de cambios (CDC) para minimizar el tiempo de transición. Si utiliza una herramienta de los CDC, por ejemplo AWS DMS, puede migrar a la base de datos de destino en cuestión de minutos.

- Una estrategia sin conexión con mysqldump puede ser suficiente si el tamaño de la base de datos y la latencia de la red permiten una transición breve a la migración. (Le recomendamos que lleve a cabo pruebas para obtener un tiempo aproximado).
- Por lo general, una estrategia de los CDC AWS DMS requiere más supervisión y complejidad que una opción fuera de línea.

Tools (Herramientas)

AWS servicios

- AWS Database Migration Service (AWS DMS) admite varias bases de datos de origen y destino. Para obtener información sobre las bases de datos de origen y destino de MySQL compatibles con AWS DMS, consulte Uso de una base de datos compatible con MySQL como fuente AWS DMS y Uso de una base de datos compatible con MySQL como destino para. AWS DMS Si su base de datos de origen no es compatible con AWS DMS, debe elegir otro método para migrar los datos.

Otras herramientas

- mysqldump es una utilidad de MySQL que crea un archivo de volcado desde una base de datos MySQL con fines de copia de seguridad o migración.
- Percona XtraBackup es una utilidad de código abierto para realizar copias de seguridad sin bloqueo en bases de datos MySQL.

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos.	Valide las versiones de las bases de datos de origen y de destino. Para obtener información sobre las versiones de MySQL compatibles AWS DMS, consulte Fuentes AWS DMS	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	y destinos AWS DMS en la AWS DMS documentación.	
Identifique el sistema operativo de destino.	Determine la versión del sistema operativo de destino. Para obtener una lista de los sistemas operativos de destino compatibles con Amazon EC2, consulte Amazon EC2. FAQs	Administrador de base de datos, administrador de sistemas
Identifique los requisitos de hardware.	Determine los requisitos de hardware para la instancia del servidor de destino en función de la lista de compatibilidad de MySQL y los requisitos de capacidad.	Administrador de base de datos, administrador de sistemas
Identifique los requisitos de almacenamiento.	Determine el tipo de almacenamiento y la capacidad para la base de datos de destino.	Administrador de base de datos, administrador de sistemas
Identifique requisitos de red.	Determine los requisitos de la red, como la latencia y el ancho de banda.	Administrador de base de datos, administrador de sistemas
Elija el tipo de instancia de destino.	Elija el tipo de instancia de destino en función de la capacidad, las características de almacenamiento y las características de red.	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Identifique los requisitos de seguridad.	Determine los requisitos de seguridad para acceder a la red o al host de las bases de datos de origen y destino.	Administrador de base de datos, administrador de sistemas
Identifique los usuarios.	Determine la lista de los usuarios del sistema operativo para la instalación del software de MySQL. Para obtener más información, consulte la documentación de MySQL.	Administrador de base de datos, administrador de sistemas
Determine una estrategia de copia de seguridad.		Administrador de base de datos
Determine los requisitos de disponibilidad.		Administrador de base de datos
Identifique la estrategia de migración o transición de aplicaciones.		Administrador de base de datos, administrador de sistemas

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC) y subredes.	Configure las tablas de enrutamiento, las puertas de enlace de Internet, las puertas de enlace NAT y las subredes. Para obtener más información, consulte VPC configuration options en la documentación de Amazon VPC.	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Cree grupos de seguridad y listas de control de acceso a la red ()ACLs.	Configure los puertos (el valor predeterminado para MySQL es 3306) y rangos de CIDR o específicos IPs según sus requisitos.	Administrador de sistemas
Configure e inicie una instancia EC2.	Para obtener instrucciones, consulte Launch an EC2 instance en la documentación de Amazon EC2.	Administrador de sistemas

Instalar el software MySQL

Tarea	Descripción	Habilidades requeridas
Cree usuarios y grupos.	Cree los usuarios y grupos del sistema operativo que necesitan acceder al servidor y a la base de datos. Para obtener más información, consulte Control de acceso y administración de cuentas en la documentación de MySQL.	Administrador de base de datos, administrador de sistemas
Descargue MySQL.	Descargue el software de MySQL. Para obtener instrucciones y archivos binarios, consulte Installing MySQL en la documentación de MySQL.	Administrador de base de datos, administrador de sistemas
Instale MySQL en la instancia de EC2 y configure el servidor.	Conéctese a la instancia de EC2 e instale el software de MySQL. Para obtener más información, consulte Connect to your EC2 instance en la	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	documentación de Amazon EC2.	

Migración de datos: opción 1

Tarea	Descripción	Habilidades requeridas
Migre los datos con herramientas de terceros o de MySQL nativas.	Esta opción utiliza herramientas de MySQL nativas o herramientas de terceros para migrar los objetos y datos de la base de datos. Para obtener instrucciones, consulte la documentación de mysqldump o XtraBackupPercona (para la migración física). Para obtener más información sobre el uso de estas herramientas, consulte la entrada del AWS blog Opciones de migración de MySQL a Amazon RDS for MySQL o Amazon Aurora MySQL.	Administrador de base de datos

Migración de datos: opción 2

Tarea	Descripción	Habilidades requeridas
Migre datos con AWS DMS.	Para obtener más información, consulte la vista de alto nivel de AWS DMS en la AWS DMS documentación.	Administrador de base de datos

Preparación para la transición

Tarea	Descripción	Habilidades requeridas
Reúna recuentos de objetos.	Reúna los recuentos de objetos de la base de datos de origen y de las nuevas bases de datos de destino. Corrija cualquier discrepancia en la base de datos de destino.	Administrador de base de datos
Compruebe las dependencias.	Confirme que las dependenc ias (los enlaces) con destino y origen en otras bases de datos sigan siendo válidas y funcionen correctamente.	Administrador de base de datos
Pruébelo.	Si se trata de un ciclo de pruebas, lleve a cabo pruebas de consulta, recopile métricas y solucione cualquier problema.	Administrador de base de datos

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Traslade los clientes.	Cambie los clientes de la aplicación a la nueva infraestr uctura.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Proporcione soporte.	Proporcione soporte durante las pruebas de aplicaciones funcionales.	Administrador de base de datos

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cierre los recursos.	Cierre la instancia de AWS DMS replicación y otros AWS recursos temporales.	Administrador de base de datos, administrador de sistemas
Revise los documentos del proyecto.	Revise y valide los documento s del proyecto.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Recopile métricas.	Recopile métricas como el tiempo para la migración , el porcentaje de cambios manuales en comparación con los cambios asistidos por herramientas y el ahorro de costos.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Cierre el proyecto.	Cierre el proyecto de migración y envíe sus comentarios.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Reitre del servicio la base de datos de origen.	Retire del servicio la base de datos MySQL en las instalaci ones.	Administrador de base de datos, administrador de sistemas

Recursos relacionados

Referencias

- Documentación de Amazon EC2
- AWS DMS documentación
- Precios de Amazon EC2

- AWS DMS Step-by-Step Tutoriales
- mysqldump
- Percona XtraBackup

Tutoriales y videos

- Empezando con AWS DMS
- Introduction to Amazon EC2 – Elastic Cloud Server & Hosting with AWS (video)

Supervise GoldenGate los registros de Oracle mediante Amazon CloudWatch

Chithra Krishnamurthy, Amazon Web Services

Resumen

Oracle GoldenGate proporciona replicación en tiempo real entre Amazon Relational Database Service (Amazon RDS) para bases de datos Oracle, o entre bases de datos Oracle alojadas en Amazon Elastic Compute Cloud (Amazon EC2). Admite la replicación unidireccional y bidireccional.

Cuando se utiliza GoldenGate para la replicación, la supervisión es fundamental para comprobar que el GoldenGate proceso está en funcionamiento y garantizar que las bases de datos de origen y destino estén sincronizadas.

Este patrón explica los pasos para implementar la CloudWatch supervisión de Amazon para un registro de GoldenGate errores y cómo configurar alarmas para enviar notificaciones de eventos específicos, por ejemplo, para `ABEND` que pueda tomar las medidas adecuadas para reanudar la replicación rápidamente. `STOP`

Requisitos previos y limitaciones

Requisitos previos

- GoldenGate instalado y configurado en una instancia EC2, para que pueda configurar la CloudWatch supervisión en esas instancias EC2. Si desea supervisar la replicación bidireccional GoldenGate en todas las regiones de AWS, debe instalar el CloudWatch agente en cada instancia de EC2 en la que se ejecute el GoldenGate proceso.

Limitaciones

- Este patrón explica cómo monitorear el GoldenGate proceso mediante el uso de. CloudWatch CloudWatch no supervisa el retraso en la replicación ni los problemas de sincronización de datos durante la replicación. Debe ejecutar consultas SQL independientes para controlar el retraso en la replicación o los errores relacionados con los datos, como se explica en la GoldenGate documentación.

Versiones de producto

- Este documento se basa en la implementación de Oracle GoldenGate 19.1.0.0.4 para Oracle en Linux x86-64. Sin embargo, esta solución es aplicable a todas las versiones principales de. GoldenGate

Arquitectura

Pila de tecnología de destino

- GoldenGate binarios para Oracle instalados en una instancia EC2
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)

Arquitectura de destino

Tools (Herramientas)

Servicios de AWS

- Amazon CloudWatch es un servicio de supervisión que se utiliza en este patrón para supervisar los registros GoldenGate de errores.
- Amazon SNS es un servicio de notificación de mensajes que se utiliza en este patrón para enviar notificaciones por correo electrónico.

Otras herramientas

- Oracle GoldenGate es una herramienta de replicación de datos que puede utilizar para las bases de datos Amazon RDS for Oracle o las bases de datos Oracle alojadas en Amazon EC2.

Pasos de implementación de alto nivel

1. Cree un rol de AWS Identity and Access Management (IAM) para el CloudWatch agente.
2. Adjunte la función de IAM a la instancia EC2 en la que se generan los registros GoldenGate de errores.
3. Instale el CloudWatch agente en la instancia EC2.
4. Configure los archivos de configuración del CloudWatch agente: `awscli.conf` `yawslogs.conf`.

5. Inicie el CloudWatch agente.
6. Cree filtros de métricas en el grupo de registros.
7. Configure Amazon SNS.
8. Cree una alarma para los filtros de métricas. Amazon SNS envía alertas por correo electrónico cuando esos filtros capturan eventos.

Para obtener instrucciones, consulte la sección siguiente.

Epics

Paso 1. Cree un rol de IAM para el agente CloudWatch

Tarea	Descripción	Habilidades requeridas
Creación del rol de IAM.	El acceso a los recursos de AWS requiere permisos, por lo que debe crear funciones de IAM para incluir los permisos necesarios para que cada servidor ejecute el CloudWatch agente. Para crear el rol de IAM: 1. Inicie sesión en la consola de administración de AWS y abra la consola de IAM en https://console.aws.amazon.com/iam/. 2. En el panel de navegación, seleccione Roles y luego seleccione Crear rol. 3. En Trusted entity type (Tipo de entidad de confianza), seleccione AWS service. 4. En Common use cases (Casos de uso común),	AWS general

Tarea	Descripción	Habilidades requeridas
	seleccione EC2 y, a continuación, Next. 5. En la lista de políticas, seleccione la casilla de verificación situada junto a CloudWatchAgentServerPolicy. Si es necesario, utilice el cuadro de búsqueda para encontrar la política. 6. Elija Siguiente. 7. En Role name (Nombre del rol), escriba un nombre para el rol nuevo (por ejemplo, `goldengate-cw-monitoring-role` o el nombre que prefiera). 8. (Opcional) En Role description (Descripción del rol), escriba una descripción. 9. Confirme que CloudWatchAgentServerPolicy aparece en el nombre de la política. 10. (Opcional) Agregue una o varias etiquetas (pares clave-valor) para organizar o controlar el acceso a este rol o realizar su seguimiento y, a continuación, seleccione Create role (Crear rol).	

Paso 2. Adjunte la función de IAM a la instancia GoldenGate EC2

Tarea	Descripción	Habilidades requeridas
Adjunte la función de IAM a la instancia EC2 en la que se generan los registros de GoldenGate errores.	Los registros de errores generados por GoldenGate deben rellenarse CloudWatch y supervisarse, por lo que debe adjuntar la función de IAM que creó en el paso 1 a la instancia de EC2 en la que se está ejecutando. GoldenGate Para asociar un rol de IAM a una instancia: 1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/. 2. En el panel de navegación, elija Instances y, a continuación, busque la instancia en la que se GoldenGate está ejecutando. 3. Seleccione la instancia y, a continuación, Actions (Acciones), Security (Seguridad), Modify IAM role (Cómo modificar el rol de IAM). 4. Seleccione el rol de IAM creado en el primer paso para asociarlo con la instancia y seleccione Save (Guardar).	AWS general

Pasos 3 a 5. Instale y configure el CloudWatch agente en la instancia EC2 de Goldengate

Tarea	Descripción	Habilidades requeridas
Instale el CloudWatch agente en la instancia EC2. GoldenGate	Para instalar el agente, ejecute el siguiente comando: `sudo yum install -y awslogs`	AWS general

Edite los archivos de configuración del agente.	1. Ejecute el comando siguiente.
	`sudo su -`
	2. Edite este archivo para actualizar la región de AWS según sea necesario.
	`cat /etc/awslogs/conf [plugins] cwlogs = cwlogs [default] region = us-east-1`
	3. Edite el `/etc/awslogs/awslogs.conf` archivo para actualizar el nombre del archivo, el nombre del grupo de registros y el date/time formato. Debe especificarlo date/time para que coincida con el formato de fecha`ggserror.log` ; de lo contrario, el flujo de registro no fluirá hacia él CloudWatch. Por ejemplo:
		AWS general

Tarea	Descripción	Habilidades requeridas

	`datetime_format = %Y-%m-%dT%H:%M:%S%z`
	`file = /u03/oracle/oragg/ggserr.log`
	`log_group_name = goldengate_monitor`	

Inicie el CloudWatch agente.	Para iniciar el agente, utilice el comando siguiente. `$ sudo service awslogsd start` Tras iniciar el agente, podrá ver el grupo de registros en la CloudWatch consola. El flujo de registro incluirá el contenido del archivo.	AWS general

Paso 6. Crear filtros de métricas en el grupo de registros

Tarea	Descripción	Habilidades requeridas
Cree filtros de métricas para las palabras clave ABEND y STOPPED.	Al crear filtros de métricas para el grupo de registros , cada vez que los filtros se identifican en el registro de errores, se activa una alarma y se envía una notificación por correo electrónico basada en la configuración de Amazon SNS. Para crear un filtro de métricas:	CloudWatch

Tarea	Descripción	Habilidades requeridas
	1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/. 2. Elija el nombre del grupo de registro. 3. Elija Actions (Acciones) y, a continuación, seleccione Create metric filter (Crear filtro de métrica). 4. En Filter pattern (Patrón de filtro), especifique un patrón como `ABEND`. 5. Elija Next (Siguiente) y luego ingrese un nombre para el filtro de métricas. 6. En Detalles de la métrica, en Espacio de nombres métrico, introduzca un nombre para el espacio de CloudWatch nombres en el que se publicará la métrica. Si este espacio de nombres no existe todavía, asegúrese de que la opción Create new (Crear nuevo) esté seleccionada. 7. En Metric value (Valor de la métrica), especifique 1, ya que el filtro de métrica cuenta las ocurrencias de las palabras clave en el filtro.	

Tarea	Descripción	Habilidades requeridas
	8. Defina Unit como None (Ninguna). 9. Elija Create metric filter (Crear filtro de métricas). Puede encontrar el filtro de métricas que ha creado desde el panel de navegación. 10. Cree otro filtro de métricas para el patrón `STOPPED`. Dentro de un grupo de registros, puede crear varios filtros de métricas y configurar las alarmas de forma individual.	

Paso 7. Configurar Amazon SNS

Tarea	Descripción	Habilidades requeridas
Cree un tema de SNS.	En este paso, configurará Amazon SNS para crear alarmas para los filtros de métricas. Para crear un tema de SNS: 1. Inicia sesión en la consola Amazon SNS de tu casahttps://console.aws.amazon.com/sns/. 2. En Create topic (Crear tema), escriba el nombre de su tema como `goldengat`	Amazon SNS

Tarea	Descripción	Habilidades requeridas
	`e-alert` y, a continuación, seleccione Next step (Paso siguiente). 3. En Tipo, seleccione Estándar. 4. Desplácese hasta el final del formulario y elija Create topic (Crear tema). En la consola se abre la página Details (Detalles) del nuevo tema.	

Tarea	Descripción	Habilidades requeridas
Cree una suscripción.	Para crear una suscripción al tema: 1. En el panel de navegación izquierdo, elija Suscripciones. 2. En la página Subscriptions (Suscripciones), elija Create subscription (Crear suscripción). 3. En la página Create subscription (Crear una suscripción), seleccione el campo Topic ARN (ARN del tema) para ver una lista de los temas de la cuenta de AWS. 4. Elija el tema que creó en el paso anterior. 5. En Protocolo, elige Correo electrónico. 6. En Endpoint (Punto de conexión), ingrese una dirección de correo electrónico que pueda utilizar para recibir notificaciones. 7. Seleccione Create subscription (Crear suscripción). La consola abre la página Details (Detalles) de la suscripción.	Amazon SNS

Tarea	Descripción	Habilidades requeridas
	8. Revise la bandeja de entrada del correo electrónico en busca de un mensaje de AWS Notifications y, a continuación, seleccione Confirm subscription (Confirmar la suscripción) en el correo electrónico. En Amazon SNS, se abre su navegador web y se muestra una confirmación de suscripción con su ID de suscripción.	

Paso 8. Crear una alarma para enviar notificaciones a los filtros de métricas

Tarea	Descripción	Habilidades requeridas
Cree una alarma para el tema de SNS.	Para crear una alarma basada en un filtro de métricas del grupo de registros: 1. Abra la CloudWatch consola en. https://console.aws.amazon.com/cloudwatch/ 2. En el panel de navegación, elija Logs (Registros) y, luego, Log groups (Grupos de registro). 3. Elija el grupo de registro que incluye el filtro de métricas.	CloudWatch

Tarea	Descripción	Habilidades requeridas
	4. Elija Metric filters (Filtros de métricas). 5. En la pestaña Metric filters (Filtros de métricas) , seleccione la casilla del filtro de métricas en el que quiera basar la alarma. 6. Elija Crear alarma. 7. En Conditions, especifiq ue lo siguiente en cada sección: • En Threshold type (Tipo de umbral), elija Static (Estático). • En Whenever <metric-n ame> is . . ., seleccione Greater (Mayor que). • En than . . ., especifique 0. 8. Elija Siguiente. 9. En Notification: • En Alarm state trigger (Desencadenador de estado de alarma), elija In Alarm (En alarma). • En Send notification to following SNS topic (Enviar notificación para el tema de SNS siguiente), seleccione Select an existing topic (Seleccio nar un tema existente).	

Tarea	Descripción	Habilidades requeridas
	• En la bandeja de correo electrónico, seleccione el tema de Amazon SNS que creó en el paso anterior. 10 Elija Siguiente. 11 En Name and description (Nombre y descripción), ingrese un nombre y una descripción para la alarma. **Note** En la descripción, puede especificar el nombre de la instancia para que el correo electrónico de notificación sea descriptivo. 12 En Preview and create (Previsualizar y crear), compruebe que su configuración sea correcta y seleccione Create alarm (Crear alarma). Tras estos pasos, cada vez que se detecten estos patrones en el archivo de registro de GoldenGate errores (`ggserr.log`) que está supervisando, recibirá	

Tarea	Descripción	Habilidades requeridas
	una notificación por correo electrónico.	

Resolución de problemas

Problema	Solución
El flujo de registro del registro de GoldenGate errores no fluye hacia él CloudWatch.	Compruebe el `/etc/awslogs/awslogs.conf` archivo para comprobar el nombre del archivo, el nombre del grupo de registros y el date/time formato. Debe especificar el formato de fecha date/time para que coincida con el formato de fecha`ggserror.log` . De lo contrario, el flujo de registro no fluirá hacia CloudWatch.

Recursos relacionados

- CloudWatch Documentación de Amazon
- Recopilación de métricas y registros con el CloudWatch agente
- Documentación de Amazon SNS

Redefina la plataforma de Oracle Database Enterprise Edition a Standard Edition 2 en Amazon RDS para Oracle

Lanre (Lan-Ray) showunmi y Tarun Chawla, Amazon Web Services

Resumen

Oracle Database Enterprise Edition (EE) es una opción popular para ejecutar aplicaciones en muchas empresas. Sin embargo, en algunos casos, las aplicaciones utilizan pocas o ninguna de las características de Oracle Database EE, por lo que no está justificado incurrir en enormes costos de licencia. Puede ahorrar costes al degradar dichas bases de datos a Oracle Database Standard Edition 2 (SE2) al migrar a Amazon RDS.

Este patrón describe cómo pasar de Oracle Database EE a Oracle Database SE2 al migrar de una base de datos local a Amazon RDS for Oracle. Los pasos que se presentan en este patrón también se aplican si la base de datos EE Oracle ya se está ejecutando en Amazon RDS o en una instancia de Amazon Elastic Compute Cloud (Amazon EC2).

Para obtener más información, consulte la guía Recomendaciones de AWS sobre cómo evaluar el cambio de versión de las bases de datos de Oracle a la edición estándar 2 en AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Oracle Database Enterprise Edition
- Una herramienta de cliente, como Oracle SQL Developer o SQL*Plus, para conectarse a oo ejecutar comandos SQL en la base de datos de Oracle
- Usuario de base de datos para realizar la evaluación; por ejemplo, uno de los siguientes:
  - Usuario con privilegios suficientes para ejecutar la evaluación de la Herramienta de conversión de esquemas de AWS (AWS SCT)
  - Usuario con privilegios suficientes para ejecutar consultas SQL en las tablas del diccionario de bases de datos de Oracle
- Usuario de base de datos para realizar la migración de base de datos; por ejemplo, uno de los siguientes:
  - Usuario con privilegios suficientes para ejecutar AWS Database Migration Service (AWS DMS)

- Usuario con privilegios suficientes para realizar la exportación e importación de Oracle Data Pump
- Usuario con privilegios suficientes para ejecutar Oracle GoldenGate

Limitaciones

- Amazon RDS para Oracle tiene un tamaño máximo de la base de datos. Para obtener más información, consulte Almacenamiento de instancias de base de datos de Amazon RDS.

Versiones de producto

La lógica general descrita en este documento se aplica a las versiones de Oracle de la versión 9i y posteriores. Para ver las versiones compatibles de las bases de datos autogestionadas y de Amazon RDS para Oracle, consulte la documentación de AWS DMS.

Para identificar el uso de características en los casos en que no se admite AWS SCT, ejecute consultas SQL en la base de datos de origen. Para migrar desde versiones anteriores de Oracle en las que no se admiten AWS DMS y Oracle Data Pump, utilice las utilidades de exportación e importación de Oracle.

Para obtener una lista actualizada de las versiones y ediciones compatibles, consulte Oracle en Amazon RDS en la documentación de AWS. Para obtener más información sobre los precios y las clases de instancias compatibles, consulte Precios de Amazon RDS para Oracle.

Arquitectura

Pila de tecnología de origen

- Oracle Database Enterprise Edition que se ejecuta en las instalaciones o en Amazon EC2

Pila de tecnología de destino con herramientas nativas de Oracle

- Amazon RDS para Oracle con Oracle Database SE2

1. Exporte datos mediante Oracle Data Pump.
2. Copie los archivos de volcado a Amazon RDS a través de un enlace a una base de datos.

3. Importe los archivos de volcado a Amazon RDS mediante Oracle Data Pump.

Pila de tecnología de destino con AWS DMS

- Amazon RDS para Oracle con Oracle Database SE2
- AWS DMS

1. Exporte datos mediante Oracle Data Pump con FLASHBACK_SCN.
2. Copie los archivos de volcado a Amazon RDS a través de un enlace a una base de datos.
3. Importe los archivos de volcado a Amazon RDS mediante Oracle Data Pump.
4. Utilice la captura de datos de cambio de AWS DMS (CDC).

Tools (Herramientas)

Servicios de AWS

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS. Este patrón utiliza Amazon RDS para Oracle.
- AWS SCT ofrece una interfaz de usuario basada en proyectos para evaluar, convertir y copiar automáticamente el esquema de base de datos de su base de datos de Oracle de origen a un formato compatible con Amazon RDS para Oracle. AWS SCT le permite analizar los posibles ahorros de costos que se pueden lograr al cambiar el tipo de licencia de Enterprise Edition a Standard Edition de Oracle. La sección Evaluación de licencias y soporte en la nube del informe SCT de AWS proporciona información detallada sobre las características de Oracle en uso para que pueda tomar una decisión informada al migrar a Amazon RDS para Oracle.

Otras herramientas

- Las utilidades de importación y exportación nativas de Oracle admiten mover datos de Oracle dentro y fuera de las bases de datos de Oracle. Oracle ofrece dos tipos de utilidades de importación y exportación de bases de datos: Oracle Export and Import (para versiones anteriores)

y Oracle Data Pump Export and Import (disponible en Oracle Database 10g y versiones posteriores).

- Oracle GoldenGate ofrece capacidades de replicación en tiempo real para que pueda sincronizar la base de datos de destino después de una carga inicial. Esta opción puede ayudar a reducir el tiempo de inactividad de las aplicaciones durante la puesta en marcha.

Epics

Realice una evaluación previa a la migración

Tarea	Descripción	Habilidades requeridas
Valide los requisitos de la base de datos para sus aplicaciones.	Asegúrese de que sus aplicaciones estén certificadas para ejecutarse en Oracle SE2 Database. Consulte directamente con el proveedor del software, el desarrollador o la documentación de la aplicación.	Desarrollador de aplicaciones, administrador de bases de datos, propietario de la aplicación
Investigue el uso de las características de EE directamente en la base de datos.	Para determinar el uso de la característica EE, lleve a cabo alguna de las siguientes operaciones: • Genere un informe de evaluación de AWS SCT para su base de datos de Oracle EE. El informe le indica qué características de su base de datos EE actual deberían eliminarse si desea cambiar el tio de licencia. • Si tiene una cuenta de Oracle Support, obtenga y	Propietario de la aplicación, administrador de base de datos, desarrollador de la aplicación

Tarea	Descripción	Habilidades requeridas
	ejecute el script `options_packs_usage_statistics.sql` del documento de soporte 1317265.1 para generar un informe de las opciones y características que se utilizan en la base de datos de Oracle. • Consulte DBA_FEATURE_USAGE_STATISTICS para ver los detalles de todas las características que están en uso.	

Tarea	Descripción	Habilidades requeridas
Identifique el uso de las características de EE para las actividades operativas.	Los administradores de bases de datos o aplicaciones a veces utilizan características exclusivas de EE para sus actividades operativas. Algunos ejemplos comunes incluyen las actividades de mantenimiento en línea (reconstrucción de índices, movimiento de tablas) y el uso del paralelismo en los trabajos por lotes. Estas dependencias se pueden mitigar modificando las operaciones siempre que sea posible. Identifique el uso de estas características y tome una decisión basada en el costo en comparación con los beneficios. Utilice la tabla de comparación de Oracle Database EE y sus SE2 características como guía para identificar las funciones que están disponibles en Oracle Database SE2.	Desarrollador de aplicaciones, administrador de bases de datos, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Revise los patrones de carga de trabajo de la base de datos EE Oracle.	Oracle Database restringe SE2 automáticamente el uso a un máximo de 16 subprocesos de CPU en cualquier momento. Si su base de datos Oracle EE tiene licencia para utilizar el paquete de diagnóstico de Oracle, utilice la herramienta Automatic Workload Repository (AWR), o las vistas DBA_HIST_*, para analizar los patrones de carga de trabajo de la base de datos y determinar si el límite máximo de 16 subprocesos de la CPU afectará negativamente a los niveles de servicio cuando pase a una versión inferior a. SE2 Asegúrese de que su evaluación cubra los períodos de máxima actividad, como el procesamiento al final del día, del mes o del año.	Propietario de la aplicación, administrador de base de datos, desarrollador de la aplicación

Prepare la infraestructura de destino en AWS

Tarea	Descripción	Habilidades requeridas
Implemente y configure la infraestructura de redes.	Cree una nube privada virtual (VPC) y subredes, grupos de	Administrador de AWS, arquitecto de nube, administr

Tarea	Descripción	Habilidades requeridas
	seguridad y listas de control de acceso a la red.	ador de redes, DevOps ingeniero
Aprovisione la base de datos Amazon RDS for SE2 Oracle.	Aprovisione la base de datos Amazon RDS for SE2 Oracle de destino para cumplir con los requisitos de rendimiento, disponibilidad y seguridad de sus aplicaciones. Recomendamos zonas de disponibilidad múltiples para las cargas de trabajo de producción. Sin embargo, para mejorar el rendimiento de la migración, puede aplazar la activación de zonas de disponibilidad múltiples hasta después de la migración de datos.	Administrador de nube, arquitecto de nube, DBA, DevOps ingeniero, administrador de AWS
Personalice el entorno de Amazon RDS.	Configure parámetros y opciones personalizados y habilite una supervisión adicional. Para obtener más información, consulte Prácticas recomendadas para migrar a Amazon RDS para Oracle.	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube, administrador de bases de datos, arquitecto de la nube

Realice la migración, el simulacro y las pruebas de la aplicación

Tarea	Descripción	Habilidades requeridas
Migre los datos (simulacro).	Migre los datos de la base de datos Oracle EE de origen a la instancia de base de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	datos Amazon RDS for SE2 Oracle utilizando el enfoque que mejor se adapte a su entorno específico. Seleccione una estrategia de migración en función de factores como el tamaño, la complejidad y el período de inactividad disponible. Use una de las siguientes o una combinación de ellas: • Herramientas nativas de Oracle, como Oracle Data Pump (recomendada), las utilidades Oracle Import-Export y Oracle. GoldenGate • AWS DMS, que utiliza toda la carga con replicación continua a través de CDC.	
Validar la base de datos objetivo.	Realice una validación posterior a la migración del almacenamiento de la base de datos y de los objetos de código. Revise los registros de migración y solucione los problemas detectados. Para obtener más información, consulte la guía Migración de bases de datos de Oracle a la nube de AWS.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Pruebe las aplicaciones.	Los administradores de aplicaciones y bases de datos deben realizar pruebas funcionales, de rendimien to y operativas según corresponda. Para obtener más información, consulte Prácticas recomendadas para migrar a Amazon RDS para Oracle. Por último, obtenga la aprobación de las partes interesadas sobre los resultados de las pruebas.	Desarrollador de aplicaciones, propietario de aplicaciones, ingeniero de migraciones, líder de migración

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Actualice los datos de Oracle Database EE.	Seleccione un enfoque de actualización de datos en función del requisito de disponibilidad de la aplicació n. Para obtener más informaci ón, consulte los métodos de migración en Estrategias de migración de bases de datos de Oracle a AWS. Por ejemplo, puede lograr un tiempo de inactividad prácticamente nulo mediante el uso de herramientas como Oracle GoldenGate o AWS	Propietario de aplicaciones, jefe de transición, administr ador de base de datos, ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
	DMS con replicación continua. Si el período de inactividad lo permite, puede realizar la transición final de los datos mediante métodos fuera de línea, como Oracle Data Pump o las utilidades Original Export-Import.	
Dirija las aplicaciones a la instancia de la base de datos de destino.	Actualice los parámetros de conexión en las aplicacio nes y otros clientes para que apunten a la base de datos Amazon RDS for SE2 Oracle.	Desarrollador de aplicaciones, propietario de aplicaciones, ingeniero de migraciones, líder de migración, jefe de transició n
Realice actividades posterior es a la migración.	Realice tareas posteriores a la migración de datos, como habilitar las zonas de disponibi lidad múltiples, la validación de datos y otras comprobac iones.	Administrador de base de datos, ingeniero de migracion es
Realice una supervisión posterior a la transición.	Utilice herramientas como Amazon CloudWatch y Amazon RDS Performance Insights para supervisar la base de datos Amazon RDS for SE2 Oracle.	Desarrollador de aplicacio nes, propietario de aplicacio nes, administrador de AWS, administrador de bases de datos, ingeniero de migracion es

Recursos relacionados

Recomendaciones de AWS

- Migración de bases de datos de Oracle a la nube de AWS (guía)
- Evalúe cambiar la versión de las bases de datos de Oracle a Standard Edition 2 en AWS (guía)

- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle (patrón)
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump (patrón)

Publicaciones de blog

- Migración de bases de datos de Oracle con un tiempo de inactividad prácticamente nulo mediante AWS DMS
- Análisis del manejo del rendimiento en Oracle SE mediante Amazon RDS para Oracle
- Administración de su plan SQL en Oracle SE con Amazon RDS para Oracle
- Implementación del particionamiento de tablas en Oracle Standard Edition: primera parte

Replicar bases de datos de unidades centrales en AWS mediante Precisely Connect

Lucio Pereira, Sayantan Giri y Balaji Mohan, Amazon Web Services

Resumen

Este patrón describe los pasos para replicar datos de bases de datos de unidades centrales a los almacenes de datos de Amazon casi en tiempo real mediante Precisely Connect. El patrón implementa una arquitectura basada en eventos con Amazon Managed Streaming para Apache Kafka (Amazon MSK) y conectores de bases de datos personalizados en la nube para mejorar la escalabilidad, la resiliencia y el rendimiento.

Precisely Connect es una herramienta de replicación que captura datos de sistemas de unidades centrales heredados y los integra en entornos en la nube. Los datos se replican desde las unidades centrales a AWS mediante la captura de datos de cambios (CDC) mediante flujos de mensajes prácticamente en tiempo real con canalizaciones de datos heterogéneas de baja latencia y alto rendimiento.

Este patrón también abarca una estrategia de recuperación de desastres para canalizaciones de datos resilientes con replicación de datos multirregional y enrutamiento de conmutación por error.

Requisitos previos y limitaciones

Requisitos previos

- Una base de datos de mainframe existente, por ejemplo, IBM DB2, IBM Information Management System (IMS) o Virtual Storage Access Method (VSAM), que desee replicar en la nube de AWS
- Una cuenta de AWS activa
- AWS Direct Connect o red privada virtual de AWS (AWS VPN) desde su entorno corporativo a AWS
- Una nube privada virtual con una subred a la que pueda acceder su plataforma antigua

Arquitectura

Pila de tecnología de origen

Un entorno de unidad central que incluya al menos una de las siguientes bases de datos:

- Base de datos IBM IMS
- DB2 Base de datos de IBM
- Archivos VSAM

Pila de tecnología de destino

- Amazon MSK
- Amazon Elastic Kubernetes Service (Amazon EKS) y Amazon EKS Anywhere
- Docker
- Una base de datos relacional o NoSQL de AWS como la siguiente:
  - Amazon DynamoDB
  - Amazon Relational Database Service (Amazon RDS) para Oracle, Amazon RDS para PostgreSQL o Amazon Aurora
  - Amazon ElastiCache para Redis
  - Amazon Keyspaces (para Apache Cassandra)

Arquitectura de destino

Replicación de datos de unidad central en bases de datos de AWS

El siguiente diagrama ilustra la replicación de datos de mainframe en una base de datos de AWS, como DynamoDB, Amazon RDS, Amazon o Amazon Keyspaces ElastiCache. La replicación se produce prácticamente en tiempo real mediante el uso de Precisely Capture y Publisher en su entorno de unidad central en las instalaciones, Precisely Dispatcher en Amazon EKS Anywhere en su entorno distribuido en las instalaciones y Precisely Apply Engine y los conectores de base de datos en la nube de AWS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Precisely Capture obtiene los datos de unidad central de los registros CDC y los mantiene en un almacenamiento transitorio interno.
2. Precily Publisher escucha los cambios en el almacenamiento interno de datos y envía los registros CDC a Precily Dispatcher a través de una conexión. TCP/IP
3. Precisely Dispatcher recibe los registros de los CDC de Publisher y los envía a Amazon MSK. Dispatcher crea claves de Kafka en función de la configuración del usuario y de varias tareas de

trabajo para enviar los datos en paralelo. Dispatcher envía un acuse de recibo a Publisher cuando los registros se han almacenado en Amazon MSK.

4. Amazon MSK guarda los registros de los CDC en el entorno de nube. El tamaño de las particiones de los temas depende de los requisitos de rendimiento del sistema de procesamiento de transacciones (TPS). La clave de Kafka es obligatoria para seguir ordenando transformaciones y transacciones.
5. Precisely Apply Engine escucha los registros de CDC de Amazon MSK y transforma los datos (por ejemplo, filtrándolos o mapeándolos) en función de los requisitos de la base de datos de destino. Puede añadir una lógica personalizada a los scripts de Precisely SQD. (SQD es el lenguaje propiedad de Precisely). Precisely Apply Engine transforma cada registro de CDC al formato Apache Avro o JSON y lo distribuye a diferentes temas según sus necesidades.
6. Los temas de Kafka de destino contienen los registros CDC en varios temas según la base de datos de destino, y Kafka facilita la ordenación de las transacciones en función de la clave de Kafka definida. Las claves de partición se alinean con las particiones correspondientes para permitir un proceso secuencial.
7. Los conectores de bases de datos (aplicaciones Java personalizadas) escuchan los registros CDC de Amazon MSK y los almacenan en la base de datos de destino.
8. Puede seleccionar una base de datos de destino en función de sus requisitos. Este patrón es compatible con bases de datos NoSQL y relacionales.

Recuperación de desastres

La continuidad empresarial es clave para el éxito de su organización. La nube de AWS proporciona capacidades de alta disponibilidad (HA) y recuperación de desastres (DR), y respalda los planes de conmutación por error y alternativos de su organización. Este patrón sigue una estrategia de active/passive DR y proporciona una guía de alto nivel para implementar una estrategia de DR que cumpla con sus requisitos de RTO y RPO.

En el siguiente diagrama, se ilustra el flujo de trabajo de DR.

En el diagrama se muestra lo siguiente:

1. Se requiere una conmutación por error semiautomática si se produce algún error en la Región de AWS 1. En caso de que se produzca un error en la Región 1, el sistema debe iniciar los cambios de enrutamiento para conectar a Precisely Dispatcher con la Región 2.

2. Amazon MSK replica los datos mediante la duplicación entre regiones. Por este motivo, durante la conmutación por error, hay que promover al clúster de Amazon MSK de la región 2 como líder principal.
3. Precisely Apply Engine y los conectores de bases de datos son aplicaciones sin estado que pueden funcionar en cualquier región.
4. La sincronización de la base de datos depende de la base de datos de destino. Por ejemplo, DynamoDB puede usar tablas globales ElastiCache y almacenes de datos globales.

Procesamiento de baja latencia y alto rendimiento mediante conectores de bases de datos

Los conectores de bases de datos son componentes fundamentales en este patrón. Los conectores siguen un enfoque basado en el oyente para recopilar datos de Amazon MSK y enviar las transacciones a la base de datos mediante un procesamiento de alto rendimiento y baja latencia para aplicaciones de misión crítica (niveles 0 y 1). En el siguiente diagrama se ilustra este proceso.

Este patrón permite desarrollar una aplicación personalizada con un consumo de un solo subproceso mediante un motor de procesamiento de subprocesos múltiples.

1. El proceso principal del conector consume los registros CDC de Amazon MSK y los envía al grupo de subprocesos para su procesamiento.
2. Los subprocesos del grupo de subprocesos procesan los registros de los CDC y los envían a la base de datos de destino.
3. Si todos los subprocesos están ocupados, la cola de subprocesos mantiene en espera los registros de la CDC.
4. El subproceso principal espera a que se borren todos los registros de la cola de subprocesos y envía las compensaciones a Amazon MSK.
5. Los subprocesos secundarios gestionan los errores. Si se producen errores durante el procesamiento, los mensajes fallidos se envían al tema DLQ (cola de mensajes fallidos).
6. Los subprocesos secundarios inician actualizaciones condicionales (consulte Expresiones de condición en la documentación de DynamoDB), en función de la marca de tiempo del mainframe, para evitar cualquier duplicación o actualización en la base de datos. out-of-order

Para obtener información sobre cómo implementar una aplicación de consumidor de Kafka con capacidades de subprocesos múltiples, consulte la entrada del blog Consumo de mensajes multiprocesos con el consumidor de Apache Akfka en el sitio web de Confluent.

Tools (Herramientas)

Servicios de AWS

- Amazon Managed Streaming para Apache Kafka (Amazon MSK) es un servicio completamente administrado que le permite crear y ejecutar aplicaciones que utilizan Apache Kafka para procesar datos de streaming.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar Kubernetes en AWS sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.
- Amazon EKS Anywhere le permite implementar, usar y administrar los clústeres de Kubernetes que se ejecutan en sus propios centros de datos.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- Amazon le ElastiCache ayuda a configurar, gestionar y escalar entornos de caché en memoria distribuidos en la nube de AWS.
- Amazon Keyspaces (para Apache Cassandra) es un servicio de base de datos administrada que le permite migrar, ejecutar y escalar sus cargas de trabajo de Cassandra en la nube de AWS.

Otras herramientas

- Precisely Connect integra los datos de los sistemas de unidad central heredados, como los conjuntos de datos de VSAM o las bases de datos de unidad central de IBM, en plataformas de datos y nube de próxima generación.

Prácticas recomendadas

- Encuentre la mejor combinación de particiones Kafka y conectores multiprocesos para lograr un equilibrio óptimo entre rendimiento y costo. Varias instancias de Precisely Capture y Dispatcher pueden aumentar el costo debido al mayor consumo de MIPS (millones de instrucciones por segundo).
- Evite añadir lógica de manipulación y transformación de datos a los conectores de bases de datos. Para ello, utilice Precisely Apply Engine, que proporciona tiempos de procesamiento en microsegundos.

- Cree solicitudes periódicas o llamadas de comprobación de estado a la base de datos (latidos) en los conectores de la base de datos para calentar la conexión con frecuencia y reducir la latencia.
- Implemente una lógica de validación de grupos de subprocesos para comprender las tareas pendientes en la cola de subprocesos y espere a que se completen todos los subprocesos antes del siguiente sondeo de Kafka. Esto ayuda a evitar la pérdida de datos si un nodo, contenedor o proceso se bloquea.
- Exponga las métricas de latencia a través de puntos de conexión de estado para mejorar las capacidades de observabilidad mediante paneles y mecanismos de rastreo.

Epics

Prepare el entorno de origen (en las instalaciones)

Tarea	Descripción	Habilidades requeridas
Configure el proceso de la unidad central (por lotes o en línea) para iniciar el proceso de CDC desde las bases de datos de la unidad central.	1. Identifique el entorno de unidad central. 2. Identifique las bases de datos de unidad central que participarán en el proceso de los CDC. 3. En el entorno de unidad central, desarrolle un proceso que lance la herramienta de los CDC para capturar los cambios en la base de datos fuente. Para obtener instrucciones, consulte la documentación de su unidad central. 4. Documente el proceso de los CDC, incluida la configuración.	Ingeniero de unidad central

Tarea	Descripción	Habilidades requeridas
	5. Implemente el proceso en entornos de prueba y producción.	
Active los flujos de registro de la base de datos de unidad central.	1. Configure los flujos de registro en el entorno de unidad central para capturar los registros de los CDC. Para obtener instrucciones, consulte la documentación de su unidad central. 2. Pruebe los flujos de registro para asegurarse de que capturan los datos necesarios. 3. Implemente los flujos de registro en entornos de prueba y producción.	Especialista en bases de datos para unidad central

Tarea	Descripción	Habilidades requeridas
Utilice el componente Capture para capturar los registros de los CDC.	1. Instale y configure el componente Precisely Capture en el entorno de la unidad central. Para obtener instrucciones, consulte la documentación de Precisely. 2. Pruebe la configuración para asegurarse de que el componente Capture funciona correctamente. 3. Configure un proceso de replicación para replicar los registros de los CDC capturados mediante el componente Capture. 4. Documente la configuración de Capture para cada base de datos de origen. 5. Desarrolle un sistema de supervisión para garantizar que el componente Capture recopile los registros correctamente a lo largo del tiempo. 6. Implemente la instalación y las configuraciones en los entornos de prueba y producción.	Ingeniero de unidad central, Precisely Connect SME

Tarea	Descripción	Habilidades requeridas
Configure el componente Publisher para que escuche al componente Capture.	1. Instale y configure el componente Precisely Publisher en el entorno de la unidad central. Para obtener instrucciones, consulte la documentación de Precisely. 2. Pruebe la configuración para asegurarse de que el componente Publisher funciona correctamente. 3. Configure un proceso de replicación para publicar los registros de CDC en el componente Precisely Dispatcher de Publisher. 4. Documente la configuración de Publisher. 5. Desarrolle un sistema de supervisión para garantizar que el componente Publisher recopile los registros correctamente a lo largo del tiempo. 6. Implemente la instalación y las configuraciones en los entornos de prueba y producción.	Ingeniero de unidad central, Precisely Connect SME

Tarea	Descripción	Habilidades requeridas
Aprovisione Amazon EKS Anywhere en el entorno distribuido en las instalaciones.	1. Instale Amazon EKS Anywhere en la infraestructura en las instalaciones y asegúrese de que esté configurado correctamente. Para obtener instrucciones, consulte la documentación de Amazon EKS Anywhere. 2. Configure un entorno de red seguro para el clúster de Kubernetes, incluidos los firewalls. 3. Implemente y pruebe la implementación de la aplicación de muestra en el clúster Amazon EKS Anywhere. 4. Implemente capacidades de escalado automático para el clúster. 5. Desarrolle e implemente procedimientos de copia de seguridad y recuperación de desastres.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Implemente y configure el componente Dispatcher en el entorno distribuido para que publique los temas en la nube de AWS.	1. Configure y organice en contenedores el componente Precisely Dispatcher. Para obtener instrucciones, consulte la documentación de Precisely. 2. Implemente la imagen de Docker de Dispatcher en el entorno en las instalaciones de Amazon EKS Anywhere. 3. Configure una conexión segura entre la nube de AWS y Dispatcher. 4. Desarrolle un sistema de supervisión para garantizar que el componente Dispatcher recopile los registros correctamente a lo largo del tiempo. 5. Implemente la instalación y las configuraciones en los entornos de prueba y producción.	DevOps ingeniero, Precisely Connect SME

Prepare el entorno de destino (AWS)

Tarea	Descripción	Habilidades requeridas
Aprovisione un clúster de Amazon EKS en la región de AWS designada.	1. Inicie sesión en su cuenta de AWS y configúrela para asegurarse de que cuenta con los permisos necesario	DevOps ingeniero, administrador de redes

Tarea	Descripción	Habilidades requeridas
	s para crear y administrar el clúster de Amazon EKS. 2. Cree una nube privada virtual (VPC) y subredes en la región de AWS seleccionada. Para obtener instrucciones, consulte la documentación de Amazon EKS. 3. Cree y configure los grupos de seguridad de red necesarios para permitir las comunicaciones entre el clúster de Amazon EKS y otros recursos de la VPC. Para obtener más informaci ón, consulte la documenta ción de Amazon EKS. 4. Cree el clúster de Amazon EKS y configúrelo con el tamaño de grupo de nodos y los tipos de instancias correctos. 5. Valide el clúster de Amazon EKS mediante la implement ación de una aplicación de muestra.	

Tarea	Descripción	Habilidades requeridas
Aprovisione un clúster de MSK y configure los temas de Kafka aplicables.	1. Configure su cuenta de AWS para asegurarse de que cuenta con los permisos necesarios para crear y administrar el clúster de MSK. 2. Cree y configure los grupos de seguridad de red necesarios para permitir las comunicaciones entre el clúster MSK y otros recursos de la VPC. Para obtener más información, consulte la documentación de Amazon VPC. 3. Cree el clúster de MSK y configúrelo para que incluya los temas de Kafka que utilizará la aplicación. Para obtener más información, consulte la documentación de Amazon MSK.	DevOps ingeniero, administrador de red

Tarea	Descripción	Habilidades requeridas
Configure el component e Apply Engine para que escuche los temas de Kafka replicados.	1. Configure y organice en contenedores el component e Precisely Apply Engine. 2. Implemente la imagen de Docker de Apply Engine en el clúster de Amazon EKS de su cuenta de AWS. 3. Configure Apply Engine para que escuche los temas de MSK. 4. Desarrolle y configure un script SQD en Apply Engine para gestionar el filtrado y la transformación. Para obtener más información, consulte la documentación de Precisely. 5. Implemente Apply Engine en entornos de prueba y producción.	Precisely Connect SME

Tarea	Descripción	Habilidades requeridas
Aprovisione instancias de base de datos en la nube de AWS.	1. Configure su cuenta de AWS para asegurarse de que cuenta con los permisos necesarios para crear y administrar los clústeres y tablas de bases de datos. Para obtener instrucciones, consulte la documentación de AWS del servicio de base de datos de AWS que desee utilizar. (Consulte los enlaces en la sección de recursos). 2. Cree una VPC y subredes en la región de AWS seleccionada. 3. Cree y configure los grupos de seguridad de red necesarios para permitir las comunicaciones entre las instancias de bases de datos y otros recursos de la VPC. 4. Cree las bases de datos y configúrelas para que incluyan las tablas que utilizará la aplicación. 5. Diseñe y valide los esquemas de las bases de datos.	Ingeniero de datos, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Configure e implemente conectores de bases de datos para que escuchen los temas publicados por Apply Engine.	1. Diseñe conectores de bases de datos para conectar los temas de Kafka con las bases de datos de AWS que creó en los pasos anteriores. 2. Desarrolle los conectores en función de la base de datos de destino. 3. Configure los conectores para que escuchen los temas de Kafka publicados por Apply Engine. 4. Implemente los conectores en el clúster de Amazon EKS.	Desarrollador de aplicaciones, arquitecto de la nube, ingeniero de datos

Configure la continuidad empresarial y la recuperación de desastres

Tarea	Descripción	Habilidades requeridas
Defina los objetivos de recuperación de desastres para sus aplicaciones empresariales.	1. Defina los objetivos de RPO y RTO para las canalizaciones de datos CDC en función de las necesidades de su empresa y del análisis de impacto. 2. Defina los procedimientos de comunicación y notificación para garantizar que todas las partes interesadas conozcan el plan de recuperación de desastres.	Arquitecto de la nube, ingeniero de datos, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	3. Determine el presupuesto y los recursos necesarios para implementar el plan de recuperación de desastres. 4. Documente los objetivos de recuperación de desastres , incluidos los objetivos de RPO y RTO.	

Tarea	Descripción	Habilidades requeridas
Diseñe estrategias de recuperación de desastres basadas en un RTO/RPO definido.	1. Determine las estrategias de recuperación de desastres más adecuadas para las canalizaciones de CDC en función de su jerarquía de importancia y sus requisitos de recuperación. 2. Defina la arquitectura y la topología de la recuperación de desastres. 3. Defina los procedimientos de conmutación por error y conmutación por recuperación de las canalizaciones de CDC para garantizar que puedan conmutar de forma rápida y sin problemas a la región de respaldo. 4. Documente las estrategias y los procedimientos de recuperación de desastres y asegúrese de que todas las partes interesadas comprendan claramente el diseño.	Arquitecto de la nube, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
Aprovisione clústeres y configuraciones de recuperación de desastres.	1. Aprovisione una región de AWS secundaria para la recuperación de desastres. 2. En la región de AWS secundaria, cree un entorno que sea idéntico a la región de AWS principal. 3. Configure Apache Kafka MirrorMaker entre las regiones principal y secundaria. Para obtener más información, consulte la documentación de Amazon MSK. 4. Configure las aplicaciones en espera en la región secundaria. 5. Configure las replicaciones de bases de datos entre las regiones principal y secundaria.	DevOps ingeniero, administrador de redes, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
Ponga a prueba la capacidad de recuperación de desastres de la canalización de CDC.	1. Defina el alcance y los objetivos de la prueba de recuperación de desastres de la canalización de CDC, incluidos los escenarios de prueba y el RTO que deben lograrse. 2. Identifique el entorno y la infraestructura de prueba para realizar la prueba de recuperación de desastres. 3. Prepare los conjuntos de datos y el script de la prueba para simular los escenarios de error. 4. Verifique la integridad y la coherencia de los datos para garantizar que no se pierdan datos.	Propietario de aplicaciones, ingeniero de datos, arquitecto de la nube

Recursos relacionados

Recursos de AWS

- Amazon DynamoDB
- Expresiones de condición con Amazon DynamoDB
- Amazon EKS
- Amazon EKS Anywhere
- Amazon ElasticCache
- Amazon Keyspaces
- Amazon MSK
- Amazon RDS y Amazon Aurora

- Amazon VPC

Recursos de Precisely Connect

- Descripción general de Precisely Connect
- Captura de datos de cambio con Precise Connect

Recursos Confluent

- Consumo de mensajes multiproceso con Apache Kafka Consumer

Programe trabajos para Amazon RDS para PostgreSQL y Aurora PostgreSQL mediante Lambda y Secrets Manager

Yaser Raja, Amazon Web Services

Resumen

En el caso de las bases de datos locales y las bases de datos alojadas en instancias de Amazon Elastic Compute Cloud (Amazon EC2), los administradores de bases de datos suelen utilizar la utilidad cron para programar los trabajos.

Por ejemplo, un trabajo de extracción de datos o un trabajo de purga de datos se puede programar fácilmente mediante con cron. Para estos trabajos, las credenciales de la base de datos suelen tener una codificación rígida o estar almacenadas en un archivo de propiedades. Sin embargo, al migrar a Amazon Relational Database Service (Amazon RDS) o a Amazon Aurora PostgreSQL Compatible Edition, pierde la capacidad de iniciar sesión en la instancia host para programar trabajos cron.

Este patrón describe cómo usar AWS Lambda y programar trabajos para bases de datos compatibles AWS Secrets Manager con Amazon RDS for PostgreSQL y Aurora PostgreSQL después de la migración.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Una base de datos compatible con Amazon RDS para PostgreSQL o Aurora PostgreSQL

Limitaciones

- Un trabajo debe completarse en 15 minutos, que es el límite de tiempo de espera de la función de Lambda. Para ver otros límites, consulte la documentación de AWS Lambda.
- El código de trabajo debe escribirse en un lenguaje compatible con Lambda.

Arquitectura

Pila de tecnología de origen

Esta pila incluye tareas escritas en lenguajes como Bash, Python y Java. Las credenciales de la base de datos se almacenan en el archivo de propiedades y el trabajo se programa usando cron de Linux.

Pila de tecnología de destino

Esta pila tiene una función de Lambda que usa las credenciales almacenadas en Secrets Manager para conectarse a la base de datos y realizar la actividad. La función Lambda se inicia en el intervalo programado mediante Amazon CloudWatch Events.

Arquitectura de destino

Tools (Herramientas)

- Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en AWS los recursos. Con reglas sencillas que puede configurar rápidamente, puede hacer coincidir los eventos y dirigirlos a una o más funciones o transmisiones de destino. CloudWatch Los eventos se dan cuenta de los cambios operativos a medida que se producen. Responde a estos cambios operativos y toma medidas correctoras según sea necesario, enviando mensajes para responder al entorno, activando funciones, realizando cambios y captando información de estado. También puedes usar CloudWatch Events para programar acciones automatizadas que se inicien automáticamente en determinados momentos mediante expresiones cron o rate.
- AWS Lambda es un servicio automático que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo se paga el tiempo de computación que se consume; no hay ningún cargo mientras el código no se ejecuta. Con Lambda puede ejecutar código para prácticamente cualquier tipo de aplicación o servicio de backend, sin ningún esfuerzo de administración. Lambda ejecuta el código en una infraestructura informática de alta disponibilidad y realiza todas las tareas de administración de los recursos informáticos, incluidos el mantenimiento del servidor y del sistema operativo, el aprovisionamiento de capacidad y el escalado automático, así como la supervisión del código y las funciones de registro. Lo único que tiene que hacer es proporcionar el código en uno de los lenguajes que admite Lambda.
- AWS Secrets Manager le permite proteger los secretos necesarios para acceder a sus aplicaciones, servicios y recursos de TI. Puede rotar, administrar y recuperar fácilmente credenciales de bases de datos, claves de API y otros datos confidenciales durante todo su ciclo de vida. Los usuarios y las aplicaciones recuperan los secretos llamando a Secrets Manager APIs, lo que elimina la necesidad de codificar información confidencial en texto plano. Secrets

Manager ofrece una rotación de secretos con una integración incorporada para Amazon RDS, Amazon Redshift y Amazon DocumentDB. El servicio se puede extender a otros tipos de secretos, incluidas las claves y OAuth los tokens de API. Secrets Manager le permite controlar el acceso a los secretos mediante permisos detallados y auditar la rotación de secretos de forma centralizada para detectar los recursos en los Nube de AWS servicios de terceros y en las instalaciones.

Epics

Almacenar credenciales de base de datos en Secrets Manager

Tarea	Descripción	Habilidades requeridas
Creación de un usuario de una base de datos para la función de Lambda.	Es una buena práctica utilizar usuarios de bases de datos independientes para las distintas partes de la aplicación. Si ya existe un usuario de base de datos independiente para sus trabajos cron, utilícelo. De lo contrario, cree un nuevo usuario de base de datos. Para obtener más información, consulte Administración de usuarios y roles de PostgreSQLAWS (entrada del blog).	Administrador de base de datos
Almacene las credenciales de las bases de datos como un secreto en Secrets Manager.	Siga las instrucciones de Crear un secreto de base de datos (documentación de Secrets Manager).	DBA, DevOps

Autor del código para la función de Lambda

Tarea	Descripción	Habilidades requeridas
Elija un lenguaje de programación compatible con Lambda.	Para obtener una lista de los lenguajes compatibles, consulte los tiempos de ejecución de Lambda (documentación de Lambda).	Desarrollador
Escriba la lógica para obtener las credenciales de la base de datos de Secrets Manager.	Para ver un ejemplo de código, consulte Cómo proporcionar de forma segura credenciales de bases de datos a funciones Lambda mediante AWS Secrets Manager (entrada del AWS blog).	Desarrollador
Escriba la lógica para realizar la actividad programada de la base de datos.	Migre el código existente para el trabajo de programación que está utilizando en las instalaciones a la función de Lambda. Para más información, consulte Implementación de funciones de Lambda (documentación de Lambda).	Desarrollador

Implemente el código y cree la función de Lambda

Tarea	Descripción	Habilidades requeridas
Cree el paquete de implementación de funciones de Lambda.	Este paquete contiene el código y sus dependencias. Para obtener más información, consulte Paquetes de	Desarrollador

Tarea	Descripción	Habilidades requeridas
	implementación (document ación de Lambda).	
Crear la función de Lambda.	En la consola de Lambda, elija Crear función, ingrese el nombre de una función, elija el entorno de tiempo de ejecución y, a continuación, elija Crear función.	DevOps
Cargue el paquete de implementación.	Elija la función de Lambda que creó para abrir su configura ción. Puede escribir el código directamente en la sección de códigos o cargar el paquete de implementación. Para cargar su paquete, vaya a la sección Function code (Código de función), elija el Code entry type (tipo de entrada de código) para cargar un archivo .zip y, a continuación, seleccione el paquete.	DevOps
Configure la función de Lambda según sus requisitos.	Por ejemplo, puede establece r el parámetro Tiempo de espera a la duración que espera que dure la función de Lambda. Para obtener más información, consulte Configuración de las opciones de las funciones (document ación de Lambda).	DevOps

Tarea	Descripción	Habilidades requeridas
Establezca los permisos para que el rol de la función de Lambda acceda a Secrets Manager.	Para obtener instrucciones, consulte Usar secretos en AWS Lambda las funciones (documentación de Secrets Manager).	DevOps
Pruebe la función de Lambda.	Inicie la función de Lambda manualmente para asegurarse de que funciona según lo esperado.	DevOps

Programe la función Lambda mediante eventos CloudWatch

Tarea	Descripción	Habilidades requeridas
Cree una regla para ejecutar su función de Lambda de manera programada.	Programe la función Lambda mediante CloudWatch Eventos. Para obtener instrucciones, consulte Programar funciones de Lambda mediante CloudWatch eventos (tutorial sobre CloudWatch eventos).	DevOps

Recursos relacionados

- AWS Secrets Manager
- Introducción a Lambda
- Creación de una regla de CloudWatch eventos que se active en un evento
- AWS Lambda Límites
- Consulte su AWS base de datos desde su aplicación sin servidor (entrada de blog)

Envíe notificaciones para una instancia de base de datos de Amazon RDS para SQL Server mediante un servidor SMTP en las instalaciones y el Correo de base de datos

Nishad Mankar, Amazon Web Services

Resumen

Correo de base de datos (documentación de Microsoft) envía mensajes de correo electrónico, como notificaciones o alertas, desde una base de datos de Microsoft SQL Server mediante un servidor de Protocolo simple de transferencia de correo (SMTP). La documentación del Amazon Relational Database Service (Amazon RDS) para Microsoft SQL Server proporciona instrucciones para utilizar Amazon Simple Email Service (Amazon SES) como servidor SMTP para el Correo de base de datos. Para obtener más información, consulte Uso de Database Mail en Amazon RDS for SQL Server. Como configuración alternativa, este patrón explica cómo configurar la base de datos para enviar correos electrónicos desde una instancia de base de datos (DB) de Amazon RDS para SQL Server mediante un servidor SMTP en las instalaciones como servidor de correo.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una instancia de base de datos de Amazon RDS que ejecute una edición Standard o Enterprise de SQL Server
- La dirección IP o el nombre de host del servidor SMTP local.
- Una regla de grupo de seguridad entrante que permite las conexiones a la instancia de base de datos de Amazon RDS para SQL Server desde la dirección IP del servidor SMTP
- Una conexión, como una conexión AWS Direct Connect, entre la red en las instalaciones y la nube privada virtual (VPC) que contiene la instancia de base de datos de Amazon RDS

Limitaciones

- No se admiten las ediciones Express de SQL Server.
- Para obtener más información sobre las limitaciones, consulte Limitaciones en Uso del Correo de base de datos en Amazon RDS para SQL Server en la documentación de Amazon RDS.

Versiones de producto

- RDS admite las versiones Standard y Enterprise de SQL Server

Arquitectura

Pila de tecnología de destino

- Instancia de base de datos de Amazon RDS para SQL Server
- Amazon Route 53 (Amazon Route 53)
- Correo electrónico de base de datos
- Host local del servidor SMTP
- Microsoft SQL Server Management Studio (SSMS)

Arquitectura de destino

La siguiente imagen muestra la arquitectura de destino para este patrón. Cuando se produce un evento o una acción que inicia una notificación o alerta relativa a la instancia de base de datos, Amazon RDS para SQL Server utiliza el Correo de base de datos para enviar una notificación por correo electrónico. Correo de base de datos utiliza el servidor SMTP en las instalaciones para enviar el correo electrónico.

Tools (Herramientas)

Servicios de AWS

- Puede utilizar Amazon Relational Database Service (Amazon RDS) para configurar, utilizar y escalar una base de datos relacional de SQL Server en la nube de AWS.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.

Otras herramientas

- Correo de base de datos es una herramienta que envía mensajes de correo electrónico, como notificaciones y alertas, desde el motor de base de datos de SQL Server a los usuarios.

- Microsoft SQL Server Management Studio (SSMS) es una herramienta para administrar SQL Server, que incluye el acceso, la configuración y la administración de los componentes de SQL Server. En este patrón, utiliza SSMS para ejecutar los comandos SQL para configurar Correo de base de datos en una instancia de base de datos de Amazon RDS para SQL Server.

Epics

Habilite la conectividad de red con el servidor SMTP en las instalaciones

Tarea	Descripción	Habilidades requeridas
Elimine Multi-AZ de la instancia de base de datos de RDS.	Si utiliza una instancia de base de datos Multi-AZ, convierta la instancia Multi-AZ en una instancia Single-AZ. Cuando termine de configura r el Correo de base de datos, convertirá la instancia de base de datos de nuevo a una implementación Multi-AZ. La configuración de Database Mail funciona entonces tanto en el nodo primario como en el secundari o. Para más información, consulte Eliminación de Multi-AZ de una instancia de base de datos de Microsoft SQL Server.	Administrador de base de datos
Cree una lista de direcciones IP o de punto de conexión de Amazon RDS en el servidor SMTP en las instalaciones.	El servidor SMTP está fuera de la red de AWS. En el servidor SMTP local, cree una lista de permisos que permita al servidor comunicarse con el punto de enlace saliente o la dirección IP de la instancia	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de Amazon RDS o la instancia de Amazon Elastic Compute Cloud (Amazon EC2) alojada en Amazon RDS. Este procedimiento varía de una organización a otra. Para obtener más información sobre el punto de conexión de la instancia de base de datos, consulte Búsqueda del punto de conexión y el número de puerto de la instancia de base de datos.	

Tarea	Descripción	Habilidades requeridas
Elimine las restricciones del puerto 25.	De forma predeterminada, AWS restringe el puerto 25 en las EC2 instancias. Para eliminar la restricción del puerto 25, haga lo siguiente: 1. Inicie sesión con su cuenta de AWS y, a continuación, abra el formulario de Solicitud para eliminar las limitaciones de envío de correo electrónico. 2. Introduzca su dirección de correo electrónico para que AWS Support pueda ponerse en contacto con usted para informarle sobre las actualizaciones de su solicitud. 3. Proporcione la información requerida en el campo de Descripción del caso de uso. 4. Elija Enviar. Note • Si tiene instancias en más de una región de AWS, envíe una solicitud por separado para cada región.	AWS general

Tarea	Descripción	Habilidades requeridas
	• Su solicitud de transacción puede tardar hasta 48 horas en procesarse.	
Añada una regla de Route 53 para resolver las consultas de DNS para el servidor SMTP.	Utilice Route 53 para resolver las consultas de DNS entre los recursos de AWS y el servidor SMTP en las instalaciones. Debe crear una regla que reenvíe las consultas de DNS al dominio del servidor SMTP, por ejemplo `example.com` . Para obtener instrucciones, consulte Creación de reglas de reenvío en la documentación de Route 53.	Administrador de red

Configuración de Correo de base de datos en la instancia de base de datos de Amazon RDS para SQL Server

Tarea	Descripción	Habilidades requeridas
Habilitación de Database Mail.	Cree un grupo de parámetros para el Correo de base de datos, defina el parámetro `database mail xps` en `1`, a continuación, asocie el grupo de parámetros del Correo de base de datos a la instancia de base de datos de RDS de destino. Para obtener instrucciones, consulte la Habilitación de Database Mail en la documentación de Amazon RDS. No continúe con la	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	sección de Configuración del correo de base de datos de estas instrucciones. La configuración del servidor SMTP en las instalaciones es diferente a la de Amazon SES.	
Conéctese a la instancia de base de datos.	Desde un host bastión, utilice Microsoft SQL Server Management Studio (SSMS) para conectarse a la instancia de base de datos de Amazon RDS para SQL Server. Para obtener instrucciones, consulte Conexión de una instancia de base de datos que ejecuta el motor de base de datos de Microsoft SQL Server. Si encuentra algún error, consulte las referencias para la solución de problemas de conexión en la sección de Recursos relacionados.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree el perfil.	En SSMS, inserte la siguiente instrucción SQL para crear el perfil del Correo de base de datos. Reemplace los siguientes valores: • Para `profile_name` , escriba un nombre para el nuevo perfil. • Para `description` , escriba una breve descripci ón del nuevo perfil. Para obtener más información acerca de este procedimiento almacenado y sus argumento s, consulte sysmail_add_profil e_sp en la documentación de Microsoft. `EXECUTE msdb.dbo. sysmail_add_profil e_sp @profile_name = 'SQL Alerts profile', @description = 'Profile used for sending outgoing notifications using OM SMTP Server.';`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Añada las entidades principal es al perfil.	Introduzca la siguiente instrucción SQL para añadir directores públicos o privados al perfil de correo de la base de datos. Una entidad principal es una entidad que puede solicitar recursos de SQL Server. Reemplace los siguientes valores: • Para `profile_name` , inserte el nombre del perfil que creó anteriormente. • Para `principal_name` , inserte el nombre del usuario o rol de base de datos. Este valor debe corresponder a un usuario de autenticación de SQL Server, un usuario de autenticación de Windows o un grupo de autenticación de Windows. Para obtener más información acerca de este procedimiento almacenado y sus argumento s, consulte sysmail_add_princi palprofile_sp en la documenta ción de Microsoft. `EXECUTE msdb.dbo. sysmail_add_princi palprofile_sp`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`@profile_name = 'SQL Alerts profile', @principal_name = 'public', @is_default = 1 ;`	

Tarea	Descripción	Habilidades requeridas
Cree la cuenta.	Inserte la siguiente instrucción SQL para crear el perfil de la cuenta de Database Mail. Reemplace los siguientes valores: • For `account_name` , escriba un nombre para la nueva cuenta. • Para `description` , escriba una breve descripción de la nueva cuenta. • Para `email_address` , introduzca la dirección de correo electrónico desde la que desea enviar los mensajes de correo de la base de datos. • Para `display_address` , especifique un nombre para mostrar y usarlo en los mensajes salientes de esta cuenta, por ejemplo `SQL Server Automated Notification` . También puede utilizar el valor que ha introducido para `email_address` . • Para `mailserver_name` , introduzca el nombre o la dirección IP del servidor de correo SMTP. • Para `port`, deje el valor de `25`.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	• Para `enable_ssl` , deje el valor en `1` o introduzca `0` si no desea que el Correo de base de datos cifre las comunicaciones mediante SSL.
	• Para `username`, introduzca el nombre de usuario de registro en el servidor de correo SMTP. Si el servidor no requiere autenticación, inserte `NULL`.
	• Para `password`, introduzca la contraseña para acceder al servidor de correo SMTP. Si el servidor no requiere autenticación, inserte `NULL`.
	
	Para obtener más información acerca de este procedimiento almacenado y sus argumentos, consulte sysmail_add_account_sp en la documentación de Microsoft.
	
	`EXECUTE msdb.dbo.sysmail_add_account_sp`
	`@account_name = 'SQL Alerts account',`
	`@description = 'Database Mail account for sending outgoing notifications.',`
	`@email_address = 'xyz@example.com',`	

Tarea	Descripción	Habilidades requeridas
	<pre>@display_name = 'xyz@example.com', @mailserver_name = 'test_smtp.example.com', @port = 25, @enable_ssl = 1, @username = 'SMTP-username', @password = 'SMTP-password';</pre>	

Tarea	Descripción	Habilidades requeridas
Agregue la cuenta al perfil	Inserte la siguiente instrucción SQL para agregar la cuenta de Database Mail al perfil de Database Mail. Reemplace los siguientes valores: • Para `profile_name` , inserte el nombre del perfil que creó anteriormente. • Para `account_name` , inserte el nombre de la cuenta que creó anteriorm ente. Para obtener más información acerca de este procedimiento almacenado y sus argumento s, consulte sysmail_add_profil eaccount_sp en la documenta ción de Microsoft. `EXECUTE msdb.dbo. sysmail_add_profil eaccount_sp @profile_name = 'SQL Alerts profile', @account_name = 'SQL Alerts account', @sequence_number = 1;`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
(Opcional) Añada Multi-AZ a la instancia de base de datos de RDS.	Si desea agregar Multi-AZ con duplicación de bases de datos (DBM) o grupos de disponibilidad Always On (AGs), consulte las instrucciones de Agregar Multi-AZ a una instancia de base de datos de Microsoft SQL Server.	Administrador de base de datos

Recursos relacionados

- Uso de Database Mail en Amazon RDS para SQL Server (documentación de Amazon RDS)
- Trabajar con archivos adjuntos (documentación de Amazon RDS)
- Solución de problemas de conexión a la instancia de base de datos de SQL Server (documentación de Amazon RDS)
- No se puede conectar a la instancia de base de datos de Amazon RDS (documentación de Amazon RDS)

Configurar la recuperación de desastres para SAP en IBM Db2 en AWS

Ambarish Satarkar y Debasis Sahoo, Amazon Web Services

Resumen

Este patrón describe los pasos para configurar un sistema de recuperación de desastres (DR) para cargas de trabajo de SAP con IBM Db2 como plataforma de base de datos ejecutada en la nube de Amazon Web Services (AWS). El objetivo es proporcionar una solución de bajo costo para garantizar la continuidad empresarial en caso de interrupción.

El patrón emplea el enfoque de prueba piloto. Al implementar una prueba piloto de DR en AWS, puede reducir el tiempo de inactividad y mantener la continuidad empresarial. Este enfoque piloto se centra en configurar un entorno de DR mínimo en AWS, con un sistema SAP y una base de datos Db2 en espera sincronizada con el entorno de producción.

Esta solución es escalable. Puede ampliarla a un entorno de recuperación de desastres a gran escala si lo necesita.

Requisitos previos y limitaciones

Requisitos previos

- Una instancia de SAP que se ejecuta en una instancia de Amazon Elastic Compute Cloud (Amazon EC2)
- Base de datos Db2 de IBM
- Un sistema operativo compatible con la matriz de disponibilidad de producto (PAM) de SAP
- Diferentes nombres de host de bases de datos físicas para los hosts de bases de datos de producción y espera
- Un bucket de Amazon Simple Storage Service (Amazon S3) en cada región de AWS con la replicación entre regiones (CRR) habilitada

Versiones de producto

- Base de datos IBM Db2, versión 11.5.7 o posterior

Arquitectura

Pila de tecnología de destino

- Amazon EC2
- Amazon Simple Storage Service (Amazon S3)
- Nube privada virtual de Amazon (VPC peering)
- Amazon Route 53
- Recuperación de desastres de alta disponibilidad (HADR) en IBM Db2

Arquitectura de destino

Esta arquitectura implementa una solución de DR para cargas de trabajo de SAP con Db2 como plataforma de base de datos. La base de datos de producción se implementa en la región 1 de AWS, y la base de datos de espera se implementa en una segunda región. La base de datos de espera se denomina sistema DR. La base de datos Db2 admite varias bases de datos de espera (hasta tres). Emplea el HADR de Db2 para configurar la base de datos de recuperación de desastres y automatizar el envío de registros entre las bases de datos de producción y espera.

Si la disponibilidad de la región 1 se interrumpe a causa de un desastre, la base de datos en espera de la región de DR asume la función de base de datos de producción. Los servidores de aplicaciones de SAP se pueden crear con antelación mediante AWS Elastic Disaster Recovery o con una imagen de máquina de Amazon (AMI) para satisfacer los requisitos del objetivo de tiempo de recuperación (RTO). Este patrón emplea un AMI.

El HADR de Db2 implementa una configuración de producción en espera en la que producción actúa como servidor principal al que se conectan todos los usuarios. Todas las transacciones se escriben en archivos de registro que se transfieren al servidor en espera mediante TCP/IP. El servidor en espera actualiza su base de datos local enviando los registros transferidos, lo que ayuda a garantizar la sincronización con el servidor de producción.

El emparejamiento de VPC permite que las instancias de la región de producción y la región de DR puedan comunicarse entre sí. Amazon Route 53 dirige a los usuarios finales a las aplicaciones de Internet.

1. Cree una AMI del servidor de aplicaciones en la región 1 y copie la AMI en la región 2. Use la AMI para lanzar servidores en la Región 2 en caso de desastre.
2. Configure la replicación HADR de Db2 entre la base de datos de producción (en la región 1) y la base de datos en espera (en la región 2).

3. En EC2 caso de desastre, cambie el tipo de instancia para que coincida con la instancia de producción.
4. En la Región 1, `LOGARCHMETH1` se establece en `db2remote: S3 path`.
5. En la Región 2, `LOGARCHMETH1` se establece en `db2remote: S3 path`.
6. La replicación entre regiones se realiza entre los buckets de S3.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS. Este patrón emplea interconexión de VPC.

Prácticas recomendadas

- La red desempeña un papel crucial a la hora de decidir el modo de replicación HADR. Para la recuperación de desastres en todas las regiones de AWS, le recomendamos que use el modo Db2 HADR ASYNC o SUPERASYNC.
- Para obtener más información sobre los modos de replicación de Db2 HADR, consulte la documentación de IBM.
- Puede usar la consola de administración de AWS o la interfaz de la línea de comandos de AWS (AWS CLI) para crear una nueva AMI de su sistema SAP existente. A continuación, puede usar la AMI para recuperar su sistema SAP existente o crear un clon.
- AWS Systems Manager Automation puede ayudar con las tareas habituales de mantenimiento e implementación de las EC2 instancias y otros recursos de AWS.

- AWS proporciona varios servicios nativos para supervisar y gestionar la infraestructura y las aplicaciones en AWS. CloudTrail Se pueden utilizar servicios como Amazon CloudWatch y AWS para supervisar la infraestructura subyacente y las operaciones de la API, respectivamente. Para obtener más información, consulte SAP en AWS: IBM Db2 HADR con Pacemaker.

Epics

Prepare el entorno

Tarea	Descripción	Habilidades requeridas
Compruebe el sistema y los registros.	1. Confirme que el SAP de producción en el sistema Db2 esté configurado. 2. Confirme que la copia de seguridad de registros esté habilitada y configurada para guardar los registros en el bucket de S3. Puede comprobarlo mediante el parámetro `LOGARCHMETH1` de Db2. 3. Cree una AMI del servidor de aplicaciones adicional.	Administrador de AWS, administrador de SAP Basis

Configure los servidores y la replicación

Tarea	Descripción	Habilidades requeridas
Cree los servidores de SAP y de bases de datos.	1. Para implementar la infraestructura en la región de DR, utilice un CloudFormation script de AWS o una AMI de la instancia de producción. Como parte del enfoque	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	piloto, puede utilizar una EC2 instancia más pequeña de la misma familia que la instancia de producción. Por ejemplo, si su tipo de instancia de producción es `r6i.12xlarge` , puede usar el tipo de instancia `r6i.xlarge` para la compilación de DR. De cualquier modo, asegúrese de asignar la misma capacidad de almacenam iento a la instancia de DR para restaurar la copia de seguridad de la base de datos de producción. 2. Cree puntos de montaje para `/sapmnt/<SID>/` en Amazon Elastic File System (Amazon EFS) y asegúrese de que está configurado para replicarse desde el sistema principal. 3. Realice una copia de seguridad completa de la base de datos (online u offline) del sistema de producción. Usará esta copia de seguridad para crear la base de datos de DR. 4. En el sistema de recuperac ión ante desastres, utilice	

Tarea	Descripción	Habilidades requeridas
	el método de copia del sistema SAP Software Provisioning Manager (SWPM) junto con el método Using system copy with backup/restore para HA/DR crear el sistema SAP de recuperación ante desastres. 5. Cuando SWPM lo solicite, restaure la base de datos de DR con la copia de seguridad que recuperó de producción. La base de datos de DR estará en estado pendiente de avance de transacciones. El estado pendiente de avance de transacciones se establece de forma predeterminada una vez restaurada la copia de seguridad completa. El estado pendiente de avance de transacciones indica que la base de datos está en proceso de restauración, y que es posible que se necesite aplicar algunos cambios. Para obtener más información, consulte la documentación de IBM.	

Tarea	Descripción	Habilidades requeridas
Compruebe la configuración.	1. Para configurar el archivado de registros para HADR, tanto las bases de datos de producción como las de DR deben poder recuperar los registros automáticamente de todas las ubicaciones de archivo de registros. Compruebe que el parámetro `LOGARCHMETH1` de la base de datos de DR esté establecido en la misma ubicación que en la base de datos de producción. Si no se puede acceder a la misma ubicación debido a las limitaciones regionales, asegúrese de que el sistema de DR pueda recuperar automáticamente los registros del sistema principal. 2. Para habilitar TCP/IP los puertos para permitir la replicación de bases de datos, modifique `/etc/services` los hosts de producción y DR añadiendo las dos entradas siguientes. En el código, `<SID>` hace referencia a la ID de sistema (SID) de la base	Administrador de AWS, administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas

	de datos Db2 (por ejemplo, PR1).
	
	`<SID>_HADR_1 55001/tcp # DB2 HADR Port1`
	`<SID>_HADR_2 55002/tcp # DB2 HADR Port2`
	
	Confirme que ambos puertos permiten el tráfico entrante y saliente entre las bases principal y en espera.
	3. Compruebe `/etc/hosts` en los hosts de producció n y DR para asegurarse de que los nombres de host de los hosts de producció n y espera apuntan a las direcciones IP correctas.	

Tarea	Descripción	Habilidades requeridas

Configure la replicación desde la base de datos de producció n a la base de datos de DR (mediante el modo ASYNC).	1. En la base de datos de producción, ejecute los siguientes comandos para actualizar los parámetros.
	
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_HOST HOST1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_SVC <SID>_HADR_1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_HOST HOST2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_SVC <SID>_HADR_2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_INST db2<sid>`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_TIMEOUT 120`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SYNCMODE ASYNC`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SPOOL_LIMIT 1000`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_PEER_WINDOW 240`
	`db2 UPDATE DB CFG FOR <SID> USING indexrec RESTART logindexbuild ON`
	
	2. En la base de datos DR, ejecute los siguientes
		Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas

	comandos para actualizar los parámetros.
	
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_HOST HOST2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_SVC <SID>_HADR_2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_HOST HOST1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_SVC <SID>_HADR_1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_INST db2<sid>`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_TIMEOUT 120`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SYNCMODE ASYNC`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SPOOL_LIMIT 1000`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_PEER_WINDOW 240`
	`db2 UPDATE DB CFG FOR <SID> USING indexrec RESTART logindexbuild ON`
	
	Estos parámetros son necesarios para proporcionar información de HADR a ambas bases de datos. En la base de datos Db2,	

Tarea	Descripción	Habilidades requeridas

	HADR se activa en función de los valores de cada uno de los parámetros estableci dos anteriormente. Para más información sobre estos parámetros, consulte la documentación de IBM.
	3. Inicie primero HADR en la base de datos de espera recién creada ejecutando el siguiente comando.
	`db2 deactivate db <SID>`
	`db2 start hadr on db <SID> as standby`
	4. Inicie HADR en la base de datos de producción ejecutando el siguiente comando.
	`db2 deactivate db <SID>`
	`db2 start hadr on db <SID> as primary`
	5. Compruebe si las bases de datos Db2 en producción y en espera están sincroniz adas, y si el envío de registros está en curso.
	Para supervisar el estado de la replicación de HADR, ejecute el comando db2pd.	

Tarea	Descripción	Habilidades requeridas
	`db2pd -d <SID> -hadr` Para más información sobre la monitorización de HADR, consulte la documentación de IBM.	

Pruebe las tareas de conmutación por error de DR

Tarea	Descripción	Habilidades requeridas
Planifique el tiempo de inactividad empresarial de producción para la prueba de DR.	Asegúrese de planificar el tiempo de inactividad empresarial necesario en el entorno de producción para probar el escenario de conmutación por error de DR.	Administrador de SAP Basis
Crear un usuario de prueba.	Cree un usuario de prueba (o cualquier cambio de prueba) que pueda validarse en el host de DR para confirmar la replicación del registro tras la conmutación por error de DR.	Administrador de SAP Basis
En la consola, detenga las instancias de producción EC2 .	En este paso se inicia un cierre imprevisto para simular un escenario de desastre.	Administrador de sistemas de AWS
Amplíe la EC2 instancia de recuperación ante desastres para adaptarla a los requisitos.	En la EC2 consola, cambie el tipo de instancia en la región de DR. 1. Detenga la instancia: si la instancia se está ejecutand	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas

	o, debe detenerla para poder cambiar el tipo de instancia. En la EC2 consola, selecciona la instancia y elige Detener.
	2. Modifique el tipo de instancia: en la EC2 consola, seleccione la instancia y elija Acciones, Configuración de instancia y Cambiar tipo de instancia. Seleccione el tipo de instancia que coincida con la instancia principal y elija Aplicar.
	3. Iniciar la instancia: cuando se complete el cambio de tipo de instancia, inicie la instancia desde la EC2 consola. Para ello, seleccione la instancia y elija Iniciar.
	4. Para iniciar la base de datos Db2, utilice el comando siguiente.
	`db2start`
	`db2 start HADR on db <SID> as standby`	

Tarea	Descripción	Habilidades requeridas

Inicie la toma de control.	Desde el sistema de DR (`host2`), inicie el proceso de toma de control y active la base de datos de recuperación de desastres como principal.
	`db2 takeover hadr on database <SID> by force`
	Si lo desea, puede configurar los siguientes parámetros para ajustar automáticamente la asignación de memoria de la base de datos en función del tipo de instancia. El valor `INSTANCE_MEMORY` se puede decidir en función de la parte dedicada de la memoria que se va a asignar a la base de datos Db2.
	`db2 update db cfg for <SID> using INSTANCE_MEMORY <FIXED VALUE> IMMEDIATE;`
	`db2 get db cfg for <SID> | grep -i DATABASE_MEMORY AUTOMATIC IMMEDIATE;`
	`db2 update db cfg for <SID> using self_tuning_mem ON IMMEDIATE;`
	Verifique el cambio usando los siguientes comandos.
		Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	`db2 get db cfg for <SID> | grep -i MEMORY` `db2 get db cfg for <SID> | grep -i self_tuning_mem`	
Inicie el servidor de aplicaciones para SAP en la región de DR.	Con la AMI que creó en el sistema de producción, lance un nuevo servidor de aplicaciones adicional en la región de DR.	Administrador de SAP Basis
Realice la validación antes de iniciar la aplicación SAP.	1. Valide las entradas `/etc/hosts` y `/etc/fstab`. 2. Monte `/sapmnt/<SID>/` en el sistema de DR. 3. Valide que el sistema de archivos de DR `/sapmnt/<SID>/` esté sincronizado con el `/sapmnt/<SID>/` de producción. 4. Inicie sesión con el usuario `<sid>adm`, ejecute `R3trans -d` y verifique el resultado del archivo `trans.log`. El archivo `trans.log` se genera en la misma ubicación en la que se ejecutó el comando `R3trans -d`.	Administrador de AWS, administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas

Inicie la aplicación SAP en el sistema de DR.	Inicie la aplicación SAP en el sistema de DR utilizando el usuario `<sid>adm`. Use el siguiente código, en el que XX representa el número de instancia de su servidor ABAP SAP Central Services (ASCS) de SAP, y YY representa el número de instancia de su servidor de aplicación SAP.
	`sapconrol -nr XX -function StartService <SID>`
	`sapconrol -nr XX -function StartSystem`
	`sapconrol -nr YY -function StartService <SID>`
	`sapconrol -nr YY -function StartSystem`
		Administrador de SAP Basis

Realice la validación de SAP.	Esto se lleva a cabo como una prueba de DR para proporcionar pruebas o comprobar que la replicación de los datos en la región de DR se realiza correctamente.	Ingeniero de pruebas

Lleve a cabo tareas de conmutación por recuperación en DR

Tarea	Descripción	Habilidades requeridas
Inicie los servidores de bases de datos y SAP de producció n.	En la consola, inicie las EC2 instancias que alojan SAP y la base de datos en el sistema de producción.	Administrador de SAP Basis

Iniciar la base de datos de producción y configurar HADR.	Inicie sesión en el sistema de producción (`host1`) y compruebe que la base de datos está en modo de recuperación ejecutando el siguiente comando.
	`db2start`
	`db2 start HADR on db P3V as standby`
	`db2 connect to <SID>`
	Compruebe que el estado de HADR sea `connected` . El estado de la replicación debe ser `peer`.
	`db2pd -d <SID> -hadr`
	Si la base de datos no es incoherente y no se encuentra en estado `connected` y `peer`, es posible que sea necesario realizar una copia de seguridad y una restaurac ión para que la base de datos (en `host1`) se sincronice con la base de datos actualmen
		Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	te activa (`host2` en la región de DR). En ese caso, restaure la copia de seguridad de la base de datos de la región de DR `host2` a la base de datos de la región de producción `host1`.	

Tarea	Descripción	Habilidades requeridas
Conmute por recuperación la base de datos a la región de producción.	En un business-as-usual escenario normal, este paso se realiza en un tiempo de inactividad programado. Las aplicaciones que se ejecutan en el sistema de DR se detienen, y la base de datos se conmuta por recuperac ión a la región de producción (región 1) para reanudar las operaciones desde la región de producción. 1. Inicie sesión en el servidor de aplicaciones SAP de la región de DR y detenga la aplicación de SAP. 2. Desmonte `/sapmnt/<SID>` del sistema de DR y asegúrese de que los cambios se replican de forma inversa al sistema de producción `/sapmnt/<SID>` . 3. Inicie sesión en el servidor de base de datos (`host1`) de la región de producción y tome el control. `db2 takeover hadr on database <SID>` 4. Compruebe el estado de HADR: `HADR_ROLE` debe	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	ser PRIMARY en host1 y StandBy en host2. `db2pd -d <SID> -hadr`	
Realice la validación antes de iniciar la aplicación SAP.	1. Valide las entradas /etc/hosts y /etc/fstab . 2. Monte /sapmnt/<SID>/ en el sistema de producción. 3. Asegúrese de que esté sincronizado con el sistema de DR /sapmnt/<SID>/ . 4. Inicie sesión con el usuario <sid>adm, ejecute R3trans -d y verifique el resultado del archivo trans.log . El archivo trans.log se genera en la misma ubicación en la que se ejecutó el comando R3trans -d.	Administrador de AWS, administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas

Inicie la aplicación de SAP.	1. Inicie la aplicación SAP en el sistema de producción con el usuario `<sid>adm`. Use el siguiente código, en el que XX representa el número de instancia de su servidor SAP ASCS, y YY representa el número de instancia de su servidor de aplicación SAP.
	`sapconrol -nr XX -function StartService <SID>`
	`sapconrol -nr XX -function StartSystem`
	`sapconrol -nr YY -function StartService <SID>`
	`sapconrol -nr YY -function StartSystem`
	2. Para confirmar que los servidores de aplicacio nes están disponibles, inicie sesión en SAP y realice las comprobaciones mediante el SICK y SM51 las transacciones.
		Administrador de SAP Basis

Resolución de problemas

Problema	Solución
Archivos de registro de clave y comandos para solucionar problemas relacionados con HADR	• `db2 get db cfg | grep -i hadr`

Problema	Solución
	• `db2pd -d sid -hadr` • `Db2diag.log` (Por lo general, este archivo se encuentra dentro del directorio `db2dump`, y la ruta de `db2dump` está definida por el parámetro `DIAGPATH`).
Nota de SAP para la resolución de problemas de HADR en Db2 UDB	Consulte la nota 1154013 de SAP DB6: Problemas con la base de datos en un entorno HADR. (Necesitará las credenciales del portal SAP para acceder a esta nota).

Recursos relacionados

- Enfoques de recuperación de desastres para bases de datos Db2 en AWS (publicación del blog)
- SAP en AWS: IBM Db2 HADR con Pacemaker
- Procedimiento paso a paso para configurar la replicación de HADR entre bases de datos DB2
- Wiki de HADR Db2

Información adicional

Con este patrón puede configurar un sistema de recuperación de desastres para un sistema SAP que se ejecute en una base de datos Db2. En una situación de desastre, la empresa debería poder mantener sus requisitos de Objetivo de tiempo de recuperación (RTO) y Objetivo de punto de recuperación (RPO):

- El RTO es la máxima demora aceptable entre la interrupción del servicio y el restablecimiento del servicio. Este valor determina el período de tiempo que se considera aceptable cuando el servicio no está disponible.
- El RPO es la cantidad máxima de tiempo aceptable desde el último punto de recuperación de datos. Esto determina qué se considera una pérdida de datos aceptable entre el último punto de recuperación y la interrupción del servicio.

Para obtener FAQs información sobre el HADR, consulte la nota #1612105 de SAP DB6: Preguntas frecuentes sobre la recuperación ante desastres de alta disponibilidad (HADR) de Db2. (Necesitará las credenciales del portal SAP para acceder a esta nota).

Configure una CI/CD canalización para la migración de bases de datos mediante Terraform

Dr. Rahul Sharad Gaikwad, Ashish Bhatt, Aniket Dekate, Ruchika Modi, Tamilselvan P, Nadeem Rahaman, Aarti Rajput y Naveen Suthar, Amazon Web Services

Resumen

Este patrón consiste en establecer un proceso de integración e implementación continuas (CI/CD) para administrar migraciones de bases de datos de una manera confiable y automatizada. Abarca el proceso de aprovisionamiento de la infraestructura necesaria, migración de datos y personalización de los cambios de esquema mediante Terraform, que es una herramienta de infraestructura como código (IaC).

En concreto, el patrón configura una CI/CD canalización para migrar una base de datos local de Microsoft SQL Server a Amazon Relational Database Service (Amazon RDS) en adelante. AWS También puede utilizar este patrón para migrar a Amazon RDS una base de datos de SQL Server que se encuentre en una máquina virtual (VM) o en otro entorno de nube.

Este patrón aborda los desafíos siguientes relacionados con la administración y la implementación de bases de datos:

- Las implementaciones manuales de bases de datos son tardadas, propensas a errores y carecen de coherencia en los entornos.
- Coordinar el aprovisionamiento de la infraestructura, las migraciones de datos y los cambios de esquema puede resultar complejo y difícil de administrar.
- Garantizar la integridad de los datos y minimizar el tiempo de inactividad durante las actualizaciones de las bases de datos es fundamental para los sistemas de producción.

Este patrón proporciona los beneficios siguientes:

- Simplifica el proceso de actualización e implementación de los cambios en la base de datos mediante la implementación de una CI/CD canalización para las migraciones de bases de datos. Esto reduce el riesgo de errores, garantiza la coherencia en todos los entornos y minimiza el tiempo de inactividad.
- Ayuda a mejorar la fiabilidad, la eficiencia y la colaboración. Permite una comercialización más rápida y reduce el tiempo de inactividad durante las actualizaciones de las bases de datos.

- Le ayuda a adoptar DevOps prácticas modernas para la administración de bases de datos, lo que se traduce en una mayor agilidad, confiabilidad y eficiencia en sus procesos de entrega de software.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- La versión 0.12 o posterior de Terraform instalada en su máquina local (para obtener instrucciones, consulte la documentación de Terraform)
- Terraform AWS Provider versión 3.0.0 o posterior de HashiCorp (consulte el GitHub repositorio de este proveedor)
- Política de privilegios mínimos AWS Identity and Access Management (IAM) (consulte la entrada del blog Técnicas para redactar políticas de IAM con privilegios mínimos)

Arquitectura

Este patrón implementa la arquitectura siguiente, que proporciona la infraestructura completa para el proceso de migración de la base de datos.

En esta arquitectura:

- La base de datos de origen es una base de datos de SQL Server en las instalaciones, en una máquina virtual (VM) o alojada por otro proveedor de nube. El diagrama asume que la base de datos de origen está en un centro de datos en las instalaciones.
- El centro de datos local y AWS están conectados a través de una VPN o conexión. AWS Direct Connect Esto proporciona comunicaciones seguras entre la base de datos de origen y la AWS infraestructura.
- La base de datos de destino es una base de datos de Amazon RDS que se aloja en la nube privada virtual (VPC) con la ayuda de una AWS canalización de aprovisionamiento de bases de datos.
- AWS Database Migration Service (AWS DMS) replica su base de datos local en. AWS Se utiliza para configurar la replicación de la base de datos de origen en la base de datos de destino.

El siguiente diagrama muestra la infraestructura configurada con diferentes niveles del proceso de migración de la base de datos, que implica el aprovisionamiento, la AWS DMS configuración y la validación.

En este proceso:

- El proceso de validación valida todos los controles. La canalización integrada pasará al próximo paso cuando se hayan completado todas las validaciones necesarias.
- El proceso de aprovisionamiento de la base de datos consta de varias AWS CodeBuild etapas que realizan acciones de Terraform en el código de Terraform proporcionado para la base de datos. Cuando se completan estos pasos, implementa los recursos en la Cuenta de AWS de destino.
- El AWS DMS proceso consta de varias CodeBuild etapas en las que se realizan las pruebas y, a continuación, se aprovisiona la AWS DMS infraestructura necesaria para realizar la migración mediante el uso de la IaC.

Tools (Herramientas)

Servicios de AWS y herramientas

- AWS CodeBuildes un servicio de integración continua totalmente gestionado que compila el código fuente, ejecuta pruebas y produce paquetes de ready-to-deploy software.
- AWS CodePipeline es un servicio de entrega continua totalmente administrado que ayuda a automatizar las canalizaciones de lanzamiento para actualizaciones de infraestructura y aplicaciones rápidas y fiables.
- Amazon Relational Database Service (Amazon RDS) lo ayuda a configurar, utilizar y escalar una base de datos relacional en la Nube de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento líderes del sector.
- AWS Database Migration Service (AWS DMS) le ayuda a migrar los almacenes de datos a una combinación de configuraciones locales y en la nube Nube de AWS o entre ellas.

Otros servicios

- Terraform es una herramienta de iAC HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.

Repositorio de código

El código de este patrón está disponible en el DevOps marco de migración de GitHub bases de datos mediante el repositorio de muestras de Terraform.

Prácticas recomendadas

- Implemente pruebas automatizadas para la migración de su base de datos a fin de verificar la exactitud de los cambios en el esquema y la integridad de los datos. Esto incluye pruebas unitarias, pruebas de integración y end-to-end pruebas.
- Implemente una estrategia sólida de copia de seguridad y restauración para las bases de datos, sobre todo antes de la migración. Esto garantiza la integridad de los datos y proporciona una opción alternativa en caso de errores.
- Implemente una estrategia sólida de reversión para revertir los cambios en la base de datos en caso de que se produzcan errores o problemas durante la migración. Esto podría implicar volver a un estado anterior de la base de datos o revertir los scripts de migración individuales.
- Configure mecanismos de supervisión y registro para hacer un seguimiento del avance y el estado de las migraciones de bases de datos. Esto es útil para identificar y resolver los problemas de manera rápida.

Epics

Configure su equipo de trabajo local

Tarea	Descripción	Habilidades requeridas
Defina y configure Git en su estación de trabajo local.	Instale y configure Git en su estación de trabajo local con las instrucciones de la documentación de Git.	DevOps ingeniero
Cree una carpeta de proyecto y añada los archivos del GitHub repositorio.	1. Abra el GitHub repositorio para este patrón. 2. Elija Código para ver las opciones de clonación y copie la URL proporcionada en la pestaña HTTPS.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	3. Cree una carpeta para el proyecto en su estación de trabajo.
	4. Abra un terminal y vaya a esta carpeta.
	5. Clona el GitHub repositorio:
	`git clone <github-repository-url>`
	`<github-repository-url>` es la URL que copió en el paso 2.
	6. Cuando se complete la clonación, vaya al repositorio clonado de la carpeta del proyecto:
	`cd <folder-name>/aws-terraform-db-migration-framework-samples`
	7. Abra el proyecto en un entorno de desarrollo integrado (IDE) de su elección.	

Aprovisionamiento de la arquitectura de destino

Tarea	Descripción	Habilidades requeridas
Actualice los parámetros obligatorios.	El `ssm-parameters.sh` archivo almacena todos los AWS Systems Manager	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	parámetros necesarios. Puede configurar estos parámetros con los valores personalizados de su proyecto. En la `setup/db-ssm-params` carpeta de la estación de trabajo local, abra el `ssm-parameters.sh` archivo y defina estos parámetros antes de ejecutar la CI/CD canalización.	
Inicialice la configuración de Terraform.	En la carpeta `db-cicd-integration` , ingrese el comando siguiente para inicializar el directorio de trabajo que contiene los archivos de configuración de Terraform: `terraform init`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Obtenga una vista previa del plan Terraform.	Para crear un plan de ejecución de Terraform, ingrese el comando siguiente: `terraform plan -var-file ="terraform.sample"` Terraform evalúa los archivos de configuración para determinar el estado objetivo de los recursos declarados. A continuación, compara el estado objetivo con el estado actual y crea un plan.	DevOps ingeniero
Verifique el plan.	Revise el plan y confirme que configura la arquitectura requerida en su Cuenta de AWS de destino.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Implemente la solución.	1. Introduzca el siguiente comando para aplicar el plan: `terraform apply -var-file="terraform.sample"` 2. Escriba `yes` para confirmar. Terraform crea, actualiza o destruye la infraestructura para alcanzar el estado objetivo declarado en los archivos de configuración. Para más información acerca de la secuencia, consulte la sección Arquitectura de este patrón.	DevOps ingeniero

Verifique la implementación

Tarea	Descripción	Habilidades requeridas
Valide la implementación.	Verifique el estado de la canalización `db-cicd-integration` para confirmar que la migración de la base de datos se completó. 1. Inicie sesión en la AWS CodePipeline consola y Consola de administración de AWS, a continuación, ábrala.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	2. En el panel de navegación, seleccione Canalizaciones. 3. Configure la canalización de `db-cicd-integration` . 4. Valide que la ejecución de la canalización finalizó correctamente.	

Limpieza de la infraestructura después de utilizarla

Tarea	Descripción	Habilidades requeridas
Limpie la infraestructura.	1. Una vez completado el proyecto, elimine la infraestructura que creó mediante el comando: `terraform destroy --var-file=terrafo rm.sample` 2. Escriba `yes` para confirmar.	DevOps ingeniero

Recursos relacionados

AWS documentación

- Cómo empezar con un producto de Terraform

Documentación de Terraform

- Instalación de Terraform
- Terraform backend configuration

- Documentación de Terraform Provider AWS

Configure un clúster de conmutación por error de Microsoft SQL Server en Amazon EC2 FSx mediante Windows File Server

Sweta Krishna y Ramesh Babu Donti, Amazon Web Services

Resumen

Microsoft SQL Server Standard Edition con una instancia de clúster de conmutación por error (FCI) puede proporcionar una alternativa más rentable a SQL Server Enterprise. La configuración de SQL FCI requiere un almacenamiento de archivos compartido entre los nodos, y Amazon FSx for Windows File Server proporciona un almacenamiento totalmente gestionado que se replica automáticamente y de forma sincrónica en todas las zonas de disponibilidad. Amazon FSx reduce los costes de almacenamiento mediante el uso de la deduplicación de datos integrada para los recursos compartidos de archivos de uso general, lo que elimina la necesidad de mantener soluciones de terceros. Amazon FSx también admite lo siguiente:

- Pague solo por lo que use, sin tarifas ni compromisos iniciales.
- Configura FCI manualmente con Amazon FSx como almacenamiento compartido.
- Utilice Amazon FSx como testigo del uso compartido de archivos para su clúster de SQL.
- Amazon FSx para Windows File Server es compatible con Server Message Block (SMB) 3.0 para compartir archivos de forma continua, lo que lo hace adecuado para las implementaciones de FCI de SQL Server.

Requisitos previos y limitaciones

Requisitos previos

- Activo. Cuenta de AWS
- Permisos para crear y gestionar los recursos de Amazon Virtual Private Cloud (Amazon VPC), la instancia de Amazon Elastic Compute Cloud (Amazon EC2), los grupos de seguridad y las funciones (IAM). AWS Identity and Access Management
- AWS Managed Microsoft AD o su propio Active Directory local.
- Un usuario de dominio de Active Directory con los permisos necesarios para configurar un clúster de conmutación por error.
- Reglas de grupo de seguridad para la FCI de SQL Server y los puertos de Microsoft Active Directory para una conectividad híbrida segura.

- Una cuenta de servicio en Active Directory para SQL Server configurada con los permisos adecuados en todos los nodos de SQL.
- Amazon FSx para Windows File Server en un clúster de conmutación por error.
- Archivos binarios de instalación de SQL Server.

Limitaciones

- Algunas Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- Amazon EC2 para Windows Server 2012 R2 o versiones posteriores
- Amazon FSx para Windows File Server con todas las versiones actuales de Windows Server
- Amazon FSx for NetApp ONTAP como alternativa de almacenamiento compartido
- SQL Server 2012/2016/2019/2022

Arquitectura

Pila de tecnología

- Amazon EC2
- Servidor FSx de archivos Amazon para Windows
- Amazon VPC
- AWS Directory Service
- AWS Systems Manager
- IAM

Arquitectura de destino

El siguiente diagrama muestra la arquitectura de alto nivel de Microsoft SQL Server FCI en Amazon EC2 mediante FSx Amazon for Windows File Server.

Infraestructura de red

- Amazon VPC proporciona un contenedor de red que abarca tres zonas de disponibilidad.
- Las subredes privadas proporcionan subredes aisladas en cada zona de disponibilidad para implementar recursos.

Capa de computación

- Amazon EC2 contiene un nodo 1 de clúster de SQL Server, implementado en la zona de disponibilidad 1 como parte del clúster de conmutación por error de Windows Server (WSFC).
- Amazon EC2 contiene un nodo 2 de clúster de SQL Server, implementado en la zona de disponibilidad 2 como parte del WSFC.
- El clúster WSFC conecta ambos nodos de SQL Server para ofrecer una capacidad de conmutación por error.

Capa de almacenamiento para Amazon FSx para Windows File Server

FSx Implementación Multi-AZ (que abarca las zonas de disponibilidad 1 y 2)

- Un sistema de FSx archivos principal de la zona de disponibilidad 1 aloja los archivos de registro y datos activos de SQL Server.
- Un sistema de FSx archivos secundario en la zona de disponibilidad 2 proporciona una capacidad de conmutación por error automática.
- Un recurso compartido de archivos SMB (\\fsx.domain\sqlshare) al que pueden acceder ambos nodos del clúster para las bases de datos de SQL Server.

FSx Implementación en una zona de disponibilidad única (in) AZ3

- El testigo del servidor de FSx archivos de Amazon en la zona de disponibilidad 3 actúa como testigo del quórum del clúster.
- El testigo del recurso compartido de archivos (`\\fsx.domain\witness`) mantiene el quorum del clúster y evita situaciones de cerebro dividido.

Servicios de directorio

- AWS Managed Microsoft AD proporciona los servicios de autenticación y dominio de Windows necesarios para la funcionalidad del clúster.

Características de alta disponibilidad

- Los componentes multi-AZ ofrecen tolerancia a errores en todas las zonas de disponibilidad.
- FSx el servidor de archivos en espera proporciona una conmutación por error automática si el servidor principal falla.
- El testigo del recurso compartido de archivos administra el quorum del clúster en la zona de disponibilidad 3 para garantizar el correcto funcionamiento del clúster durante los errores.
- El dominio está integrado AWS Managed Microsoft AD para una autenticación de Windows perfecta.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon FSx proporciona sistemas de archivos que admiten los protocolos de conectividad estándares del sector y ofrecen alta disponibilidad y replicación en todos Regiones de AWS los niveles.
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.
- AWS Directory Service for Microsoft Active Directorypermite que sus cargas de trabajo y AWS recursos compatibles con directorios utilicen Microsoft Active Directory en. Nube de AWS
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Systems Manager lo ayuda a administrar las aplicaciones y la infraestructura que se ejecutan en la Nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo necesario para detectar y resolver problemas operativos y le ayuda a administrar sus AWS recursos de forma segura y a escala.

Prácticas recomendadas

- Coloque las instancias de bases de datos en subredes privadas para evitar que el público pueda acceder a ellas desde Internet y, al mismo tiempo, permitirles conectarse Servicios de AWS y realizar actualizaciones.
- Para usarlo PowerShell para administrar su servidor de archivos de Amazon FSx para Windows, consulte Administración FSx de sistemas de archivos de Windows.

Epics

Creación y configuración de nodos de Amazon EC2 para SQL Server

Tarea	Descripción	Habilidades requeridas
Agregar nombres y etiquetas.	1. En Consola de administración de AWS, navegue hasta Amazon EC2. 2. Seleccione Iniciar instancia. 3. Agregue las etiquetas necesarias.	Administrador de base de datos
Elegir una AMI de Windows.	Elija una Imagen de máquina de Amazon (AMI) para Windows que cumpla con sus requisitos de SQL Server.	Administrador de base de datos
Seleccione un tipo de instancia.	Seleccione un tipo de instancia de Amazon EC2 que cumpla con sus requisitos.	Administrador de base de datos
Usar un par de claves.	Puede utilizar un par de claves para conectarse de forma segura a su instancia . Asegúrese de tener acceso al par de claves seleccionado antes de lanzar la instancia.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Configure los valores de red.	1. Elija la VPC que utilizó para configurar Active Directory. 2. Elija la VPC y la subred privada. 3. Elija un grupo de seguridad existente. Si no tiene uno, elija Crear grupo de seguridad.	Administrador de base de datos
Definir los ajustes de red avanzados.	1. Elija Configuración de red avanzada. 2. Seleccione la IP secundaria. 3. Seleccione la casilla Asignar automáticamente para asignar la IP secundaria de la subred.	Administrador de base de datos
Configurar almacenamiento.	Configure el almacenamiento total necesario y elija el tipo de almacenamiento requerido.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Configurar los detalles avanzados y lanzar la instancia.	1. Elija el dominio de Active Directory de la lista de directorios. 2. Elija un rol de IAM que tenga asociadas las políticas `AmazonSSMManagedInstanceCore` y `AmazonSSMDirectoryServiceAccess`. 3. (Opcional) Configure otras opciones disponibles. 4. Lanzamiento de la instancia.	Administrador de base de datos
Crear el nodo 2.	Repita estos pasos para crear y configurar el nodo 2.	Administrador de base de datos

Instalación y configuración del clúster de conmutación por error de Windows Server en los nodos 1 y 2

Tarea	Descripción	Habilidades requeridas
Iniciar sesión en el nodo 1.	Inicie sesión en la instancia de Amazon EC2 de Windows como administrador.	Administrador de base de datos
Instalar las características de la FCI en el nodo 1.	1. En PowerShell, ejecute el siguiente script: `Install-WindowsFeature -Name Failover-`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`Clustering -IncludeM anagementTools` 1. Tras la instalación, compruebe si hay actualizaciones pendientes de Windows e instálelas. 2. Reinicie la instancia.	
Iniciar sesión en el nodo 2.	Inicie sesión en la instancia de Amazon EC2 de Windows como administrador.	Administrador de base de datos
Instalar las características de la FCI en el nodo 2.	1. En PowerShell, ejecute el siguiente script: `Install-WindowsFea ture -Name Failover-Clustering -IncludeM anagementTools` 1. Tras la instalación, compruebe si hay actualizaciones pendientes de Windows e instálelas. 2. Reinicie la instancia.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Agregar nodos al clúster.	1. Use Escritorio remoto para conectarse al nodo 1 y elija Iniciar administrador de servidores. 2. En el menú Herramien tas, elija Administrador de clústeres de conmutación por error. 3. En el panel Administrador de clústeres de conmutaci ón por error, en Administr ación, elija Crear clúster para abrir el asistente de creación de clústeres. 4. En la página Antes de empezar, elija Siguiente. 5. Si aparece la página Seleccionar los servidore s, en el campo Ingrese el nombre, elija Examinar, busque sus servidores y, a continuación, elija Agregar. Repita este paso para cada servidor que desee agregar y, a continuación, elija Siguiente. 6. En la página Punto de acceso para administrar el clúster, elija el clúster y, a continuación, elija Siguiente . 7. En la página Confirmac ión se muestra el nombre	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	del clúster, el nodo y otra información del dominio. Revise estos detalles y, a continuación, elija Siguiente . 8. En la página Resumen, compruebe que la FCI se haya creado correctamente. Si hay alguna advertencia o error, consulte el resultado del resumen o elija Ver informe. 9. Seleccione Finalizar. 10. Cuando el clúster esté configurado, el sistema mostrará Ha completado el asistente de creación de clústeres. 11. Repita estos pasos para el nodo 2.	

Tarea	Descripción	Habilidades requeridas
Poner en línea el clúster.	Para poner en línea el clúster, actualice las direcciones IP estáticas de ambos nodos: 1. Seleccione el nombre del objeto del clúster. 2. Abra el menú contextual (con el botón derecho) y, a continuación, elija Propiedades. 3. Seleccione la subred y una dirección IP secundaria sin usar de la instancia de EC2. 4. Tras actualizar la dirección IP secundaria, abra el menú contextual (con el botón derecho) y seleccione Nombre del objeto del clúster. 5. Seleccione Poner en línea.	Administrador de base de datos
Validar el clúster.	Va a Administrador de clústeres de conmutación por error y compruebe que los recursos principales del clúster estén en línea.	Administrador de base de datos

Instalación de SQL Server en los nodos 1 y 2

Tarea	Descripción	Habilidades requeridas
Iniciar sesión en el servidor.	Inicie sesión en la instancia de Amazon EC2 como administrador.	Administrador de base de datos
Montar los archivos binarios de SQL.	1. Inicie el centro de instalación de SQL Server y, a continuación, elija Instalación. 2. Elija Nueva instalación de clúster de conmutación por error de SQL Server. 3. Siga las instrucciones hasta Archivos de configuración. 4. En el cuadro de diálogo Reglas globales, verifique que todas las comprobaciones sean correctas. 5. En el cuadro de diálogo Instalar reglas de clúster de conmutación por error, verifique que todas las comprobaciones sean correctas. Aborde cualquier advertencia antes de continuar. 6. En el cuadro de diálogo Selección de características, seleccione las casillas de verificación Servicios de motores de bases de datos y Conectivi	

Tarea	Descripción	Habilidades requeridas
	dad de herramientas de cliente. 7. En el cuadro de diálogo Reglas de características, verifique que todas las reglas se hayan superado. 8. En el cuadro de diálogo Configuración de instancia s, ingrese el nombre de la red de SQL Server. 9. En el grupo Recursos del clúster, especifique el nombre del grupo de recursos. Seleccione un grupo de la lista desplegab le o ingrese un nombre personalizado. 10. En el cuadro de diálogo de configuración de red de clústeres, active IPv4y desactive DHCP. Proporcio ne una dirección IP privada secundaria para cada nodo. 11. En el cuadro de diálogo Configuración del servidor: • En la pestaña Cuentas de servicio, proporcione los detalles necesarios para el nombre de la cuenta de servicio de SQL y las credenciales de SQL Server.	

Tarea	Descripción	Habilidades requeridas
	• Compruebe que el valor de Tipo de inicio del agente y el motor de base de datos esté establecido en Manual. • Seleccione la casilla de verificación Conceder el privilegio de realizar tareas de mantenimiento de volúmenes al servicio de motor de base de datos de SQL Server. Esto permite la inicialización instantánea de archivos para SQL Server. 12 En el cuadro de diálogo Configuración del motor de base de datos: • En la pestaña Configuración del servidor, en Modo de autenticación de Windows, compruebe que esté seleccionado Modo de autenticación. • En la pestaña Directorios de datos, especifique la ubicación de la FSx ruta de Amazon para los datos, los registros, el tempdb y los archivos de respaldo (por ejemplo, para `.mdf` los archivos y `\\fsx.domain\sqlsh`	

Tarea	Descripción	Habilidades requeridas
	are\data \\fsx.domain\sqlshare\logs para `.ldf` los archivos). 13. En el cuadro de diálogo de reglas Configuración de características, compruebe que todas las comprobaciones sean correctas y, a continuación, seleccione Siguiente. 14. En el cuadro de diálogo Listo para la instalación, compruebe todos los ajustes de configuración. 15. Seleccione Instalar para continuar con la instalación. 16. En el cuadro de diálogo Completar, elija Cerrar.	

Tarea	Descripción	Habilidades requeridas
Agregar el nodo 2 al clúster de conmutación por error.	1. Vaya al centro de instalación de SQL Server. 2. Elija Instalación. 3. Elija Agregar nodo a un clúster de conmutación por error de SQL Server y siga las instrucciones hasta Configuración del nodo del clúster. 4. En el cuadro de diálogo de configuración del nodo del clúster, active IPv4y desactive DHCP. 5. Agregue una dirección IP para el nodo 2. 6. En Cuentas de servicio, compruebe que los detalles coincidan con los nodos 1 y 2. 7. Proporcione las credencia les de las cuentas de servicio de SQL Server correspondientes. 8. En el cuadro de diálogo Reglas de características, verifique que todas las comprobaciones sean correctas. 9. Seleccione Siguiente y siga el resto de las instrucci ones. 10. Seleccione Instalar para continuar con la instalación.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	11 En el cuadro de diálogo Completar, elija Cerrar.	

Configurar el testigo de FSx compartición de archivos de Amazon

Tarea	Descripción	Habilidades requeridas
Configurar los ajustes de quorum.	1. Use RDP para conectarse a la instancia de Amazon EC2. 2. Vaya a Administrador de clústeres de conmutación por error. 3. Abra el menú contextual (clic con el botón derecho) del clúster y elija Más acciones. 4. Elija Configurar los ajustes de quorum del clúster. 5. Configure los ajustes de quorum.	Administrador de base de datos
Recuperar los detalles del DNS.	En la FSx consola de Amazon, selecciona Managed AD y, a continuación, Attach. El DNS debe tener el siguiente formato: `\\example.example.net\share` .	Administrador de base de datos
Configurar el testigo de uso compartido de archivos.	Selecciona la ruta de FSx compartición de archivos de Amazon y, a continuación, Finalizar.	Administrador de base de datos

Recursos relacionados

AWS resources

- Servidor de archivos Amazon FSx para Windows (vídeo)
- Análisis profundo de Amazon FSx para Windows File Server (vídeo)
- Cómo implementar un clúster de conmutación por error de SQL Server con Amazon EBS Multi-Attach en Windows Server (AWS entrada del blog)
- Simplifique sus despliegues de alta disponibilidad de Microsoft SQL Server con Amazon FSx for Windows File Server (entrada del AWS blog)
- Implementaciones de alta disponibilidad de SQL Server con Amazon FSx for NetApp ONTAP (AWS entrada del blog)
- Uso FSx para Windows File Server con Microsoft SQL Server
- ¿Qué es FSx para Windows File Server?

Otros recursos

- Create a failover cluster

Información adicional

Configurar el testigo de uso compartido de archivos

Asegúrese de estar conectado al sistema de archivos desde ambos nodos añadiendo reglas en el grupo de FSx seguridad de Amazon que permitan las conexiones entrantes. Se debe permitir el puerto SMB. Por ejemplo, si el nombre de DNS es `\\example.example.com\share`, use `\\example.example.com\share`. Utilice el mismo valor para el testigo de uso compartido de archivos en el clúster de disponibilidad Always On. Siga los pasos que se describen a continuación para configurar el testigo de uso compartido de archivos:

1. Use RDP para conectarse a la instancia de Amazon EC2.
2. Vaya a Administrador de clústeres de conmutación por error.
3. Abra el menú contextual (clic con el botón derecho) y elija Más acciones.
4. Elija Configurar los ajustes de quorum del clúster.
5. Elija Siguiente.

6. Seleccione Configuración de quorum y configure un testigo de uso compartido de archivos.
7. Proporcione el nombre de DNS.
8. Revise el resumen y, a continuación, elija Finalizar. El testigo de uso compartido de archivos debe estar en línea en la sección de recursos principales del clúster.

Configure una HA/DR arquitectura para Oracle E-Business Suite en Amazon RDS Custom con una base de datos en espera activa

Simon Cunningham, Jaydeep Nandy y Nitin Saxena, Amazon Web Services

Resumen

Este patrón describe cómo puede diseñar su solución Oracle E-Business en Amazon Relational Database Service (Amazon RDS) Custom para lograr una alta disponibilidad (HA) y recuperación de desastres (DR) configurando una base de datos de réplicas de lectura de Amazon RDS Custom en otra zona de disponibilidad de Amazon Web Services (AWS) y convirtiéndola en una base de datos en espera activa. La creación de la réplica de lectura de Amazon RDS Custom está totalmente automatizada mediante la consola de administración de AWS.

Este patrón no describe los pasos para añadir niveles de aplicaciones adicionales y sistemas de archivos compartidos, que también pueden formar parte de una arquitectura. HA/DR Para obtener más información sobre estos temas, consulte las siguientes notas de soporte de Oracle: 1375769.1, 1375670.1 y 1383621.1 (sección 5, Opciones de clonación avanzadas). (El acceso requiere una cuenta de Oracle Support).

Para migrar el sistema E-Business Suite a una arquitectura de un solo nivel y zona de disponibilidad única en Amazon Web Services (AWS), consulte el patrón Migración de Oracle E-Business Suite a Amazon RDS Custom.

Oracle E-Business Suite es una solución de planificación de recursos empresariales (ERP) que automatiza procesos de toda la empresa, como finanzas, recursos humanos, cadena de suministro y fabricación. Ofrece una arquitectura de tres niveles: cliente, aplicación y base de datos. Anteriormente, tenía que ejecutar la base de datos de E-Business Suite en una instancia autogestionada de Amazon Elastic Compute Cloud EC2 (Amazon), pero ahora puede beneficiarse de Amazon RDS Custom.

Requisitos previos y limitaciones

Requisitos previos

- Una instalación existente de E-Business Suite en Amazon RDS Custom; consulte el patrón Migración de Oracle E-Business Suite a Amazon RDS Custom

- Si quiere cambiar la réplica de lectura a una de solo lectura y utilizarla para transferir los informes a los que están en espera, adquiera una licencia de base de datos de Oracle Active Data Guard (consulte la lista de precios comerciales de Oracle Technology)

Limitaciones

- Limitaciones y configuraciones no compatibles con las bases de datos de Oracle en Amazon RDS Custom
- Limitaciones asociadas a las réplicas de lectura de Amazon RDS Custom para Oracle

Versiones de producto

Para ver las versiones de Oracle Database y clases de instancia compatibles con Amazon RDS Custom, consulte Requisitos y limitaciones de Amazon RDS Custom para Oracle.

Arquitectura

El siguiente diagrama ilustra una arquitectura representativa de E-Business Suite en AWS que incluye varias zonas de disponibilidad y niveles de aplicaciones en una active/passive configuración. La base de datos usa una instancia de base de datos de Amazon RDS Custom y una réplica de lectura de Amazon RDS Custom. La réplica de lectura utiliza Active Data Guard para replicarse en otra zona de disponibilidad. También puede usar la réplica de lectura para descargar el tráfico de lectura en la base de datos principal y para generar informes.

Para obtener más información, consulte Trabajar con réplicas de lectura para Amazon RDS Custom para Oracle en la documentación de Amazon RDS.

La réplica de lectura de Amazon RDS Custom se crea de forma predeterminada cuando está montada. Sin embargo, si desea transferir algunas de sus cargas de trabajo de solo lectura a la base de datos en espera para reducir la carga de la base de datos principal, puede cambiar manualmente el modo de las réplicas montadas a las de solo lectura siguiendo los pasos de la sección Epics. Un caso de uso típico sería ejecutar los informes desde la base de datos en espera. Para cambiar a una base de datos de solo lectura se requiere una licencia de base de datos en espera activa.

Al crear una réplica de lectura en AWS, el sistema utiliza el agente Oracle Data Guard de forma clandestina. Esta configuración se genera automáticamente y se configura en el modo de máximo rendimiento de la siguiente manera:

```
DGMGRL> show configuration
Configuration - rds_dg
  Protection Mode: MaxPerformance
  Members:
  vis_a - Primary database
    vis_b - Physical standby database
Fast-Start Failover: DISABLED
Configuration Status:
SUCCESS   (status updated 58 seconds ago)
```

Tools (Herramientas)

Servicios de AWS

- Amazon RDS Custom para Oracle es un servicio de base de datos administrado para aplicaciones heredadas, personalizadas y empaquetadas que requieren acceso al sistema operativo y al entorno de base de datos subyacentes. Amazon RDS Custom automatiza las tareas y operaciones de administración de bases de datos y le permite, como administrador de bases de datos, acceder y personalizar el entorno de base de datos y el sistema operativo.

Otras herramientas

- Oracle Data Guard es una herramienta que le ayuda a crear y gestionar las bases de datos en espera de Oracle. Este patrón utiliza Oracle Data Guard para configurar una base de datos en espera activa en Amazon RDS Custom.

Epics

Crear una réplica de lectura

Tarea	Descripción	Habilidades requeridas
Crear una réplica de lectura para la instancia de base de datos de Amazon RDS Custom.	Para crear una réplica de lectura, siga las instrucciones de la documentación de Amazon RDS y utilice la instancia de base de datos de Amazon RDS Custom	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	que creó (consulte la sección Requisitos previos) como base de datos de origen. De forma predeterminada, la réplica de lectura de Amazon RDS Custom se crea como una copia física en espera y está en el estado montado. Esto tiene la intención de garantizar el cumplimiento de la licencia de Oracle Active Data Guard. Siga los siguiente s pasos para convertir la réplica de lectura al modo de solo lectura.	

Cambie la réplica de lectura a un modo de espera activo de solo lectura

Tarea	Descripción	Habilidades requeridas
Conéctese a la réplica de lectura de Amazon RDS Custom.	Utilice los siguientes comandos para convertir la base de datos física en espera en una base de datos en espera activa. ⚠ Important Estos comandos requieren una licencia de espera activa de Oracle. Para obtener una licencia, póngase en contacto con su	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	representante de Oracle.	

```
$ sudo su - rdsdb
-bash-4.2$ sql
SQL> select process,s
tatus,sequence# from v
$managed_standby;

PROCESS    STATUS
 SEQUENCE#
--------- ------------
 ----------
ARCH       CLOSING
      3956
ARCH       CONNECTED
         0
ARCH       CLOSING
      3955
ARCH       CLOSING
      3957
RFS        IDLE
         0
RFS        IDLE
      3958
MRP0       APPLYING_LOG
       3958
SQL> select name,
 database_role,
 open_mode from v
$database;

NAME       DATABASE_
ROLE    OPEN_MODE
--------- ---------
------- ---------
-----------
VIS        PHYSICAL
 STANDBY MOUNTED
```

Tarea	Descripción	Habilidades requeridas
	SQL> alter database recover managed standby database cancel; Database altered. Open the standby database SQL> alter database open; Database altered. SQL> select name, database_role, open_mode from v $database; NAME DATABASE_ ROLE OPEN_MODE --------- --------- ------- --------- ----------- VIS PHYSICAL STANDBY READ ONLY	

Tarea	Descripción	Habilidades requeridas

Inicie la recuperación multimedia con la aplicación de un registro en tiempo real.	Para activar la característica de aplicación de registros en tiempo real, utilice los siguientes comandos. Estos convierten y validan la base de datos en espera (réplica de lectura) como una base de datos en espera activa, de modo que pueda conectarse y ejecutar consultas de solo lectura.
	`SQL>  alter database recover managed standby database using current logfile disconnect from session;`
	`Database altered`
		Administrador de base de datos

Compruebe el estado de la base de datos.	Para comprobar el estado de la base de datos, use el comando siguiente.
	`SQL> select name, database_role, open_mode from v$database;`
	`NAME DATABASE_ROLE OPEN_MODE`
	`--------- ---------- ----------`
	`VIS PHYSICAL STANDBY READ ONLY WITH APPLY`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

Marque el modo de reaplicación.	Para comprobar el modo de reaplicación, utilice el siguiente comando.
	
	`SQL> select process,status,sequence# from v$managed_standby;`
	`PROCESS STATUS SEQUENCE#`
	`--------- ------------ ----------`
	`ARCH CLOSING 3956`
	`ARCH CONNECTED 0`
	`ARCH CLOSING 3955`
	`ARCH CLOSING 3957`
	`RFS IDLE 0`
	`RFS IDLE 3958`
	`MRP0 APPLYING_LOG 3958`
	
	`SQL> select open_mode from v$database;`
	`OPEN_MODE`
	`--------------------`
	`READ ONLY WITH APPLY`
		Administrador de base de datos

Recursos relacionados

- Migración de Oracle E-Business Suite a Amazon RDS Custom (Recomendaciones de AWS)
- Uso de Amazon RDS Custom (documentación de Amazon RDS)
- Trabajo con réplicas de lectura para Amazon RDS Custom para Oracle (documentación de Amazon RDS)

- Amazon RDS Custom for Oracle – New Control Capabilities in Database Environment (blog de AWS News)
- Migración de Oracle E-Business Suite a AWS (documento técnico de AWS)
- Arquitectura de Oracle E-Business Suite en AWS (documento técnico de AWS)

Transmita datos desde IBM Db2, SAP, Sybase y otras bases de datos a MongoDB Atlas en AWS

Battulga Purevragchaa e Igor Alekseev, Amazon Web Services

Babu Srinivasan, MongoDB

Resumen

Este patrón describe los pasos para migrar los datos de IBM Db2 y otras bases de datos, como bases de datos de mainframe y Sybase a MongoDB Atlas en la Nube de AWS. Utiliza AWS Glue para acelerar la migración de los datos a MongoDB Atlas.

El patrón acompaña a la guía Migración a MongoDB Atlas que se encuentra en AWS el sitio web de orientación prescriptiva. AWS Proporciona los pasos de implementación para uno de los escenarios de migración que se analizan en esa guía. Para ver otros escenarios de migración, consulte los siguientes patrones en el sitio web de la Guía prescriptiva: AWS

- Migre un entorno MongoDB autohospedado a MongoDB Atlas en AWS
- Migre bases de datos relacionales a MongoDB Atlas en AWS

El patrón está destinado a socios y AWS usuarios de AWS Managed Services.

Requisitos previos y limitaciones

Requisitos previos

- Una base de datos de origen como SAP, Sybase, IBM Db2 y otras para migrar a MongoDB Atlas.
- Familiaridad con bases de datos como SAP, Sybase, IBM Db2, MongoDB Atlas y. Servicios de AWS

Versiones de producto

- MongoDB versión 5.0 o posterior.

Arquitectura

El siguiente diagrama ilustra la carga de datos por lotes y la transmisión de datos mediante AWS Glue Studio Amazon Kinesis Data Streams y MongoDB Atlas.

Esta arquitectura de referencia se utiliza AWS Glue Studio para crear canalizaciones de extracción, transformación y carga (ETL) para migrar datos a MongoDB Atlas. An Rastreador de AWS Glue se integra con MongoDB Atlas para facilitar la gobernanza de los datos. Los datos pueden transferirse por lotes o transmitirse a MongoDB Atlas mediante Amazon Kinesis Data Streams.

Carga de datos por lotes

Para obtener más información sobre la migración de datos por lotes, consulte la entrada del AWS blog Componga sus trabajos de ETL para MongoDB Atlas con. AWS Glue

Transmisión de datos

Para ver las arquitecturas de referencia de MongoDB Atlas que admiten diferentes escenarios de uso, consulte Migración a MongoDB Atlas en el sitio web de orientación prescriptiva. AWS AWS

Tools (Herramientas)

- AWS Glue es un servicio de ETL completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.
- Amazon Kinesis Data Streams ayuda a recopilar y procesar grandes secuencias de registros de datos en tiempo real.
- MongoDB Atlas es una base de datos como servicio (DbaaS) completamente administrada para implementar y administrar bases de datos de MongoDB en la nube.

Prácticas recomendadas

Para obtener pautas, consulte la Guía de mejores prácticas para MongoDB en el repositorio de MongoDB. GitHub

Epics

Descubrimiento y evaluación

Tarea	Descripción	Habilidades requeridas
Determine el tamaño del clúster.	Calcule el tamaño del conjunto de trabajo utilizando la información de `db.stats(`	Administrador de base de datos de MongoDB, arquitecto de aplicaciones

Tarea	Descripción	Habilidades requeridas
	) para el espacio total del índice. Presuponga que se accederá con frecuencia a un porcentaje de su espacio de datos. O bien, puede estimar las necesidades de memoria según sus presuposiciones. Esta tarea puede necesitar aproximadamente una semana. Para obtener más información y ejemplos de esta y otras historias de esta épica, consulte los enlaces de la sección Recursos relacionados.	

Tarea	Descripción	Habilidades requeridas
Calcule los requisitos de ancho de banda de la red.	Para calcular los requisitos de ancho de banda de la red, multiplique el tamaño medio de los documentos por el número de documentos servidos por segundo. Tenga en cuenta el tráfico máximo que soportará cualquier nodo del clúster como base. Para calcular las velocidades de transferencia de datos descendentes del clúster a las aplicaciones cliente, utilice la suma del total de documentos devueltos durante un período de tiempo. Si sus aplicaciones leen desde nodos secundarios, divida este número total de documentos por el número de nodos que pueden realizar operaciones de lectura. Para encontrar el tamaño medio de los documentos de una base de datos, utilice el comando `db.stats().avgObjSize` . Esta tarea suele necesitar un día.	Administrador de base de datos de MongoDB
Seleccione la capa de Atlas.	Siga las instrucciones de la documentación de MongoDB para seleccionar la capa del clúster de Atlas correcta.	Administrador de base de datos de MongoDB

Tarea	Descripción	Habilidades requeridas
Planifique la transición.	Planifique la transición de la aplicación.	Administrador de base de datos de MongoDB, arquitecto de aplicaciones

Configurar un nuevo entorno de MongoDB Atlas en AWS

Tarea	Descripción	Habilidades requeridas
Cree un nuevo clúster de MongoDB Atlas en. AWS	En MongoDB Atlas, elija Crear un clúster y AWS selecciónelo como proveedor de nube.	Administrador de base de datos de MongoDB
Seleccione una Regiones de AWS configuración de clúster global.	Seleccione una opción de la lista de disponibles Regiones de AWS para su clúster de Atlas. Configure clústeres globales si es necesario.	Administrador de base de datos de MongoDB
Seleccione la capa del clúster.	Seleccione la capa del clúster que prefiera. La selección de la capa determina factores como la memoria, el almacenamiento y las especificaciones de IOPS.	Administrador de base de datos de MongoDB
Configure los ajustes adicional es del clúster.	Configure los ajustes adicional es del clúster, como la versión de MongoDB, la copia de seguridad y las opciones de cifrado. Para obtener más información sobre estas opciones, consulte la sección Recursos relacionados.	Administrador de base de datos de MongoDB

Configure la seguridad y el cumplimiento

Tarea	Descripción	Habilidades requeridas
Configure la lista de acceso.	Para conectarse al clúster de Atlas, debe agregar una entrada a la lista de acceso del proyecto. Atlas utiliza seguridad de la capa de transporte (TLS) / Capa de conexión segura (SSL) para cifrar las conexiones a la nube privada virtual (VPC) de su base de datos. Para configura r la lista de acceso al proyecto y obtener más información sobre las historias de esta epic, consulte los enlaces de la sección Recursos relaciona dos.	Administrador de base de datos de MongoDB
Autentique y autorice a los usuarios.	Debe crear y autenticar a los usuarios de la base de datos que accederán a los clústeres de MongoDB Atlas. Para acceder a los clústeres de un proyecto, los usuarios deben pertenecer a ese proyecto y pueden pertenecer a varios proyectos. También puedes habilitar la autorización con AWS Identity and Access Management (IAM). Para más información, consulte Set Up Authentication with IAM en la documentación de MongoDB.	Administrador de base de datos de MongoDB

Tarea	Descripción	Habilidades requeridas
Cree roles personalizados.	(Opcional) Atlas admite la creación de roles personalizados en los casos en que los privilegios de usuario integrados en la base de datos Atlas no cubran el conjunto de privilegios deseado.	Administrador de base de datos de MongoDB
Configure las interconexiones con VPC.	(Opcional) Atlas admite el emparejamiento de VPC con otros sistemas de AWS. VPCs	Administrador de base de datos de MongoDB
Configure un punto final AWS PrivateLink .	(Opcional) Puede configurar puntos de conexión privados AWS utilizando AWS PrivateLink.	Administrador de base de datos de MongoDB
Habilitar la autenticación en dos pasos.	(Opcional) Atlas admite la autenticación en dos pasos (2FA) para ayudar a los usuarios a controlar el acceso a sus cuentas de Atlas.	Administrador de base de datos de MongoDB
Configure la autenticación y la autorización de los usuarios con LDAP.	(Opcional) Atlas admite realizar la autenticación y autorización de los usuarios con el Protocolo ligero de acceso a directorios (LDAP).	Administrador de base de datos de MongoDB
Configure el AWS acceso unificado.	(Opcional) Algunas caracterí sticas de Atlas, como Atlas Data Lake y el cifrado en reposo mediante la administr ación de claves de cliente, utilizan los roles de IAM para la autenticación.	Administrador de base de datos de MongoDB

Tarea	Descripción	Habilidades requeridas
Configure el cifrado en reposo mediante AWS KMS.	(Opcional) Atlas admite el uso de AWS Key Managemen t Service (AWS KMS) para cifrar los motores de almacenamiento y las copias de seguridad de los proveedor es de servicios en la nube.	Administrador de base de datos de MongoDB
Configure CSFLE.	(Opcional) Atlas admite el cifrado en el nivel de campo del cliente (CSFLE), como el cifrado automático de los campos.	Administrador de base de datos de MongoDB

Migración de datos

Tarea	Descripción	Habilidades requeridas
Lance el conjunto de réplicas de destino en MongoDB Atlas.	Lance el conjunto de réplicas de destino en MongoDB Atlas. En Atlas Live Migration Service, seleccione Todo está listo para migrar.	Administrador de base de datos de MongoDB
Establezca la conexión de AWS Glue con MongoDB Atlas.	Use an Rastreador de AWS Glue para conectarse AWS Glue con MongoDB Atlas (base de datos de destino). Este paso ayuda a preparar el entorno de destino para la migración. Para obtener más información, consulte la Documentación de AWS Glue.	Administrador de base de datos de MongoDB

Tarea	Descripción	Habilidades requeridas
Establezca la conexión AWS Glue con la base de datos de origen o el flujo de origen.	Esto ayuda a preparar el entorno de destino para la migración.	Administrador de base de datos de MongoDB
Configure la transformación de los datos.	Configure la lógica de transformación para migrar los datos del esquema estructur ado heredado al esquema flexible de MongoDB.	Administrador de base de datos de MongoDB
Migre los datos.	Programe la migración en AWS Glue Studio.	Administrador de base de datos de MongoDB

Configurar la integración operativa

Tarea	Descripción	Habilidades requeridas
Conecte el clúster.	Conéctese al clúster de MongoDB Atlas.	Desarrollador de aplicaciones
Interactúe con los datos.	Interactúe con los datos del clúster.	Desarrollador de aplicaciones
Supervise los clústeres.	Supervise los clústeres de MongoDB Atlas.	Administrador de base de datos de MongoDB
Haga una copia de seguridad de los datos y una restaurac ión.	Realice copias de seguridad y restaure los datos del clúster.	Administrador de base de datos de MongoDB

Resolución de problemas

Problema	Solución
En caso de tener problemas	Consulte Solución de problemas en el repositorio de MongoDB Atlas Resources CloudFormation .

Recursos relacionados

Todos los enlaces siguientes, a menos que se indique lo contrario, van a páginas web de la documentación de MongoDB.

Guía de migración

- Migración a MongoDB Atlas AWS en (Guía prescriptiva)AWS

Detectar y evaluar

- Memoria
- Ejemplo de dimensionamiento con conjuntos de datos de muestra de Atlas
- Ejemplo de dimensionamiento para aplicaciones móviles
- Tráfico de red
- Escalado automático de clústeres
- Plantilla de dimensionamiento de Atlas

Configure la seguridad y el cumplimiento

- Configurar entradas de la lista de acceso IP
- Configure Database Users
- Configure Access to the Atlas UI
- Configure Custom Database Roles
- Configure Database Users
- Configurar un emparejamiento de red

- Learn About Private Endpoints in Atlas
- Manage Your Multi-Factor Authentication Options
- Configurar la autenticación y la autorización de usuarios con LDAP
- Lago de datos Atlas
- Cifrado en reposo mediante la administración de claves de cliente
- Métodos para asumir un rol (documentación de IAM)
- Configurar el cifrado en el nivel de campo del cliente
- Automatic Encryption
- MongoDB Atlas Security Controls
- Centro de confianza de MongoDB
- Configure Security Features for Clusters

Configuración de un nuevo entorno de MongoDB Atlas en AWS

- Proveedores y regiones de la nube
- Manage Global Clusters
- Select Cluster Tier
- Configure Additional Settings
- Introducción a Atlas
- Configure Access to the Atlas UI

Migración de datos

- Migrate or Import Data

Monitorear clústeres

- Monitor Your Clusters

Integrar operaciones

- Conectarse a un clúster
- Interact with Your Data

- Monitor Your Clusters
- Back Up, Restore, and Archive Data

GitHub repositorio

- Transmita datos a MongoDB Atlas usando AWS Glue

Funciones de transición para una PeopleSoft aplicación de Oracle en Amazon RDS Custom for Oracle

Sampath Kathirvel, Amazon Web Services

Resumen

Para ejecutar la solución de planificación de recursos PeopleSoft empresariales (ERP) de Oracle en Amazon Web Services (AWS), puede utilizar Amazon Relational Database Service (Amazon RDS) o Amazon RDS Custom for Oracle, que admite aplicaciones heredadas, personalizadas y empaquetadas que requieren acceso al sistema operativo (SO) y al entorno de base de datos subyacentes. Para conocer los factores clave a tener en cuenta durante la planificación de una migración, consulte Estrategias de migración de bases de datos de Oracle en Recomendaciones de AWS.

Este patrón se centra en los pasos para realizar un cambio de Oracle Data Guard, o transición de funciones, para una base de datos de PeopleSoft aplicaciones que se ejecuta en Amazon RDS Custom como base de datos principal con una base de datos de réplica de lectura. El patrón incluye los pasos para configurar la conmutación por error de inicio rápido (FSFO). Durante este proceso, las bases de datos de la configuración de Oracle Data Guard siguen funcionando en sus nuevos roles. Los casos de uso típicos de transición a Oracle Data Guard son simulacros de recuperación de desastres (DR), actividades de mantenimiento programadas de las bases de datos y parches progresivos de aplicación de parches en espera. Para obtener más información, consulte la publicación de blog Reducir los tiempos de inactividad al parchear bases de datos en Amazon RDS Custom.

Requisitos previos y limitaciones

Requisitos previos

- Finalización del proceso Add HA to Oracle PeopleSoft on Amazon RDS Custom mediante un patrón de réplica de lectura.

Limitaciones

- Limitaciones y configuraciones no compatibles con las RDS Custom for Oracle
- Limitaciones asociadas a las réplicas de lectura de Amazon RDS Custom para Oracle

Versiones de producto

- Para ver las versiones de la base de datos de Oracle compatibles con Amazon RDS Custom, consulte RDS Custom para Oracle.
- Para ver las clases de instancias de la base de datos de Oracle compatibles con Amazon RDS Custom, consulte Compatibilidad de clases de instancias de base de datos con RDS Custom para Oracle.

Arquitectura

Pila de tecnología

- Amazon RDS Custom para Oracle

Arquitectura de destino

El siguiente diagrama muestra una instancia de base de datos de Amazon RDS Custom y una réplica de lectura de Amazon RDS Custom. Oracle Data Guard proporciona transición de roles durante la conmutación por error para la DR.

Para ver una arquitectura representativa con Oracle PeopleSoft en AWS, consulte Configurar una PeopleSoft arquitectura de alta disponibilidad en AWS.

Tools (Herramientas)

Servicios de AWS

- Amazon RDS Custom para Oracle es un servicio de base de datos administrado para aplicaciones heredadas, personalizadas y empaquetadas que requieren acceso al sistema operativo y al entorno de base de datos subyacentes.
- AWS Secrets Manager le permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación. En este patrón, recupera las contraseñas de usuario de la base de datos de Secrets Manager para `RDS_DATAGUARD` con el nombre secreto `do-not-delete-rds-custom-+<<RDS Resource ID>>+-dg`.

Otros servicios

- Oracle Data Guard le ayuda a crear, mantener, gestionar y supervisar las bases de datos en espera. Este patrón emplea Oracle Data Guard Maximum Performance para la transición de roles (transición de Oracle Data Guard).

Prácticas recomendadas

Para su implementación de producción, le recomendamos lanzar la instancia de observación en una tercera zona de disponibilidad, separada de los nodos principal y de réplica de lectura.

Epics

Inicie la transición de rol

Tarea	Descripción	Habilidades requeridas
Detenga la automatización de la base de datos, tanto en la base de datos principal como en la réplica.	Si bien el marco de automatización de RDS Custom no interfiere en el proceso de transición de rol, se recomienda pausar la automatización durante la transición a Oracle Data Guard. Para pausar y reanudar la automatización de la base de datos de RDS Custom, siga las instrucciones indicadas en Pausar y reanudar la automatización de RDS Custom.	Administrador de la nube, administrador de bases de datos
Compruebe el estado de Oracle Data Guard.	Para comprobar el estado de Oracle Data Guard, inicie sesión en la base de datos principal. Este patrón incluye código para usar una base de datos de contenedor (CDB)	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	multiusuario o una instancia de no CDB.
	
	No CDB
	
	`-bash-4.2$ dgmgrl RDS_DATAGUARD@RDS_CUSTOM_ORCL_A`
	`DGMGRL for Linux: Release 19.0.0.0.0 - Production on Mon Nov 28 20:55:50 2022`
	`Version 19.10.0.0.0`
	`Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.`
	`Welcome to DGMGRL, type "help" for information.`
	`Password:`
	`Connected to "ORCL_A"`
	`Connected as SYSDG.`
	`DGMGRL> show configuration`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`orcl_a - Primary database`
	`orcl_d - Physical standby database`
	`Fast-Start Failover: Disabled`
	`Configuration Status:`
	`SUCCESS (status updated 59 seconds ago)`
	`DGMGRL>`
	
	CDB	

Tarea	Descripción	Habilidades requeridas

	CDB-bash-4.2$ dgmgrl
	 C##RDS_DATAGUARD@R
	DS_CUSTOM_RDSCDB_A
	DGMGRL for Linux:
	 Release 19.0.0.0.0 -
	 Production on Wed Jan
	 18 06:13:07 2023
	Version 19.16.0.0.0
	Copyright (c) 1982,
	 2019, Oracle and/or
	 its affiliates. All
	 rights reserved.
	Welcome to DGMGRL, type
	 "help" for informati
	on.
	Password:
	Connected to "RDSCDB_A
	"
	Connected as SYSDG.
	DGMGRL> show configura
	tion
	Configuration - rds_dg
	  Protection Mode:
	 MaxAvailability
	  Members:
	  rdscdb_a - Primary
	 database
	    rdscdb_b - Physical
	 standby database
	Fast-Start Failover:
	 Disabled
	Configuration Status:
	SUCCESS (status
	 updated 52 seconds ago)
	DGMGRL>	

Tarea	Descripción	Habilidades requeridas
Verifique el rol de instancia.	Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon RDS. En la sección Replicación de la base de datos, en la pestaña Conectividad y seguridad, verifique el rol de instancia para la instancia principal y la réplica. El rol principal debe coincidir con la base de datos principal de Oracle Data Guard, y el rol de réplica debe coincidir con la base de datos física en espera de Oracle Data Guard.	Administrador de la nube, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas

Realice la transición.	Para realizar la transición, conéctese a DGMGRL desde el nodo principal.
	
	No CDB
	
	`DGMGRL> switchover to orcl_d;`
	`Performing switchover NOW, please wait...`
	`Operation requires a connection to database "orcl_d"`
	`Connecting ...`
	`Connected to "ORCL_D"`
	`Connected as SYSDG.`
	`New primary database "orcl_d" is opening...`
	`Operation requires start up of instance "ORCL" on database "orcl_a"`
	`Starting instance "ORCL"...`
	`Connected to an idle instance.`
	`ORACLE instance started.`
	`Connected to "ORCL_A"`
	`Database mounted.`
	`Database opened.`
	`Connected to "ORCL_A"`
	`Switchover succeeded, new primary is "orcl_d"`
	`DGMGRL>`
	
	CDB
	
	`DGMGRL> switchover to rdscdb_b`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	`Performing switchover NOW, please wait...`
	`New primary database "rdscdb_b" is opening...`
	`Operation requires start up of instance "RDSCDB" on database "rdscdb_a"`
	`Starting instance "RDSCDB"...`
	`Connected to an idle instance.`
	`ORACLE instance started.`
	`Connected to "RDSCDB_A"`
	`Database mounted.`
	`Database opened.`
	`Connected to "RDSCDB_A"`
	`Switchover succeeded, new primary is "rdscdb_b"`	

Tarea	Descripción	Habilidades requeridas

Verifique la conexión de Oracle Data Guard.	Tras la transición, compruebe la conexión de Oracle Data Guard desde el nodo principal a `DGMGRL`.
	
	No CDB
	
	`DGMGRL> show configura tion;`
	`Configuration - rds_dg`
	`Protection Mode:`
	` MaxAvailability`
	`Members:`
	`orcl_d - Primary`
	` database`
	`orcl_a - Physical`
	` standby database`
	`Fast-Start Failover:`
	` Disabled`
	`Configuration Status:`
	`SUCCESS (status updated`
	` 60 seconds ago)`
	`DGMGRL>`
	
	`DGMGRL> show configura tion lag;`
	`Configuration - rds_dg`
	`Protection Mode:`
	` MaxAvailability`
	`Members:`
	`orcl_d - Primary`
	` database`
	`orcl_a - Physical`
	` standby database`
	`Transport Lag: 0`
	` seconds (computed 0`
	` seconds ago)`
	`Apply Lag: 0 seconds`
	` (computed 0 seconds`
	` ago)`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

```
Fast-Start Failover:
 Disabled
Configuration Status:
SUCCESS (status updated
 44 seconds ago)
DGMGRL>
```

CDB

```
DGMGRL> show configura
tion
DGMGRL> show configura
tion
Configuration - rds_dg
  Protection Mode:
 MaxAvailability
  Members:
  rdscdb_b - Primary
 database
    rdscdb_a - Physical
 standby database
Fast-Start Failover:
 Disabled
Configuration Status:
SUCCESS   (status
 updated 52 seconds ago)
DGMGRL>

DGMGRL> show configura
tion lag
Configuration - rds_dg
  Protection Mode:
 MaxAvailability
  Members:
  rdscdb_b - Primary
 database
    rdscdb_a - Physical
 standby database
              Transport
 Lag:      0 seconds
```

Tarea	Descripción	Habilidades requeridas
	(computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 53 seconds ago) DGMGRL>	
Verifique el rol de instancia en la consola de Amazon RDS.	Tras realizar el cambio de rol, la consola de Amazon RDS muestra los nuevos roles en la sección Replicación de la pestaña Conectividad y seguridad, en Bases de datos. Es posible que el Estado de replicación tarde unos minutos en actualizarse de vacío a Replicando.	Administrador de base de datos

Configure la FSFO

Tarea	Descripción	Habilidades requeridas
Restablezca la transición.	Vuelva a establecer la transición en el nodo principal.	Administrador de base de datos
Instale e inicie el observador.	Un proceso de observación es un componente del cliente DGMGRL que, por lo general, se ejecuta en una máquina diferente a la de las bases de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	datos principal y en espera. La instalación de ORACLE HOME para el observador puede ser una instalación de Oracle Client Administrator. También puede instalar Oracle Database Enterprise Edition o Personal Edition. Para obtener más información sobre la instalación del observador para su versión de base de datos, consulte Instalar e iniciar el observador. Para configurar la alta disponibilidad para el proceso de observación, puede hacer lo siguiente: • Habilite EC2 la recuperación automática de la EC2 instancia que ejecuta su observador. Debe automatizar el proceso de inicio del observador como parte del inicio del sistema operativo. • Implemente un observador en la EC2 instancia y configure un grupo de Amazon EC2 Auto Scaling de tamaño uno (1). En caso de que se produzca un error en la EC2 instancia, el grupo de escalado automático activa automáticamente otra EC2 instancia.	

Tarea	Descripción	Habilidades requeridas
	En la versión 2 de Oracle 12c y versiones posteriores, puede implementar hasta tres observadores. Uno es el observador principal , y el resto son observado res de respaldo. Cuando el observador principal falla, uno de los observadores de respaldo asume el rol de principal.	

Tarea	Descripción	Habilidades requeridas

Conéctese a DGMGRL desde el host del observador.	El host del observador está configurado con entradas `tnsnames.ora` para la conectividad de las bases de datos principal y en espera. Puede habilitar la FSFO con el modo de protección de máximo rendimiento siempre que la pérdida de datos esté dentro de la FastStart FailoverLagLimitconfiguración (valor en segundos). Sin embargo, debe utilizar el modo de protección de máxima disponibilidad para lograr una pérdida de datos cero (RPO=0).
	
	No CDB
	
	`DGMGRL> show configuration;`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`orcl_a - Primary database`
	`orcl_d - Physical standby database`
	`Fast-Start Failover: Disabled`
	`Configuration Status:`
	`SUCCESS (status updated 58 seconds ago)`
	`DGMGRL> show configuration lag`
	`Configuration - rds_dg`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Protection Mode: MaxAvailability Members: orcl_a - Primary database orcl_d - Physical standby database Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 5 seconds ago) DGMGRL>	
	CDB -bash-4.2$ dgmgrl C##RDS_DATAGUARD@R DS_CUSTOM_RDSCDB_A DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 18 06:55:09 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for informati on. Password: Connected to "RDSCDB_A " Connected as SYSDG.	

Tarea	Descripción	Habilidades requeridas
	`DGMGRL> show configura tion Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_a - Primary database rdscdb_b - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 18 seconds ago) DGMGRL>`	

Tarea	Descripción	Habilidades requeridas

Modifique la base de datos en espera para que sea el objetivo de la conmutación por error.	Conéctese desde el nodo principal o desde el nodo de observador a una base de datos en espera. (Aunque su configuración puede tener varias bases de datos en espera, solo necesita conectarse a una en este momento).
	
	No CDB
	
	`DGMGRL> edit database orcl_a set property FastStartFailoverTarget='orcl_d';`
	`Property "faststartfailovertarget" updated`
	`DGMGRL> edit database orcl_d set property FastStartFailoverTarget='orcl_a';`
	`Property "faststartfailovertarget" updated`
	`DGMGRL> show database orcl_a FastStartFailoverTarget;`
	`FastStartFailoverTarget = 'orcl_d'`
	`DGMGRL> show database orcl_d FastStartFailoverTarget;`
	`FastStartFailoverTarget = 'orcl_a'`
	`DGMGRL>`
	
	CDB
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	`DGMGRL> edit database orcl_a set property FastStartFailoverTarget='rdscdb_b';`
	`Object "orcl_a" was not found`
	`DGMGRL> edit database rdscdb_a set property FastStartFailoverTarget='rdscdb_b';`
	`Property "faststartfailovertarget" updated`
	`DGMGRL> edit database rdscdb_b set property FastStartFailoverTarget='rdscdb_a';`
	`Property "faststartfailovertarget" updated`
	`DGMGRL> show database rdscdb_a FastStartFailoverTarget;`
	`FastStartFailoverTarget = 'rdscdb_b'`
	`DGMGRL> show database rdscdb_b FastStartFailoverTarget;`
	`FastStartFailoverTarget = 'rdscdb_a'`
	`DGMGRL>`	

Tarea	Descripción	Habilidades requeridas

Configure la conexión FastStartFailoverThreshold a la DGMGRL.	El valor predeterminado es de 30 segundos en Oracle 19c. El valor mínimo es de 6 segundos. Un valor inferior puede acortar el objetivo de tiempo de recuperación (RTO) durante la conmutación por error. Un valor superior ayuda a reducir la posibilidad de que se produzcan errores transitorios de conmutación por error innecesarios en la base de datos principal.
	
	El marco de automatización de RDS Custom para Oracle supervisa el estado de la base de datos y lleva a cabo acciones correctivas cada pocos segundos. Por lo tanto, se recomienda establecer un valor superior FastStart FailoverThreshold a 10 segundos. En el siguiente ejemplo, se configura el valor de umbral en 35 segundos.
	
	No CBD o CDB
	
	`DGMGRL> edit configuration set property FastStartFailoverThreshold=35;`
	`Property "faststartfailoverthreshold" updated`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`DGMGRL> show configura tion FastStart FailoverThreshold; FastStartFailover Threshold = '35' DGMGRL>`	

Tarea	Descripción	Habilidades requeridas

Habilite la FSFO conectándose a DGMGRL desde el nodo principal o el nodo de observador.	Si la base de datos no tiene activada la base de datos Flashback, aparecerá el mensaje de advertencia `ORA-16827` . La base de datos retrospectiva opcional ayuda a restablecer automáticamente las bases de datos principales con errores a un punto en el tiempo anterior a la conmutación por error si la propiedad de FastStartFailoverAutoReinstateconfiguración está establecida en `TRUE` (que es la predeterminada).
	
	No CDB
	
	`DGMGRL> enable fast_start failover;`
	`Warning: ORA-16827: Flashback Database is disabled`
	`Enabled in Zero Data Loss Mode.`
	`DGMGRL>`
	`DGMGRL> show configuration`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`orcl_a - Primary database`
	`Warning: ORA-16819: fast-start failover observer not started`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	orcl_d - (*) Physical standby database Warning: ORA-16819: fast-start failover observer not started Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status: WARNING (status updated 29 seconds ago) DGMGRL>	

	CDB
	
	DGMGRL> enable fast_star
	t failover;
	Warning: ORA-16827:
	 Flashback Database is
	 disabled
	Enabled in Zero Data
	 Loss Mode.
	DGMGRL> show configura
	tion;
	Configuration - rds_dg
	  Protection Mode:
	 MaxAvailability
	  Members:
	  rdscdb_a - Primary
	 database
	  Warning: ORA-16819
	: fast-start failover
	 observer not started
	  rdscdb_b - (*)
	 Physical standby
	 database
	Fast-Start Failover:
	 Enabled in Zero Data
	 Loss Mode
	Configuration Status:	

Tarea	Descripción	Habilidades requeridas
	`WARNING (status updated 11 seconds ago)` `DGMGRL>`	

Tarea	Descripción	Habilidades requeridas

Inicie el observador para la supervisión de la FSFO y verifique el estado.	Puede iniciar el observador antes o después de activar la FSFO. Si la FSFO ya está habilitada, el observador comienza inmediatamente a supervisar el estado y las conexiones a las bases de datos principal y en espera. Si la FSFO no está habilitada, el observador no comienza a supervisar hasta que la FSFO esté habilitada.
	
	Al iniciar el observador, la configuración de base de datos principal se mostrará sin ningún mensaje de error, como demuestra el comando anterior `show configuration` .
	
	No CDB
	
	`DGMGRL> start observer;`
	`[W000 2022-12-01T06:16:51.271+00:00] FSFO target standby is orcl_d`
	`Observer 'ip-10-0-1-89' started`
	`[W000 2022-12-01T06:16:51.352+00:00] Observer trace level is set to USER`
	
	`DGMGRL> show configuration`
	`Configuration - rds_dg`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Protection Mode: MaxAvailability Members: orcl_a - Primary database orcl_d - (*) Physical standby database Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status: SUCCESS (status updated 56 seconds ago) DGMGRL> DGMGRL> show observer Configuration - rds_dg Primary: orcl_a Active Target: orcl_d Observer "ip-10-0- 1-89" - Master Host Name: ip-10-0-1 -89 Last Ping to Primary: 1 second ago Last Ping to Target: 1 second ago DGMGRL> CDB DGMGRL> start observer; Succeeded in opening the observer file "/home/oracle/fsfo _ip-10-0-1-56.dat". [W000 2023-01-1 8T07:31:32.589+00:00] FSFO target standby is rdscdb_b	

Tarea	Descripción	Habilidades requeridas

	Observer 'ip-10-0-1-56' started
	The observer log file is '/home/oracle/observer_ip-10-0-1-56.log'.
	
	DGMGRL> show configuration
	Configuration - rds_dg
	  Protection Mode: MaxAvailability
	  Members:
	  rdscdb_a - Primary database
	    rdscdb_b - (*) Physical standby database
	Fast-Start Failover: Enabled in Zero Data Loss Mode
	Configuration Status: SUCCESS (status updated 12 seconds ago)
	DGMGRL>
	
	DGMGRL> show observer;
	Configuration - rds_dg
	  Primary: rdscdb_a
	  Active Target: rdscdb_b
	Observer "ip-10-0-1-56" - Master
	  Host Name: ip-10-0-1-56
	  Last Ping to Primary: 1 second ago
	  Last Ping to Target: 2 seconds ago
	DGMGRL>	

Tarea	Descripción	Habilidades requeridas
Verifique la conmutación por error.	En este escenario, se puede realizar una prueba de conmutación por error deteniendo manualmente la instancia principal. EC2 Antes de detener la EC2 instancia , usa el `tail` comando para monitorear el archivo de registro del observador en función de tu configuración. Use `DGMGRL` para iniciar sesión en la base de datos en espera `orcl_d` con el usuario `RDS_DATAGUARD` y compruebe el estado de Oracle Data Guard. Debería mostrar que `orcl_d` es la nueva base de datos principal. **Note** En este escenario de prueba de conmutación por error, `orcl_d` es una base de datos no relacionada con CDB. Antes de la conmutación por error, la base de datos Flashback se ha habilitado en `orcl_a`. Cuando la anterior base de datos principal vuelva a estar en línea y regrese al	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	estado MOUNT, el observador la restablecerá en una nueva base de datos en espera. La base de datos restablecida actúa como destino de la FSFO para la nueva base de datos principal. Puede verificar los detalles en los registros del observador.
	
	`DGMGRL> show configuration`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`orcl_d - Primary database`
	`Warning: ORA-16824: multiple warnings, including fast-start failover-related warnings, detected for the database`
	`orcl_a - (*) Physical standby database (disabled)`
	`ORA-16661: the standby database needs to be reinstated`
	`Fast-Start Failover: Enabled in Zero Data Loss Mode`
	`Configuration Status:`
	`WARNING (status updated 25 seconds ago)`
	`DGMGRL>`	

Tarea	Descripción	Habilidades requeridas

	A continuación se muestra un ejemplo de salida`observer.log` .
	
	`$ tail -f /tmp/observer.log`
	`Unable to connect to database using rds_custom_orcl_a`
	`[W000 2023-01-18T07:50:32.589+00:00] Primary database cannot be reached.`
	`[W000 2023-01-18T07:50:32.589+00:00] Fast-Start Failover threshold has expired.`
	`[W000 2023-01-18T07:50:32.590+00:00] Try to connect to the standby.`
	`[W000 2023-01-18T07:50:32.590+00:00] Making a last connection attempt to primary database before proceeding with Fast-Start Failover.`
	`[W000 2023-01-18T07:50:32.591+00:00] Check if the standby is ready for failover.`
	`[S002 2023-01-18T07:50:32.591+00:00] Fast-Start Failover started...`
	`2023-01-18T07:50:32.591+00:00`
	`Initiating Fast-Start Failover to database "orcl_d"...`	

Tarea	Descripción	Habilidades requeridas
	[S002 2023-01-18T07:50:32.592+00:00] Initiating Fast-start Failover. Performing failover NOW, please wait... Failover succeeded, new primary is "orcl_d" 2023-01-18T07:55:32.101+00:00 [S002 2023-01-18T07:55:32.591+00:00] Fast-Start Failover finished... [W000 2023-01-18T07:55:32.591+00:00] Failover succeeded. Restart pinging. [W000 2023-01-18T07:55:32.603+00:00] Primary database has changed to orcl_d. [W000 2023-01-18T07:55:33.618+00:00] Try to connect to the primary. [W000 2023-01-18T07:55:33.622+00:00] Try to connect to the primary rds_custom_orcl_d. [W000 2023-01-18T07:55:33.634+00:00] The standby orcl_a needs to be reinstated [W000 2023-01-18T07:55:33.654+00:00] Try to connect to the new standby orcl_a. [W000 2023-01-18T07:55:33.654+00:	

Tarea	Descripción	Habilidades requeridas
	00] Connection to the primary restored! [W000 2023-01-18T07:55:35.654+00:00] Disconnecting from database rds_custom_orcl_d. [W000 2023-01-18T07:55:57.701+00:00] Try to connect to the new standby orcl_a. ORA-12170: TNS:Connect timeout occurred	

Configure la conectividad entre la aplicación Oracle Peoplesoft y la base de datos

Tarea	Descripción	Habilidades requeridas
Cree e inicie el servicio en la base de datos principal.	Puede evitar los cambios en la configuración de la aplicación durante la transición de rol con una entrada de TNS que contenga en la configuración los puntos de conexión de las bases de datos principal y en espera. Puede definir dos servicios de bases de datos basados en roles para admitir cargas de trabajo tanto como cargas de trabajo de read/write e solo lectura. En el siguiente ejemplo, `orcl_rw` es el read/write servicio que está activo en la base de datos principal. `orcl_ro`es el servicio de solo lectura y está activo en la	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	base de datos en espera que se ha abierto en modo de solo lectura. `SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- --------- ----------- ORCL READ WRITE SQL> exec dbms_serv ice.create_service ('orcl_rw','orcl_r w'); PL/SQL procedure successfully completed . SQL> exec dbms_serv ice.create_service ('orcl_ro','orcl_r o'); PL/SQL procedure successfully completed .`  `SQL> exec dbms_serv ice.start_service('orcl_rw'); PL/SQL procedure successfully completed . SQL>`	

Tarea	Descripción	Habilidades requeridas
Inicie el servicio en la base de datos en espera.	Para iniciar el servicio en la base de datos en espera de solo lectura, ejecute el siguiente código. `SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- ---------- ----------- ORCL READ ONLY WITH  APPLY SQL> exec dbms_serv ice.start_service( 'orcl_ro'); PL/SQL procedure  successfully completed . SQL>`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Automatice el inicio del servicio cuando se reinicie la base de datos principal.	Para iniciar automáticamente el servicio en la base de datos principal cuando se reinicie, ejecute el siguiente código. `SQL> CREATE OR REPLACE TRIGGER TrgDgServices after startup on database DECLARE db_role VARCHAR(30); db_open_mode VARCHAR(30); BEGIN SELECT DATABASE_ROLE, OPEN_MODE INTO db_role, db_open_mode FROM V$DATABASE; IF db_role = 'PRIMARY' THEN DBMS_SERV 2 ICE.START_SERVICE('orcl_rw'); END IF; IF db_role = 'PHYSICAL STANDBY' AND db_open_mode LIKE 'READ ONLY%' THEN DBMS_SERVICE.START_SERVICE('orcl_ro'); END IF; END; / Trigger created. SQL>`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Configure una conexión entre la base de datos y la read/write de solo lectura.	Puede usar el siguiente ejemplo de configuración de aplicaciones para la conexión de solo lectura. read/write `ORCL_RW = (DESCRIPTION = (CONNECT_TIMEOUT= 120)(RETRY_COUNT=20)(RETRY_DELAY=3)(TRANSPORT_CONNECT_TIMEOUT=3) (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST=devpsftdb.******.us-west-2.rds.amazonaws.com) (PORT=1521)) (ADDRESS = (PROTOCOL = TCP)(HOST=psftread.******.us-west-2.rds.amazonaws.com) (PORT=1521))) (CONNECT_DATA=(SERVICE_NAME = orcl_rw)))` `ORCL_RO = (DESCRIPTION = (CONNECT_TIMEOUT= 120)(RETRY_COUNT=20)(RETRY_DELAY=3)(TRANSPORT_CONNECT_TIMEOUT=3) (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST=devpsftdb.******.us-west-2.rds.amazonaws.com) (PORT=1521))`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`(ADDRESS = (PROTOCOL = TCP)(HOST=psftread.******.us-west-2.rds.amazonaws.com)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME = orcl_ro))`	

Recursos relacionados

- Habilitar la alta disponibilidad con Data Guard en Amazon RDS Custom para Oracle (guía técnica de AWS)
- Configuración de Amazon RDS como una PeopleSoft base de datos de Oracle (documento técnico de AWS)
- Guía de agente de Oracle Data Guard (documentación de referencia de Oracle)
- Oracle Data Guard Concepts and Administration(documentación de referencia de Oracle)
- Requisitos de configuración de FAN y FCF específicos de Oracle Data Guard (documentación de referencia de Oracle)

Descarga de datos de un clúster de Amazon Redshift entre las cuentas a Amazon S3

Andrew Kamel, Amazon Web Services

Resumen

Al probar aplicaciones, resulta útil disponer de datos de producción en el entorno de pruebas. El uso de los datos de producción puede proporcionarle una evaluación más precisa de la aplicación que desarrolla.

Este patrón extrae los datos de un clúster de Amazon Redshift en un entorno de producción para colocarlos en un bucket de Amazon Simple Storage Service (Amazon S3) en un entorno de desarrollo de Amazon Web Services (AWS).

El patrón sigue los pasos de configuración de las cuentas de DEV y PROD, lo que incluye lo siguiente:

- Recursos necesarios de
- AWS Identity and Access Management Funciones (IAM)
- Ajustes de red para subredes, grupos de seguridad y la nube privada virtual (VPC) para admitir la conexión de Amazon Redshift
- Un ejemplo de AWS Lambda función con un tiempo de ejecución de Python para probar la arquitectura

Para conceder acceso al clúster de Amazon Redshift, el patrón se utiliza AWS Secrets Manager para almacenar las credenciales pertinentes. La ventaja es disponer de toda la información necesaria para conectarse de manera directa al clúster de Amazon Redshift sin necesidad de saber dónde reside el clúster de Amazon Redshift. Además, puede supervisar el uso del secreto.

El secreto guardado en Secrets Manager incluye el host del clúster de Amazon Redshift, el nombre de la base de datos, el puerto y las credenciales pertinentes.

Para obtener información acerca de las consideraciones de seguridad al utilizar este patrón, consulte la sección Prácticas recomendadas.

Requisitos previos y limitaciones

Requisitos previos

- Un clúster de Amazon Redshift que se ejecuta en la cuenta de PROD
- Un bucket de S3 creado en la cuenta de DEV.
- Emparejamiento de VPC entre las cuentas de DEV y PROD, con tablas de rutas ajustadas de manera adecuada.
- Los nombres de host de DNS y la resolución de DNS están habilitados para ambos sistemas interconectados VPCs

Limitaciones

- Según la cantidad de datos que quiera consultar, es posible que se agote el tiempo de espera de la función de Lambda.

  Si la ejecución tarda más tiempo que el tiempo de espera máximo de Lambda (15 minutos), utilice un enfoque asíncrono para el código de Lambda. El ejemplo de código de este patrón utiliza la biblioteca psycopg2 para Python, que actualmente no admite el procesamiento asíncrono.
- Algunos Servicios de AWS no están disponibles en todos. Regiones de AWS Para conocer la disponibilidad de las regiones, consulte Servicios de AWS by Region. Para los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

En el diagrama siguiente, se muestra la arquitectura de destino, con cuentas de DEV y PROD.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. La función de Lambda de la cuenta de DEV asume el rol de IAM necesario para acceder a las credenciales de Amazon Redshift en Secrets Manager de la cuenta de PROD.

   A continuación, la función de Lambda recupera el secreto del clúster de Amazon Redshift.
2. La función Lambda de la cuenta DEV utiliza la información para conectarse al clúster de Amazon Redshift de la cuenta PROD a través del peered. VPCs

   A continuación, la función de Lambda envía un comando de descarga para consultar el clúster de Amazon Redshift en la cuenta de PROD.
3. El clúster de Amazon Redshift de la cuenta de PROD asume el rol de IAM correspondiente para acceder al bucket de S3 de la cuenta de DEV.

El clúster de Amazon Redshift descarga los datos consultados en el bucket de S3 de la cuenta de DEV.

Consulta de datos de Amazon Redshift

En el diagrama siguiente se muestran los roles que se utilizan para recuperar las credenciales de Amazon Redshift y conectarse al clúster de Amazon Redshift. El flujo de trabajo lo inicia la función de Lambda.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El rol `CrossAccount-SM-Read-Role` en la cuenta de DEV asume que el rol `SM-Read-Role` se encuentra en la cuenta de PROD.
2. El rol `SM-Read-Role` utiliza la política adjunta para recuperar el secreto de Secrets Manager.
3. Las credenciales se utilizan para acceder al clúster de Amazon Redshift.

Descarga de datos en Amazon S3

En el diagrama siguiente se muestra el proceso de lectura y escritura entre cuentas para extraer los datos y cargarlo a Amazon S3. El flujo de trabajo lo inicia la función de Lambda. El patrón encadena los roles de IAM en Amazon Redshift. El comando unload que proviene del clúster de Amazon Redshift asume el rol `CrossAccount-S3-Write-Role` y, a continuación, asume el rol `S3-Write-Role`. Este encadenamiento de roles da a Amazon Redshift acceso a Amazon S3.

En el flujo de trabajo se incluyen los pasos siguientes:

1. El rol `CrossAccount-SM-Read-Role` en la cuenta de DEV asume que el rol `SM-Read-Role` se encuentra en la cuenta de PROD.
2. El rol `SM-Read-Role` recupera las credenciales de Amazon Redshift de Secrets Manager.
3. La función de Lambda se conecta al clúster de Amazon Redshift y envía una consulta.
4. El clúster de Amazon Redshift asume el rol `CrossAccount-S3-Write-Role`.
5. El rol `CrossAccount-S3-Write-Role` supone que el rol `S3-Write-Role` se encuentra en la cuenta de DEV.
6. Los resultados de la consulta se descargan en el bucket de S3 de la cuenta de DEV.

Tools (Herramientas)

Servicios de AWS

- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Redshift es un servicio de almacenamiento de datos administrado de varios petabytes en la nube de AWS.
- AWS Secrets Manager lo ayuda a reemplazar las credenciales codificadas en su código, incluidas contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub unload-redshift-to-s3-python.

Prácticas recomendadas

Exención de responsabilidad de seguridad

Antes de implementar esta solución, tenga en cuenta las siguientes recomendaciones de seguridad importantes:

- Recuerde que conectar las cuentas de desarrollo y producción puede aumentar el alcance y reducir la posición de seguridad general. Recomendamos implementar esta solución solo de manera temporal, extraer la parte de los datos necesaria y, a continuación, destruir de inmediato los recursos implementados. Para destruir los recursos, debe eliminar la función de Lambda, eliminar todos los roles y políticas de IAM que se crearon para esta solución y revocar el acceso a la red que se haya concedido entre las cuentas.
- Consulte a sus equipos de seguridad y cumplimiento antes de copiar los datos de los entornos de producción a los de desarrollo. Por lo general, la información de identificación personal (PII),

la información de salud protegida (PHI) y otros datos confidenciales o regulados no deben copiarse de esta manera. Copie solo la información no confidencial que esté disponible al público (por ejemplo, datos bursátiles públicos del frontend de una tienda). Considere la posibilidad de tokenizar o anonimizar los datos, o de generar datos de prueba sintéticos, en lugar de utilizar los datos de producción siempre que sea posible. Uno de los principios de seguridad de AWS es mantener a las personas alejadas de los datos. En otras palabras, los desarrolladores no deben realizar operaciones en la cuenta de producción.

- Restrinja el acceso a la función de Lambda en la cuenta de desarrollo porque puede leer datos del clúster de Amazon Redshift en el entorno de producción.
- Para evitar interrumpir el entorno de producción, implemente las recomendaciones siguientes:
  - Utilice una cuenta de desarrollo independiente y dedicada para las actividades de prueba y desarrollo.
  - Implemente controles estrictos de acceso a la red y limite el tráfico entre las cuentas a solo lo necesario.
  - Supervise y audite el acceso al entorno de producción y a los orígenes de datos.
  - Implemente controles de acceso con privilegios mínimos para todos los recursos y servicios implicados.
  - Revise y modifique periódicamente las credenciales, como AWS Secrets Manager los secretos y las claves de acceso a los roles de IAM.
- Consulte la documentación de seguridad siguiente para ver los servicios que se utilizan en este artículo:
  - AWS Lambda seguridad
  - Seguridad de Amazon Redshift
  - Seguridad de Amazon S3
  - AWS Secrets Manager seguridad
  - Prácticas recomendadas de seguridad de IAM

La seguridad es una de las prioridades principales al acceder a los datos y recursos de producción. Siga siempre las prácticas recomendadas, implemente controles de acceso con privilegios mínimos y revise y actualice de manera periódica sus medidas de seguridad.

Epics

Datos de consulta de Amazon Redshift

Tarea	Descripción	Habilidades requeridas
Cree un secreto para el clúster de Amazon Redshift.	Para crear el secreto para el clúster de Amazon Redshift, haga lo siguiente: 1. En la cuenta PROD, inicie sesión en y abra la Consola de administración de AWS consola Secrets Manager en https://console.aws.amazon.com/secretsmanager/. 2. Elija Almacenar un secreto nuevo. 3. Seleccione Credenciales para el almacén de datos de Amazon Redshift. 4. En Nombre de usuario y Contraseña, indique los valores de la instancia y confirme o elija un valor en Clave de cifrado. 5. Elija el almacén de datos de Amazon Redshift al que accederá el secreto. 6. Escriba `Redshift-Creds-Secret` en el nombre del secreto. 7. Complete los pasos de creación restantes con las opciones predeterm	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	inadas y, a continuación, elija Almacenar. 8. Consulte su secreto y anote el valor de ARN del secreto que se generó para identific ar el secreto.	

Tarea	Descripción	Habilidades requeridas
Cree un rol para acceder a Secrets Manager.	Para crear el rol, haga lo siguiente: 1. En la cuenta PROD, abra la consola de IAM en. https://console.aws.amazon.com/iam/ 2. Seleccione Políticas. 3. Elija Crear política. 4. Elija la pestaña JSON y, a continuación, indique una política de IAM como la siguiente: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "secretsmanager:GetResourcePolicy", "secretsmanager:GetSecretValue", "secretsmanager:DescribeSecret", "secretsmanager:ListSecretVersionIds" ], "Resource": [`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	"<Redshift-Creds-Secret-ARN>"
	]
	},
	{
	"Effect": "Allow",
	"Action": "secretsmanager:ListSecrets",
	"Resource": "*"
	}
	]
	}
	Sustituya `Redshift-Creds-Secret-ARN` por el nombre de recurso de Amazon (ARN) del secreto de Secrets Manager que contiene la información y las credencia les del clúster de Amazon Redshift.	

Descargar datos en Amazon S3

Tarea	Descripción	Habilidades requeridas
Cree un rol para acceder al bucket de S3.	Para crear el rol y acceder al bucket de S3, haga lo siguiente: 1. En la cuenta de DEV, abra la consola de IAM.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	2. Seleccione Políticas. 3. Elija Crear política. 4. Elija la pestaña JSON y, a continuación, indique una política de IAM como la siguiente: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "kmsstmt", "Effect": "Allow", "Action": [ "kms:Decrypt", "kms:Encrypt", "kms:GenerateDataKey" ], "Resource": [ "<kms-key-arn>" ] }, { "Sid": "s3stmt", "Effect": "Allow", "Action": [ "s3:PutObject", "s3:Get*", "s3:List*" ],`	

Tarea	Descripción	Habilidades requeridas

	<pre>"Resource": [
	"arn:aws:
	s3:::mybucket",
	"arn:aws:
	s3:::mybucket/*"
	]
	}
	]
	}</pre>
	Sustituya `mybucket` por el nombre del bucket de S3 al que quiere acceder. Además, si el depósito de S3 está cifrado, `kms-key-arn` sustitúyalo por el ARN de la clave AWS Key Management Service (AWS KMS) utilizada para cifrar el depósito de S3. De lo contrario, no necesitará la AWS KMS sección de la política.
	5. Elija Revisar política, escriba `S3-Write-Policy` como nombre de la política y, a continuación, elija Crear política.
	6. Seleccione Roles en el panel de navegación.
	7. Elija Crear rol.
	8. Para el rol de entidad de confianza, elija Política de confianza personalizada.	

Tarea	Descripción	Habilidades requeridas
	9. Elija Siguiente: permisos y, a continuación, seleccione la política S3-Write-Policy que creó. 10. Introduzca `S3-Write-Role` como nombre del rol y, a continuación, elija Crear rol.	

Tarea	Descripción	Habilidades requeridas
Cree el rol de Amazon Redshift.	Para crear el rol de Amazon Redshift, haga lo siguiente: 1. En la cuenta de PROD, abra la consola de IAM. 2. Seleccione Políticas. 3. Elija Crear política. 4. Elija la pestaña JSON y, a continuación, indique una política de IAM como la siguiente: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "CrossAccountPolicy", "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "S3-Write-Role-ARN" } ] }` Sustituya `S3-Write-Role-ARN` por el ARN del rol `S3-Write-Role` de la cuenta de DEV. 5. Elija Revisar política, escriba `S3-Write-Role-`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`Assume-Policy` como nombre de la política y, a continuación, elija Crear política. 6. En el panel de navegación, seleccione Roles y luego seleccione Crear rol. 7. Elija Servicio de AWS como su tipo de entidad de confianza y, a continuación, elija Redshift, Redshift - personalizable. 8. Elija Siguiente: permisos y, a continuación, seleccione la política S3-Write-Role-Assume-Policy que creó. 9. Introduzca `CrossAccount-S3-Write-Role` como nombre del rol y, a continuación, elija Crear rol. 10 Asocie el rol de IAM al clúster de Amazon Redshift.	

Implementación de la función de Lambda

Tarea	Descripción	Habilidades requeridas
Implemente la función de Lambda.	Para implementar una función de Lambda en la VPC emparejada, haga lo siguiente: 1. Abra la consola Lambda en. https://console.aws.amazon.com/lambda/	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	2. Elija Funciones. 3. Elija Crear función. 4. En Basic information (Información básica), para Function name (Nombre de función), escriba un nombre para la función. 5. En Tiempo de ejecución, elija Python 3.8. 6. Amplíe Cambiar rol de ejecución predeterminado y, a continuación, haga lo siguiente: a. Elija Usar un rol existente. b. En Función existente , seleccione la función Lambda CrossAccount-RM-Read-Role que creó anteriormente. 7. Amplíe Configuración avanzada y haga lo siguiente: a. Seleccione la casilla Habilitar VPC. b. En VPC, seleccione la VPC emparejada en la cuenta de DEV. c. En Subredes, seleccione la subred privada. d. En Grupos de seguridad , seleccione el grupo de	

Tarea	Descripción	Habilidades requeridas
	seguridad predeterm inado. 8. Elija Crear función. 9. Agregue la biblioteca psycopg2 como capa a la función de Lambda. **Note** Puede utilizar una capa ya implement ada del repositorio psycopg2-lambda-layer. Asegúrese de utilizar la URL en función de su tiempo de ejecución Región de AWS y el de Python.	

Prueba de la arquitectura

Tarea	Descripción	Habilidades requeridas

Importe los recursos necesario s.	Para importar los recursos necesarios, ejecute los comandos siguientes:
	
	`import ast`
	`import boto3`
	`import psycopg2`
	`import base64`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`from botocore. exceptions import ClientError`	

Tarea	Descripción	Habilidades requeridas

Ejecute la función de controlador de Lambda.	La función Lambda usa AWS Security Token Service (AWS STS) para el acceso entre cuentas y la administración temporal de credenciales. La función utiliza la operación AssumeRole API para asumir temporalmente los permisos de la `sm_read_role` función de IAM.
	
	Para ejecutar la función de Lambda, utilice el código de ejemplo siguiente:
	
	`def lambda_handler(event, context):`
	`  sts_client = boto3.client('sts')`
	
	`  # Secrets Manager Configurations`
	`  secret_name = "redshift_creds"`
	`  sm_region = "eu-west-1"`
	`  sm_read_role = "arn:aws:iam::PROD_ACCOUNT_NUMBER:role/SM-Read-Role"`
	
	`  # S3 Bucket Configurations`
	`  s3_bucket_path = "s3://mybucket/"`
	`  s3_bucket_region = "eu-west-1"`
	`  s3_write_role = "arn:aws:iam::DEV_`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	ACCOUNT_NUMBER:role/S3-Write-Role"
	
	# Redshift Configurations
	sql_query = "select * from category"
	redshift_db = "dev"
	redshift_s3_write_role = "arn:aws:iam::PROD_ACCOUNT_NUMBER:role/CrossAccount-S3-Write-Role"
	
	chained_s3_write_role = "%s,%s" % (redshift_s3_write_role, s3_write_role)
	
	assumed_role_object = sts_client.assume_role(
	RoleArn=sm_read_role,
	RoleSessionName="CrossAccountRoleAssumption",
	ExternalId="YOUR_EXTERNAL_ID",
	)
	credentials = assumed_role_object['Credentials']
	
	secret_dict = ast.literal_eval(get_secret(credentials, secret_name, sm_region))
	execute_query(secret_dict, sql_query, s3_bucket_path,	

Tarea	Descripción	Habilidades requeridas

	<pre>chained_s3_write_role, s3_bucket_region, redshift_db)
	
	    return {
	        'statusCode': 200
	    }</pre>	

Tarea	Descripción	Habilidades requeridas

Obtenga el secreto.	Para obtener el secreto de Amazon Redshift, utilice el código de ejemplo siguiente:
	
	`def get_secret(credentials, secret_name, sm_region):`
	`  # Create a Secrets Manager client`
	`  session = boto3.session.Session()`
	`  sm_client = session.client(`
	`  service_name='secretsmanager',`
	`  aws_access_key_id=credentials['AccessKeyId'],`
	`  aws_secret_access_key=credentials['SecretAccessKey'],`
	`  aws_session_token=credentials['SessionToken'],`
	`  region_name=sm_region`
	`  )`
	
	`  try:`
	`  get_secret_value_response = sm_client.get_secret_value(`
	`  SecretId=secret_name`
	`  )`
	`  except ClientError as e:`
	`  print(e)`
	`  raise e`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	<pre> else:
	        if 'SecretSt
	ring' in get_secre
	t_value_response:
	            return
	 get_secret_value_r
	esponse['SecretStr
	ing']
	        else:
	            return
	 base64.b64decode(g
	et_secret_value_re
	sponse['SecretBina
	ry'])</pre>	

Tarea	Descripción	Habilidades requeridas

Ejecute el comando unload.	Para descargar los datos en el bucket de S3 utilice el código de ejemplo siguiente:
	
	`def execute_query(secret_dict, sql_query, s3_bucket_path, chained_s3_write_role, s3_bucket_region, redshift_db):`
	`  conn_string = "dbname='%s' port='%s' user='%s' password='%s' host='%s'" \`
	`  %(redshift_db,`
	`  secret_dict["port"],`
	`  secret_dict["username"],`
	`  secret_dict["password"],`
	`  secret_dict["host"])`
	`  con = psycopg2.connect(conn_string)`
	`  unload_command = "UNLOAD ('{}') TO '{}' IAM_ROLE '{}' DELIMITER '|' REGION '{}';" \`
	`  .format(sql_query,`
	`  s3_bucket_path + str(datetime.datetime.now()) + ".csv",`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	<pre>chained_s3_write_role,
	
	s3_bucket_region)
	
	# Opening a cursor and run query
	cur = con.cursor()
	cur.execute(unload_command)
	
	print(cur.fetchone())
	cur.close()
	con.close()</pre>	

Limpieza

Tarea	Descripción	Habilidades requeridas
Elimine la función de Lambda.	Para evitar incurrir en costos imprevistos, elimine los recursos y la conexión entre las cuentas de DEV y PROD. Para quitar la función de Lambda, haga lo siguiente: 1. Abra la AWS Lambda consola en. https://console.aws.amazon.com/lambda/ 2. Ubique y seleccione la función de Lambda que creó.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	3. Elija Acciones y, a continuación, elija Eliminar. 4. Confirme la eliminación.	

Tarea	Descripción	Habilidades requeridas
Elimine las políticas y los roles de IAM.	Elimine las políticas y los roles de IAM de las cuentas de DEV y PROD. En la cuenta de DEV, haga lo siguiente: 1. Abra la consola de IAM. 2. Elimine los roles siguientes: • `S3-Write-Role` • `CrossAccount-RM-Read-Role` (rol de Lambda) 3. Elimine las políticas asociadas: • `S3-Write-Policy` • La CrossAccount política para asumir las funciones de la cuenta PROD En la cuenta de PROD, haga lo siguiente: 1. Abra la consola de IAM. 2. Elimine los roles siguientes: • `SM-Read-Role` • `CrossAccount-S3-Write-Role` 3. Elimine las políticas asociadas: • La CrossAccount política de acceso a Secrets Manager	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• `S3-Write-Role-Assume-Policy`	
Elimine el secreto en Secrets Manager.	Para eliminar el secreto, haga lo siguiente: 1. En la cuenta de PROD, abra la consola de Secrets Manager. 2. Ubique y seleccione el nombre del secreto `Redshift-Creds-Secret` . 3. Elija Actions (Acciones) y Delete secret (Eliminar secreto). 4. Confirme la eliminación.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Elimine las reglas de grupos de seguridad y emparejamiento de VPC.	Para eliminar las reglas de grupos de seguridad y emparejamiento de VPC, haga lo siguiente: 1. En la cuenta PROD, abre la EC2 consola Amazon en https://console.aws.amazon.com/ec2/. 2. Vaya a Grupos de seguridad. 3. Encuentre el grupo de seguridad que utiliza el clúster de Amazon Redshift. 4. Edite las reglas de entrada y elimine la regla que permite las conexiones desde la VPC de Lambda de la cuenta de DEV. 5. Vaya a Conexiones de emparejamiento de VPC y elimine la conexión de emparejamiento.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Elimine los datos del bucket de S3.	Para eliminar los datos de Amazon S3, haga lo siguiente: 1. En la cuenta DEV, abra la consola Amazon S3 en https://console.aws.amazon.com/s3/. 2. Encuentre el bucket que utilizó para el almacenamiento de datos. 3. Elimine los objetos del bucket o elimine todo el bucket si ya no es necesario.	DevOps ingeniero
Limpia AWS KMS las llaves.	Si ha creado alguna AWS KMS clave personalizada para el cifrado, haga lo siguiente: 1. Abra la AWS KMS consola en https://console.aws.amazon.com/kms/. 2. Encuentre las claves creadas para este patrón. 3. Programe la eliminación de claves. (Hay un periodo de espera obligatorio para eliminar la clave).	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Revisa y elimina los CloudWatch registros de Amazon.	Para eliminar los CloudWatch registros, haga lo siguiente: 1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/. 2. Compruebe si hay grupos de registros que haya creado la función de Lambda o el clúster de Amazon Redshift. 3. Elimine estos grupos de registro si ya no son necesarios.	DevOps ingeniero

Recursos relacionados

- CloudWatch Documentación de Amazon
- documentación de IAM
- Documentación de Lambda
- Documentación de Amazon Redshift
- Documentación de Amazon S3
- AWS Secrets Manager documentación
- AWS principios de seguridad

Información adicional

Después de descargar los datos de Amazon Redshift en Amazon S3, puede analizarlos mediante Amazon Athena.

Amazon Athena es un servicio de consultas de macrodatos que resulta útil cuando es necesario acceder a volúmenes grandes de datos. Puede utilizar Athena sin tener que aprovisionar servidores ni bases de datos. Athena admite consultas complejas y puede ejecutarla en objetos distintos.

Como ocurre con la mayoría Servicios de AWS, la principal ventaja de usar Athena es que proporciona una gran flexibilidad en la forma de ejecutar las consultas sin la complejidad adicional. Cuando utiliza Athena, puede consultar distintos tipos de datos, como CSV y JSON, en Amazon S3 sin cambiar el tipo de datos. Puede consultar datos de diversas fuentes, incluso externas AWS. Athena reduce la complejidad porque no es necesario que administre los servidores. Athena lee los datos de manera directa de Amazon S3 sin cargarlos ni cambiarlos antes de ejecutar la consulta.

Patrones de migración de bases de datos según carga de trabajo

Temas

- IBM
- Microsoft
- N/A
- Código abierto
- Oracle
- SAP

IBM

- Migre una base de datos Db2 de Amazon EC2 a Aurora compatible con MySQL mediante AWS DMS
- Migre Db2 for LUW a Amazon EC2 mediante el envío de registros para reducir el tiempo de interrupción
- Migración de Db2 para LUW a Amazon EC2 con recuperación de desastres de alta disponibilidad
- Migre de IBM Db2 en Amazon EC2 a Aurora compatible con PostgreSQL mediante AWS DMS y AWS SCT
- Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2
- Transmita datos desde IBM Db2, SAP, Sybase y otras bases de datos a MongoDB Atlas en AWS

Microsoft

- Acelere el descubrimiento y la migración de las cargas de trabajo de Microsoft a AWS
- Acceda a tablas locales de Microsoft SQL Server desde Microsoft SQL Server en Amazon EC2 mediante servidores enlazados
- Evaluar el rendimiento de las consultas para migrar bases de datos de SQL Server a MongoDB Atlas en AWS
- Automatice las tareas de bases de datos en SQL Server Express en Amazon EC2 mediante un programador AWS Lambda de tareas
- Cambie las aplicaciones de Python y Perl para que admitan la migración de bases de datos de Microsoft SQL Server a una edición compatible con PostgreSQL de Amazon Aurora
- Configurar el enrutamiento de solo lectura en los grupos de disponibilidad de Always On en SQL Server on AWS
- Configure la autenticación de Windows para Amazon RDS for Microsoft SQL Server mediante AWS Managed Microsoft AD
- Cree CloudFormation plantillas de AWS para las tareas de AWS DMS con Microsoft Excel y Python
- Implemente instancias de clústeres de conmutación por error de SQL Server en Amazon EC2 y Amazon FSx mediante Terraform
- Exportación de una base de datos de Microsoft SQL Server a Amazon S3 mediante AWS DMS
- Exporte tablas de Amazon RDS for SQL Server a un bucket de S3 mediante AWS DMS
- Implemente SHA1 el hash para los datos de PII al migrar de SQL Server a PostgreSQL
- Incorpore y migre instancias de EC2 Windows a una cuenta de AWS Managed Services
- Configure un clúster de conmutación por error de Microsoft SQL Server en Amazon EC2 FSx mediante Windows File Server
- Migración de una cola de mensajes de Microsoft Azure Service Bus a Amazon SQS
- Migre una base de datos de Microsoft SQL Server de Amazon EC2 a Amazon DocumentDB mediante AWS DMS
- Migración de una base de datos de Microsoft SQL Server a Aurora MySQL mediante AWS DMS y AWS SCT
- Migración de una aplicación .NET de Microsoft Azure App Service a AWS Elastic Beanstalk
- Migre una base de datos local de Microsoft SQL Server a Amazon EC2

- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server
- Migración de bases de datos en las instalaciones de Microsoft SQL Server a Amazon RDS para SQL Server mediante servidores vinculados
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server mediante métodos nativos de copia de seguridad y restauración
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon Redshift mediante AWS DMS
- Migración de una base de datos en las instalaciones de Microsoft SQL Server a Amazon Redshift mediante agentes de extracción de datos de AWS SCT
- Migre una base de datos local de Microsoft SQL Server a Microsoft SQL Server en Amazon EC2 con Linux
- Migración de datos de Microsoft Azure Blob a Amazon S3 mediante Rclone
- Migre IIS-hosted aplicaciones a Amazon EC2 mediante appcmd.exe
- Migre el grupo de disponibilidad Always On de Microsoft SQL Server mediante AWS Transform MGN
- Migre una base de datos local de Microsoft SQL Server a Amazon EC2 mediante MGN
- Migrar una base de datos relacional a MongoDB Atlas en AWS
- Migración de SQL Server a AWS mediante grupos de disponibilidad distribuidos
- Migración de los certificados SSL de Windows a un equilibrador de carga de aplicación mediante ACM
- Vuelva a alojar las cargas de trabajo en las instalaciones en la nube de AWS: lista de verificación de migración
- Resolver los errores de conexión después de migrar Microsoft SQL Server a la nube de AWS
- Envíe notificaciones para una instancia de base de datos de Amazon RDS para SQL Server mediante un servidor SMTP en las instalaciones y el Correo de base de datos
- Configure una CI/CD canalización para la migración de bases de datos mediante Terraform
- Configure una infraestructura Multi-AZ para una FCI Always On de SQL Server mediante Amazon FSx

N/A

- Cree un proceso de aprobación para las solicitudes de firewall durante una migración de rehospedaje a AWS
- Cifrar una instancia de base de datos de Amazon RDS para PostgreSQL existente
- Costos de almacenamiento estimados para una tabla de Amazon DynamoDB
- Implemente recuperación de desastres entre regiones con AWS DMS y Amazon Aurora

Código abierto

- Generación automática de un modelo de PynamoDB y funciones CRUD para Amazon DynamoDB mediante una aplicación de Python
- Conectar mediante un túnel SSH en pgAdmin
- Crear usuarios y roles de aplicaciones en Aurora compatible con PostgreSQL
- Habilite conexiones cifradas para instancias de base de datos de PostgreSQL en Amazon RDS
- Migre Amazon RDS for Oracle a Amazon RDS for PostgreSQL con y utilizando y AWS SCT AWS DMS AWS CLI CloudFormation
- Migración de una base de datos de MariaDB en las instalaciones hasta Amazon RDS para MariaDB mediante herramientas nativas
- Migración de una base de datos MySQL en las instalaciones a Amazon EC2
- Migración de una base de datos MySQL en las instalaciones a Amazon RDS para MySQL
- Migración de una base de datos de MySQL en las instalaciones a Aurora MySQL
- Migración de una base de datos PostgreSQL en las instalaciones a Aurora PostgreSQL
- Migrar una base de datos de Couchbase Server a Amazon EC2
- Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2 con Auto Scaling
- Migre de Oracle 8i o 9i a Amazon RDS para Oracle con AWS DMS SharePlex
- Migre de PostgreSQL en EC2 Amazon a Amazon RDS para PostgreSQL mediante pglogical
- Migración de aplicaciones Java locales en las instalaciones a AWS mediante AWS App2Container
- Migre bases de datos MySQL locales a Aurora MySQL mediante Percona, XtraBackup Amazon EFS y Amazon S3
- Migración de tablas externas de Oracle a Amazon Aurora compatible con PostgreSQL
- Migración de funciones y procedimientos de Oracle con más de 100 argumentos a PostgreSQL
- Migración de las cargas de trabajo de Redis a Redis Enterprise Cloud en AWS
- Reinicie automáticamente el AWS El agente de replicación tras un reinicio de RHEL sin deshabilitar SELinux
- Programe trabajos para Amazon RDS para PostgreSQL y Aurora PostgreSQL mediante Lambda y Secrets Manager
- Transportar bases de datos PostgreSQL entre dos instancias de base de datos de Amazon RDS utilizando pg_transport
- Descarga de datos de un clúster de Amazon Redshift entre las cuentas a Amazon S3

Oracle

- Agregue HA a Oracle PeopleSoft en Amazon RDS Custom mediante una réplica de lectura
- Convertir consultas JSON de Oracle en SQL de bases de datos PostgreSQL
- Convierta VARCHAR2 (1) el tipo de datos de Oracle en un tipo de datos booleano para Amazon Aurora PostgreSQL
- Emule Oracle DR mediante una base de datos global de Aurora compatible con PostgreSQL
- Emule las matrices PL/SQL asociativas de Oracle en Amazon Aurora PostgreSQL y Amazon RDS for PostgreSQL
- Calcule el tamaño del motor de Amazon RDS para una base de datos de Oracle mediante informes de AWR
- Gestionar bloques anónimos en instrucciones SQL dinámicas en Aurora PostgreSQL
- Migración gradual de Amazon RDS para Oracle a Amazon RDS para PostgreSQL con Oracle SQL Developer y AWS SCT
- Cargar archivos BLOB en TEXT mediante la codificación de archivos en Aurora compatible con PostgreSQL
- Migración de Amazon RDS para Oracle a Amazon RDS para PostgreSQL en modo SSL mediante AWS DMS
- Migre una base de datos de Amazon RDS for Oracle a Cuenta de AWS otra Región de AWS y AWS DMS utilícela para la replicación continua
- Migre una base de datos Oracle local a Amazon EC2 mediante Oracle Data Pump
- Migre una base de datos Oracle local a Amazon OpenSearch Service mediante Logstash
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para MySQL con AWS DMS y AWS SCT
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle
- Migre una base de datos de Oracle a Amazon RDS mediante la importación directa de Oracle Data Pump a través de un enlace de base de datos
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para PostgreSQL mediante Oracle Bystander y AWS DMS
- Migre una base de datos Oracle local a Oracle on Amazon EC2

- Migre una base de datos Oracle de Amazon EC2 a Amazon RDS para MariaDB con AWS DMS y AWS SCT
- Migre una base de datos Oracle de Amazon EC2 a Amazon RDS for Oracle mediante AWS DMS
- Migración de una base de datos de Oracle a Amazon DynamoDB mediante AWS DMS
- Migre una base de datos Oracle a Amazon RDS for Oracle mediante adaptadores de archivos planos de GoldenGate Oracle
- Migración de una base de datos de Oracle a Amazon Redshift con AWS DMS y AWS SCT
- Migración de una base de datos de Oracle a Aurora PostgreSQL con AWS DMS y AWS SCT
- Migre una EnterpriseOne base de datos de Oracle JD Edwards a AWS mediante Oracle Data Pump y AWS DMS
- Migración de una tabla particionada de Oracle a PostgreSQL mediante AWS DMS
- Migre una PeopleSoft base de datos de Oracle a AWS mediante AWS DMS
- Migración de datos de una base de datos de Oracle en las instalaciones a Aurora PostgreSQL
- Migración de de Amazon RDS para Oracle a Amazon RDS para MySQL
- Migración de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante la vista materializada y AWS DMS
- Migre de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante AWS DMS SharePlex
- Migre de Oracle Database a Amazon RDS for PostgreSQL mediante Oracle GoldenGate
- Migración de Oracle en Amazon EC2 a Amazon RDS para MySQL con AWS DMS y AWS SCT
- Migre de Oracle WebLogic a Apache Tomcat (ToMEE) en Amazon ECS
- Migración de índices basados en funciones de Oracle a PostgreSQL
- Migración de aplicaciones heredadas de Oracle Pro*C a ECPG
- Migración de valores CLOB de Oracle a filas individuales en PostgreSQL en AWS
- Migración de códigos de error de Oracle Database a una base de datos Amazon Aurora compatible con PostgreSQL
- Migración de las funciones nativas de Oracle a PostgreSQL mediante extensiones
- Migre Oracle PeopleSoft a Amazon RDS Custom
- Migración de la funcionalidad ROWIdentificador de Oracle a PostgreSQL en AWS
- Migración de los paquetes pragma SERIALLY_REUTILIZABLE de Oracle a PostgreSQL
- Migración de columnas generadas de forma virtual de Oracle a PostgreSQL
- Supervise GoldenGate los registros de Oracle mediante Amazon CloudWatch

- Análisis de las dependencias de los objetos para realizar migraciones parciales de bases de datos de Oracle a PostgreSQL
- Redefina la plataforma de Oracle Database Enterprise Edition a Standard Edition 2 en Amazon RDS para Oracle
- Configure una HA/DR arquitectura para Oracle E-Business Suite en Amazon RDS Custom con una base de datos en espera activa
- Configure la funcionalidad UTL_FILE de Oracle en Aurora compatible con PostgreSQL
- Funciones de transición para una PeopleSoft aplicación de Oracle en Amazon RDS Custom for Oracle
- Validar los objetos de la base de datos después de migrar de Oracle a Amazon Aurora PostgreSQL

SAP

- Realice copias de seguridad automáticas de las bases de datos de SAP HANA mediante Systems Manager y EventBridge
- Migración de SAP ASE a Amazon RDS para SQL Server utilizando AWS DMS
- Migre SAP ASE de Amazon EC2 a Amazon Aurora compatible con PostgreSQL mediante AWS SCT y AWS DMS
- Migración de SAP HANA a AWS mediante SAP HSR con el mismo nombre de host
- Configurar la recuperación de desastres para SAP en IBM Db2 en AWS

Más patrones

- Acceso a una base de datos de Amazon Neptune desde un contenedor de Amazon EKS
- Acceder, consultar y unirse a las tablas de Amazon DynamoDB con Athena
- Permitir a EC2 las instancias el acceso de escritura a los buckets de S3 en las cuentas de AMS
- Analice y visualice datos JSON anidados con Amazon Athena y Amazon Quick Sight
- Automatizar las copias de seguridad de las instancias de base de datos de Amazon RDS para PostgreSQL mediante AWS Batch
- Archivar automáticamente los elementos en Amazon S3 con DynamoDB TTL
- Corrija automáticamente las instancias y los clústeres de bases de datos de Amazon RDS no cifrados
- Detener e iniciar automáticamente una instancia de base de datos de Amazon RDS mediante AWS Systems Manager Maintenance Windows
- Construye una AWS landing zone que incluya MongoDB Atlas
- Cree programas COBOL Db2 mediante y AWS Mainframe Modernization AWS CodeBuild
- Cree una malla de datos empresarial con Amazon DataZone y AWS CDK AWS CloudFormation
- Cambie las aplicaciones de Python y Perl para que admitan la migración de bases de datos de Microsoft SQL Server a una edición compatible con PostgreSQL de Amazon Aurora
- Convierta y desempaquete datos EBCDIC a ASCII en AWS mediante Python
- Convierta la característica temporal NORMALIZE de Teradata en Amazon Redshift SQL
- Convierta la característica RESET WHEN de Teradata en Amazon Redshift SQL
- Convierta VARCHAR2 (1) el tipo de datos de Oracle en un tipo de datos booleano para Amazon Aurora PostgreSQL
- Crear usuarios y roles de aplicaciones en Aurora compatible con PostgreSQL
- Cree CloudFormation plantillas de AWS para las tareas de AWS DMS con Microsoft Excel y Python
- Entregue registros de DynamoDB a Amazon S3 mediante Kinesis Data Streams y Firehose con AWS CDK
- Implemente un clúster de Cassandra en Amazon EC2 con estática privada IPs para evitar el reequilibrio
- Implemente un clúster de CockroachDB en Amazon EKS mediante Terraform

- Desarrolle asistentes avanzados de IA generativa basados en chat mediante RAG y solicitudes ReAct
- Emule Oracle DR mediante una base de datos global de Aurora compatible con PostgreSQL
- Habilite el archivado de DB2 registros directamente en Amazon S3 en una base de datos IBM Db2
- Habilitar el cifrado transparente de datos en Amazon RDS para SQL Server
- Exportación de una base de datos de Microsoft SQL Server a Amazon S3 mediante AWS DMS
- Implemente SHA1 el hash para los datos de PII al migrar de SQL Server a PostgreSQL
- Migración gradual de Amazon RDS para Oracle a Amazon RDS para PostgreSQL con Oracle SQL Developer y AWS SCT
- Cargar archivos BLOB en TEXT mediante la codificación de archivos en Aurora compatible con PostgreSQL
- Administrar credenciales mediante AWS Secrets Manager
- Migre una base de datos Db2 de Amazon EC2 a Aurora compatible con MySQL mediante AWS DMS
- Migre una base de datos de Microsoft SQL Server de Amazon EC2 a Amazon DocumentDB mediante AWS DMS
- Migración de una base de datos de Microsoft SQL Server a Aurora MySQL mediante AWS DMS y AWS SCT
- Migración de Amazon RDS para Oracle a Amazon RDS para PostgreSQL en modo SSL mediante AWS DMS
- Migre Amazon RDS for Oracle a Amazon RDS for PostgreSQL con y utilizando y AWS SCT AWS DMS AWS CLI CloudFormation
- Migración de una instancia de base de datos de Amazon RDS a otra VPC o cuenta
- Migre una base de datos de Amazon RDS for Oracle a Cuenta de AWS otra Región de AWS y AWS DMS utilícela para la replicación continua
- Migración de un clúster de Amazon Redshift a una región de AWS en China
- Migración de una base de datos de MariaDB en las instalaciones hasta Amazon RDS para MariaDB mediante herramientas nativas
- Migre una base de datos local de Microsoft SQL Server a Amazon EC2
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server

- Migración de bases de datos en las instalaciones de Microsoft SQL Server a Amazon RDS para SQL Server mediante servidores vinculados
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server mediante métodos nativos de copia de seguridad y restauración
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon Redshift mediante AWS DMS
- Migración de una base de datos en las instalaciones de Microsoft SQL Server a Amazon Redshift mediante agentes de extracción de datos de AWS SCT
- Migre una base de datos local de Microsoft SQL Server a Microsoft SQL Server en Amazon EC2 con Linux
- Migración de una base de datos MySQL en las instalaciones a Amazon RDS para MySQL
- Migración de una base de datos de MySQL en las instalaciones a Aurora MySQL
- Migre una base de datos Oracle local a Amazon EC2 mediante Oracle Data Pump
- Migre una base de datos Oracle local a Amazon OpenSearch Service mediante Logstash
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para MySQL con AWS DMS y AWS SCT
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para PostgreSQL mediante Oracle Bystander y AWS DMS
- Migre una base de datos Oracle local a Oracle on Amazon EC2
- Migración de una base de datos PostgreSQL en las instalaciones a Aurora PostgreSQL
- Migre una base de datos ThoughtSpot Falcon local a Amazon Redshift
- Migre una base de datos Oracle de Amazon EC2 a Amazon RDS para MariaDB con AWS DMS y AWS SCT
- Migre una base de datos Oracle de Amazon EC2 a Amazon RDS for Oracle mediante AWS DMS
- Migre una base de datos Oracle a Amazon RDS for Oracle mediante adaptadores de archivos planos de GoldenGate Oracle
- Migración de una base de datos de Oracle a Amazon Redshift con AWS DMS y AWS SCT
- Migración de una base de datos de Oracle a Aurora PostgreSQL con AWS DMS y AWS SCT

- Migre una EnterpriseOne base de datos de Oracle JD Edwards a AWS mediante Oracle Data Pump y AWS DMS
- Migración de una tabla particionada de Oracle a PostgreSQL mediante AWS DMS
- Migre una PeopleSoft base de datos de Oracle a AWS mediante AWS DMS
- Migrar una base de datos de Couchbase Server a Amazon EC2
- Migración de datos de una base de datos de Oracle en las instalaciones a Aurora PostgreSQL
- Migre datos al Nube de AWS mediante Starburst
- Migre Db2 for LUW a Amazon EC2 mediante el envío de registros para reducir el tiempo de interrupción
- Migración de Db2 para LUW a Amazon EC2 con recuperación de desastres de alta disponibilidad
- Migración de de Amazon RDS para Oracle a Amazon RDS para MySQL
- Migración de Couchbase Server a Couchbase Capella en AWS
- Migre de IBM Db2 en Amazon EC2 a Aurora compatible con PostgreSQL mediante AWS DMS y AWS SCT
- Migración de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante la vista materializada y AWS DMS
- Migre de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante AWS DMS SharePlex
- Migre de Oracle Database a Amazon RDS for PostgreSQL mediante Oracle GoldenGate
- Migración de Oracle en Amazon EC2 a Amazon RDS para MySQL con AWS DMS y AWS SCT
- Migre de PostgreSQL en EC2 Amazon a Amazon RDS para PostgreSQL mediante pglogical
- Migración de SAP ASE a Amazon RDS para SQL Server utilizando AWS DMS
- Migración de índices basados en funciones de Oracle a PostgreSQL
- Migración de aplicaciones heredadas de Oracle Pro*C a ECPG
- Migre una base de datos local de Microsoft SQL Server a Amazon EC2 mediante MGN
- Migración de cargas de trabajo de Cloudera en las instalaciones a la plataforma de datos de Cloudera en AWS
- Migre bases de datos MySQL locales a Aurora MySQL mediante Percona, XtraBackup Amazon EFS y Amazon S3
- Migración de Oracle Business Intelligence 12c a la nube de AWS desde servidores en las instalaciones
- Migración de valores CLOB de Oracle a filas individuales en PostgreSQL en AWS

- Migración de códigos de error de Oracle Database a una base de datos Amazon Aurora compatible con PostgreSQL
- Migración de tablas externas de Oracle a Amazon Aurora compatible con PostgreSQL
- Migración de las funciones nativas de Oracle a PostgreSQL mediante extensiones
- Migre Oracle PeopleSoft a Amazon RDS Custom
- Migración de la funcionalidad ROWIdentificador de Oracle a PostgreSQL en AWS
- Migración de los paquetes pragma SERIALLY_REUTILIZABLE de Oracle a PostgreSQL
- Migre SAP ASE de Amazon EC2 a Amazon Aurora compatible con PostgreSQL mediante AWS SCT y AWS DMS
- Migración de columnas generadas de forma virtual de Oracle a PostgreSQL
- Supervise ElastiCache los clústeres de Amazon para comprobar el cifrado en reposo
- Consulta de las tablas de Amazon DynamoDB con SQL mediante Amazon Athena
- Proteja y optimice el acceso de los usuarios a una base de datos de federación DB2 en AWS mediante contextos de confianza
- Configure una PeopleSoft arquitectura de alta disponibilidad en AWS
- Configure la funcionalidad UTL_FILE de Oracle en Aurora compatible con PostgreSQL
- Simplificación de las implementaciones de PostgreSQL en Amazon EKS mediante PGO
- Transfiera z/OS datos de Db2 a gran escala a Amazon S3 en archivos CSV
- Transportar bases de datos PostgreSQL entre dos instancias de base de datos de Amazon RDS utilizando pg_transport
- Validar los objetos de la base de datos después de migrar de Oracle a Amazon Aurora PostgreSQL

Almacenamiento y copia de seguridad

Temas

- Permitir a EC2 las instancias el acceso de escritura a los buckets de S3 en las cuentas de AMS
- Automatización de la ingesat del flujo de datos en una base de datos de Snowflake mediante Snowflake Snowpipe, Amazon S3, Amazon SNS y Amazon Data Firehose
- Cifrar automáticamente los volúmenes de Amazon EBS nuevos y existentes
- Realice copias de seguridad de los servidores Sun SPARC en el emulador Stromasys Charon-SSP del Nube de AWS
- Realice copias de seguridad y archive datos en Amazon S3 con Veeam Backup & Replication
- Copie datos de un bucket de Amazon S3 a otra cuenta o región mediante el AWS CLI
- Habilite el archivado de DB2 registros directamente en Amazon S3 en una base de datos IBM Db2
- Migre datos de un entorno Hadoop local a Amazon S3 con DistCp AWS PrivateLink para Amazon S3
- Más patrones

Permitir a EC2 las instancias el acceso de escritura a los buckets de S3 en las cuentas de AMS

Mansi Suratwala, Amazon Web Services

Resumen

AWS Managed Services (AMS) le ayuda a operar su AWS infraestructura de manera más eficiente y segura. Las cuentas AMS tienen barreras de seguridad para una administración estandarizada de sus AWS recursos. Una barrera es que los perfiles de instancia predeterminados de Amazon Elastic Compute Cloud EC2 (Amazon) no permiten el acceso de escritura a los buckets de Amazon Simple Storage Service (Amazon S3). Sin embargo, es posible que su organización tenga varios buckets de S3 y necesite un mayor control sobre el acceso por parte de las instancias. EC2 Por ejemplo, es posible que desee almacenar las copias de seguridad de las bases de datos de EC2 las instancias en un depósito de S3.

Este patrón explica cómo usar las solicitudes de cambio (RFCs) para permitir que tus EC2 instancias tengan acceso de escritura a los buckets de S3 de tu cuenta de AMS. Una RFC es una solicitud creada por el interesado o por AMS para realizar un cambio en el entorno administrado y que incluye un identificador de tipo de cambio (CT) para una operación concreta.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AMS Advanced. Para obtener más información al respecto, consulte los planes de operaciones de AMS en la documentación de AMS.
- Acceso al `customer-mc-user-role` rol AWS Identity and Access Management (IAM) que se va a enviar. RFCs
- AWS Command Line Interface (AWS CLI), instalado y configurado con las EC2 instancias de su cuenta AMS.
- Comprensión de cómo crear y enviar RFCs en AMS. Para más información, consulte What are AMS change types? (¿Qué son los tipos de cambio de AMS?) en la documentación de AMS.
- Comprensión de los tipos de cambios manuales y automatizados (CTs). Para obtener más información al respecto, consulte Automatizado y manual CTs en la documentación de AMS.

Arquitectura

Pila de tecnología

- AMS
- AWS CLI
- Amazon EC2
- Amazon S3
- IAM

Tools (Herramientas)

- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que te ayuda a interactuar Servicios de AWS mediante comandos en tu consola de línea de comandos.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Managed Services (AMS) le ayuda a operar su infraestructura de AWS de forma más eficiente y segura.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática escalable en el Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.

Epics

Creación de un bucket de S3 con una RFC

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3 mediante una RFC automatizada.	1. Inicie sesión en su cuenta de AMS, elija la página Elegir el tipo de cambio, elija y RFCs, a continuación, elija Crear RFC.	Administrador de sistemas de AWS, desarrollador de AWS

Tarea	Descripción	Habilidades requeridas
	2. Envíe la RFC automatizada Crear bucket de S3. **Note** Asegúrese de registrar el nombre del bucket de S3.	

Cree un perfil de instancia de IAM y asócielo a las instancias EC2

Tarea	Descripción	Habilidades requeridas
Envíe una RFC manual para crear un rol de IAM.	Cuando se incorpora una cuenta de AMS, se crea un perfil de instancia de IAM predeterminado denominado y `customer-mc-ec2-instance-profile` se asocia a cada EC2 instancia de su cuenta de AMS. Sin embargo, el perfil de instancia no tiene permisos de escritura en los buckets de S3. Para añadir los permisos de escritura, envíe la RFC manual Create IAM Resource (Crear recurso de IAM) para crear un rol de IAM que tenga las tres políticas `customer_ec2_instance_` , `customer_deny_policy`	Administrador de sistemas de AWS, desarrollador de AWS

Tarea	Descripción	Habilidades requeridas
	y `customer_ec2_s3_integration_policy` . **Important** Las políticas `customer_ec2_instance_` y `customer_deny_policy` ya existen en su cuenta de AMS. Sin embargo, debe crear `customer_ec2_s3_integration_policy` mediante el ejemplo de política siguiente: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "", "Effect": "Allow", "Principal": { "Service": "ec2.amazonaws.com" }, "Action": "sts:AssumeRole" } ]`	

Tarea	Descripción	Habilidades requeridas

	<pre>}
	
	Role Permissions:
	{
	     "Version":
	 "2012-10-17",
	     "Statement": [
	        {
	             "Action": [
	
	 "s3:ListBucket",
	
	 "s3:GetBucketLocat
	ion"
	           ],
	            "Resource
	": "arn:aws:s3:::",
	            "Effect":
	 "Allow"
	        },
	        {
	             "Action": [
	
	 "s3:GetObject",
	
	 "s3:PutObject",
	
	 "s3:ListMultipartU
	ploadParts",
	
	 "s3:AbortMultipart
	Upload"
	           ],
	            "Resource
	": "arn:aws:s3:::/*",
	            "Effect":
	 "Allow"
	        }
	    ]
	}</pre>	

Tarea	Descripción	Habilidades requeridas
Envíe una RFC manual para reemplazar el perfil de instancia de IAM.	Envíe una RFC manual para asociar las EC2 instancias de destino al nuevo perfil de instancia de IAM.	Administrador de sistemas de AWS, desarrollador de AWS
Pruebe una operación de copia en el bucket de S3.	Pruebe una operación de copia en el bucket de S3; para ello, ejecute el comando siguiente en la AWS CLI: `aws s3 cp test.txt s3://<S3 bucket>/test2.txt`	Administrador de sistemas de AWS, desarrollador de AWS

Recursos relacionados

- Cree un perfil de instancia de IAM para sus instancias de Amazon EC2
- Crear un bucket de S3 (mediante la consola Amazon S3 AWS SDKs, o AWS CLI)

Automatización de la ingesat del flujo de datos en una base de datos de Snowflake mediante Snowflake Snowpipe, Amazon S3, Amazon SNS y Amazon Data Firehose

Bikash Chandra Rout, Amazon Web Services

Resumen

Este patrón describe cómo puede utilizar los servicios de la nube de Amazon Web Services (AWS) para procesar un flujo continuo de datos y cargarlo en una base de datos de Snowflake. El patrón utiliza Amazon Data Firehose para entregar los datos a Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS), y así enviar notificaciones cuando se reciben nuevos datos. También utiliza Snowflake Snowpipe para cargar los datos en una base de datos de Snowflake.

Si sigue este patrón, podrá disponer de datos generados de forma continua para analizarlos en cuestión de segundos, evitando así múltiples comandos `COPY` manuales. También podrá conseguir un soporte completo para datos semiestructurados al cargarlos.

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- Un origen de datos que envía datos de forma continua a un flujo de entrega de Firehose.
- Un bucket de S3 existente que recibe los datos desde el flujo de entrega de Firehose.
- Una cuenta de Snowflake activa.

Limitaciones

- Snowflake Snowpipe no se conecta directamente a Firehose.

Arquitectura

Pila de tecnología

- Amazon Data Firehose

- Amazon SNS
- Amazon S3
- Snowflake Snowpipe
- Base de datos de Snowflake

Tools (Herramientas)

- Amazon Data Firehose es un servicio totalmente gestionado para entregar datos de streaming en tiempo real a destinos como Amazon S3, Amazon Redshift, OpenSearch Amazon Service, Splunk y cualquier punto de enlace HTTP personalizado o punto de enlace HTTP propiedad de proveedores de servicios externos compatibles.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet.
- Amazon Simple Notification Service (Amazon SNS) coordina y administra la entrega o el envío de mensajes a los puntos de enlace o clientes suscritos.
- Snowflake: Snowflake es un almacén de datos analíticos que se proporciona como (SaaS). Software-as-a-Service
- Snowflake Snowpipe: Snowpipe carga los datos de los archivos tan pronto como están disponibles en una etapa de Snowflake.

Epics

Configure Snowflake Snowpipe

Tarea	Descripción	Habilidades requeridas
Cree un archivo CSV en Snowflake.	Inicie sesión en Snowflake y ejecute el comando `CREATE FILE FORMAT` para crear un archivo CSV con un delimitador de campo específico. Para más información sobre este y otros comandos de Snowflake, consulte la sección Información adicional.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Cree una etapa de Snowflake externa.	Ejecute el comando `CREATE STAGE` para crear una etapa de Snowflake externa que haga referencia al archivo CSV que creó anteriormente. Importante: Necesitará la URL del bucket de S3, su clave de acceso y su clave de AWS acceso secreta. AWS Ejecute el comando `SHOW STAGES` para comprobar que se haya creado la etapa de Snowflake.	Desarrollador
Cree la tabla de destino de Snowflake.	Ejecute el comando `CREATE TABLE` para crear la tabla de Snowflake.	Desarrollador
Cree una canalización.	Ejecute el comando `CREATE PIPE` y asegúrese de que `auto_ingest=true` esté en el comando. Ejecute el comando `SHOW PIPES` para comprobar que se haya creado la canalización. Copie y guarde el valor de columna `notification_channel` . Este valor se utilizará para configurar las notificaciones de eventos de Amazon S3.	Desarrollador

Configure el bucket de S3

Tarea	Descripción	Habilidades requeridas
Cree una política de ciclo de vida de 30 días para el bucket de S3.	Inicie sesión en la consola Amazon S3 Consola de administración de AWS y ábrala. Seleccione el bucket de S3 que tiene los datos de Firehose. A continuación, seleccione la pestaña Administración en el bucket de S3 y elija Agregar regla de ciclo de vida. Escriba un nombre para la regla en el cuadro de diálogo Regla de ciclo de vida y configure una regla del ciclo de vida de 30 días para su bucket. Para obtener ayuda con esta y otras explicaciones, consulte la sección Recursos relacionados.	Administrador de sistemas, desarrollador
Cree una política de IAM para el bucket de S3.	Abra la consola AWS Identity and Access Management (IAM) y elija Políticas. Elija Crear política y, a continuación, elija la pestaña JSON. Copie y pegue la política de la sección Información adicional en el campo JSON. Esta política concederá los permisos `PutObject` y `DeleteObject`, así como los permisos `GetObject`, `GetObjectVersion` y	Administrador de sistemas, desarrollador

Tarea	Descripción	Habilidades requeridas
	`ListBucket` . Elija Revisar política, escriba un nombre para la política y después elija Crear política.	
Asigne la política a un rol de IAM.	Abra la consola de IAM, elija Roles y, a continuación, elija Crear rol. Elija Otra cuenta de AWS como entidad de confianza. Introduzca su Cuenta de AWS ID y seleccione Requerir ID externo. Introduzca un marcador de posición de ID que podrá cambiar más adelante. Elija Siguiente y asigne la política de IAM que creó anteriormente. Luego, cree el rol de IAM.	Administrador de sistemas, desarrollador
Copie el nombre de recurso de Amazon (ARN) para el rol de IAM.	Abra la consola de IAM; y elija Roles. Elija el rol de IAM que creó anteriormente y, a continuación, copie y almacene el ARN del rol.	Administrador de sistemas, desarrollador

Configure una integración de almacenamiento en Snowflake

Tarea	Descripción	Habilidades requeridas
Cree una integración de almacenamiento en Snowflake .	Inicie sesión en Snowflake y ejecute el comando `CREATE STORAGE INTEGRATION` . Esto modificará la relación de confianza, concederá acceso	Administrador de sistemas, desarrollador

Tarea	Descripción	Habilidades requeridas
	a Snowflake y proporcionará el ID externo de su etapa de Snowflake.	
Recupere el rol de IAM para su cuenta de Snowflake.	Ejecute el comando `DESC INTEGRATION` para recuperar el ARN del rol de IAM. **Important** `<integration_name>` es el nombre de la integración de almacenamiento de Snowflake que creó anteriormente.	Administrador de sistemas, desarrollador
Registre los valores de dos columnas.	Copie y guarde los valores de las columnas `storage_aws_iam_user_arn` y `storage_aws_external_id` .	Administrador de sistemas, desarrollador

Permita que Snowflake Snowpipe acceda al bucket de S3

Tarea	Descripción	Habilidades requeridas
Modifique la política del rol de IAM.	Abra la consola de IAM; y elija Roles. Elija el rol de IAM que creó anteriorm ente y seleccione la pestaña Relaciones de confianza. Elija Editar relación de confianza	Administrador de sistemas, desarrollador

Tarea	Descripción	Habilidades requeridas
	. Reemplace `snowflake_external_id` por el valor `storage_aws_external_id` que copió anteriormente. Reemplace `snowflake_user_arn` por el valor `storage_aws_iam_user_arn` que copió anteriormente. A continuación, seleccione Actualizar la política de confianza.	

Active y configure las notificaciones de SNS para el bucket de S3

Tarea	Descripción	Habilidades requeridas
Active las notificaciones de eventos para el bucket de S3.	Abra la consola de Amazon S3 y elija un bucket. Seleccione Propiedades y, en Configuración avanzada, seleccione Eventos. Seleccione Añadir notificación y especifique un nombre para este evento. Si no introduce un nombre, se generará un identificador único global (GUID) y se utilizará para el nombre.	Administrador de sistemas, desarrollador
Configure las notificaciones de Amazon SNS para el bucket de S3.	En Eventos, elija ObjectCreate (Todos) y, a continuación, elija SQS Queue en la lista desplegable Enviar a. En la lista de SNS, elija Agregar ARN de cola SQS y	Administrador de sistemas, desarrollador

Tarea	Descripción	Habilidades requeridas
	pegue el valor `notification_channel` que copió anteriormente. A continuación, elija Guardar.	
Suscriba la cola de SQS de Snowflake al tema de SNS.	Suscriba la cola de SQS de Snowflake al tema de SNS que ha creado. Para obtener más información sobre este paso, consulte la sección Recursos relacionados.	Administrador de sistemas, desarrollador

Compruebe la integración de la etapa de Snowflake

Tarea	Descripción	Habilidades requeridas
Revise y pruebe Snowpipe.	Inicie sesión en Snowflake y abra la etapa de Snowflake . Coloque los archivos en su bucket de S3 y compruebe si la tabla Snowflake los carga. Amazon S3 enviará notificaciones de SNS a Snowpipe cuando aparezcan nuevos objetos en el bucket de S3.	Administrador de sistemas, desarrollador

Recursos relacionados

- Administración del ciclo de vida del almacenamiento
- Suscriba la cola de SQS de Snowflake al tema de Amazon SNS

Información adicional

Crear un formato de archivo:

```
CREATE FILE FORMAT <name>
TYPE = 'CSV'
FIELD_DELIMITER = '|'
SKIP_HEADER = 1;
```

Crear una etapa externa:

```
externalStageParams (for Amazon S3) ::=
  URL = 's3://[//]'

  [ { STORAGE_INTEGRATION =  } | { CREDENTIALS = ( {  { AWS_KEY_ID = `` AWS_SECRET_KEY
 = `` [ AWS_TOKEN = `` ] } | AWS_ROLE = ``  } ) ) }` ]
  [ ENCRYPTION = ( [ TYPE = 'AWS_CSE' ] [ MASTER_KEY = '' ] |
                   [ TYPE = 'AWS_SSE_S3' ] |
                   [ TYPE = 'AWS_SSE_KMS' [ KMS_KEY_ID = '' ] |
                   [ TYPE = NONE ] )
```

Creación de una tabla:

```
CREATE [ OR REPLACE ] [ { [ LOCAL | GLOBAL ] TEMP[ORARY] | VOLATILE } | TRANSIENT ]
 TABLE [ IF NOT EXISTS ]
  <table_name>
    ( <col_name> <col_type> [ { DEFAULT <expr>
                                | { AUTOINCREMENT | IDENTITY } [ ( <start_num> ,
 <step_num> ) | START <num> INCREMENT <num> ] } ]
                                 /* AUTOINCREMENT / IDENTITY supported only for numeric
 data types (NUMBER, INT, etc.) */
                             [ inlineConstraint ]
     [ , <col_name> <col_type> ... ]
     [ , outoflineConstraint ]
     [ , ... ] )
  [ CLUSTER BY ( <expr> [ , <expr> , ... ] ) ]
  [ STAGE_FILE_FORMAT = ( { FORMAT_NAME = '<file_format_name>'
                           | TYPE = { CSV | JSON | AVRO | ORC | PARQUET | XML }
 [ formatTypeOptions ] } ) ]
  [ STAGE_COPY_OPTIONS = ( copyOptions ) ]
  [ DATA_RETENTION_TIME_IN_DAYS = <num> ]
  [ COPY GRANTS ]
  [ COMMENT = '<string_literal>' ]
```

Mostrar etapas:

```
SHOW STAGES;
```

Creación de una canalización:

```
CREATE [ OR REPLACE ] PIPE [ IF NOT EXISTS ]
  [ AUTO_INGEST = [ TRUE | FALSE ] ]
  [ AWS_SNS_TOPIC =  ]
  [ INTEGRATION = '' ]
  [ COMMENT = '' ]
  AS
```

Mostrar canalizaciones:

```
SHOW PIPES [ LIKE '<pattern>' ]
           [ IN { ACCOUNT | [ DATABASE ] <db_name> | [ SCHEMA ] <schema_name> } ]
```

Crear una integración de almacenamiento:

```
CREATE STORAGE INTEGRATION <integration_name>
  TYPE = EXTERNAL_STAGE
  STORAGE_PROVIDER = S3
  ENABLED = TRUE
  STORAGE_AWS_ROLE_ARN = '<iam_role>'
  STORAGE_ALLOWED_LOCATIONS = ('s3://<bucket>/<path>/', 's3://<bucket>/<path>/')
  [ STORAGE_BLOCKED_LOCATIONS = ('s3://<bucket>/<path>/', 's3://<bucket>/<path>/') ]
```

Ejemplo:

```
create storage integration s3_int
  type = external_stage
  storage_provider = s3
  enabled = true
  storage_aws_role_arn = 'arn:aws:iam::001234567890:role/myrole'
  storage_allowed_locations = ('s3://amzn-s3-demo-bucket1/mypath1/', 's3://amzn-s3-
demo-bucket2/mypath2/')
  storage_blocked_locations = ('s3://amzn-s3-demo-bucket1/mypath1/sensitivedata/',
 's3://amzn-s3-demo-bucket2/mypath2/sensitivedata/');
```

Para obtener más información sobre este paso, consulte Configuración de una integración de almacenamiento de Snowflake para acceder a Amazon S3 en la documentación de Snowflake.

Describir una integración:

```
DESC INTEGRATION <integration_name>;
```

Política de bucket de S3:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetObjectVersion",
              "s3:DeleteObject",
              "s3:DeleteObjectVersion"
            ],
            "Resource": "arn:aws:s3:::/*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::",
            "Condition": {
                "StringLike": {
                    "s3:prefix": [
                        "/*"
                    ]
                }
            }
        }
    ]
}
```

Cifrar automáticamente los volúmenes de Amazon EBS nuevos y existentes

Tony DeMarco y Josh Joy, Amazon Web Services

Resumen

El cifrado de volúmenes de Amazon Elastic Block Store (Amazon EBS) es importante para la estrategia de protección de datos de una organización. Es un paso importante para establecer un entorno bien diseñado. Aunque no hay forma directa de cifrar un volumen o una instantánea existente sin cifrar, puede cifrarlos mediante la creación de un volumen o una instantánea. Para obtener más información, consulte Cifrar los recursos de EBS en la documentación de Amazon EC2 . Este patrón proporciona controles preventivos y de detección para cifrar los volúmenes de EBS, tanto nuevos como existentes. En este patrón, configura los ajustes de la cuenta, crea procesos de corrección automatizados e implementa controles de acceso.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada en macOS, Linux o Windows.
- jq instalado y configurado en macOS, Linux o Windows.
- Los permisos de AWS Identity and Access Management (IAM) se proporcionan para tener acceso de lectura y escritura a AWS, CloudFormation Amazon Elastic Compute Cloud (Amazon EC2), AWS Systems Manager, AWS Config y AWS Key Management Service (AWS KMS)
- AWS Organizations está configurado con todas las características habilitadas, un requisito para las políticas de control de servicios.
- AWS Config está habilitado en las cuentas de destino.

Limitaciones

- En su cuenta de AWS de destino, no debe haber reglas de AWS Config denominadas encrypted-volumes. Esta solución implementa una regla con este nombre. Las reglas preexistentes con este nombre pueden provocar un error en la implementación y generar cargos innecesarios relacionados con el procesamiento de la misma regla más de una vez.
- Esta solución cifra todos los volúmenes de EBS con la misma clave de AWS KMS.

- Si habilita el cifrado de los volúmenes de EBS de la cuenta, esta configuración es específica de la región. Si lo habilita para una región de AWS, puede deshabilitarlo para volúmenes o instantáneas individuales en esa región. Para obtener más información, consulta Cifrado por defecto en la EC2 documentación de Amazon.
- Cuando corrija los volúmenes de EBS no cifrados existentes, asegúrese de que la EC2 instancia no esté en uso. Esta automatización cierra la instancia para separar el volumen no cifrado y adjuntar el cifrado. Se produce un tiempo de inactividad mientras se lleva a cabo la corrección. Si se trata de una parte fundamental de la infraestructura para su organización, asegúrese de contar con configuraciones manuales o automáticas de alta disponibilidad para no afectar la disponibilidad de las aplicaciones que se estén ejecutando en la instancia. Le recomendamos que corrija los recursos críticos solo durante los períodos de mantenimiento estándar.

Arquitectura

Flujo de trabajo de automatización

1. AWS Config detecta un volumen de EBS sin cifrar.
2. Un administrador usa AWS Config para enviar un comando de corrección a Systems Manager.
3. La automatización de Systems Manager toma una instantánea del volumen de EBS no cifrado.
4. La automatización de Systems Manager utiliza AWS KMS para crear una copia cifrada de la instantánea.
5. La automatización de Systems Manager hace lo siguiente:
   a. Detiene la EC2 instancia afectada si está en ejecución
   b. Adjunta la nueva copia cifrada del volumen a la instancia EC2
   c. Devuelve la EC2 instancia a su estado original

Tools (Herramientas)

Servicios de AWS

- AWS CLI: la interfaz de línea de comandos de AWS (AWS CLI) proporciona acceso directo a las interfaces públicas de programación de aplicaciones APIs () de los servicios de AWS. Puede explorar las capacidades de un servicio con la CLI de AWS y desarrollar scripts de shell para administrar los recursos. Además de los comandos equivalentes de la API de bajo nivel, varios

servicios de AWS ofrecen personalizaciones para la CLI de AWS. Las personalizaciones pueden incluir comandos de un nivel superior que simplifican el uso de un servicio con una API compleja.

- AWS CloudFormation: AWS CloudFormation es un servicio que le ayuda a modelar y configurar sus recursos de AWS. Crea una plantilla que describe todos los recursos de AWS que desea (como las EC2 instancias de Amazon) y CloudFormation aprovisiona y configura esos recursos por usted.
- AWS Config: AWS Config proporciona una visión detallada de la configuración de los recursos de AWS de su cuenta de AWS. Esto incluye cómo se relacionan los recursos entre sí y cómo se han configurado en el pasado, para que pueda ver cómo las configuraciones y las relaciones cambian a lo largo del tiempo.
- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona una capacidad informática de tamaño variable que se utiliza para crear y alojar los sistemas de software.
- AWS KMS: AWS Key Management Service (AWS KMS) es un servicio de cifrado y administración de claves escalado para la nube. Otros servicios de AWS utilizan las claves y la funcionalidad de AWS KMS, y usted puede utilizarlas para proteger los datos de su entorno de AWS.
- AWS Organizations: AWS Organizations es un servicio de administración de cuentas que le permite unificar varias cuentas de AWS en una organización que crea y administra de forma centralizada.
- AWS Systems Manager Automation: Systems Manager Automation simplifica las tareas habituales de mantenimiento e implementación de las EC2 instancias de Amazon y otros recursos de AWS.

Otros servicios

- jq: jq es un procesador JSON de línea de comandos ligero y flexible. Esta herramienta se utiliza para extraer información clave de la salida de la CLI de AWS.

Código

- El código de este patrón está disponible en el repositorio Cómo corregir GitHub automáticamente los volúmenes de EBS no cifrados mediante claves KMS del cliente.

Epics

Automatizar la corrección de volúmenes no cifrados

Tarea	Descripción	Habilidades requeridas
Descargue scripts y plantillas. CloudFormation	Descargue el script de shell, el archivo JSON y CloudFormation las plantillas del repositorio Remediar GitHub automáticamente volúmenes de EBS no cifrados mediante claves KMS del cliente.	Administrador de AWS, AWS general
Identifique al administrador de la clave de AWS KMS.	1. Inicie sesión en la consola de administración de AWS y abra la consola de IAM en https://console.aws.amazon.com/iam/. 2. Identifique un usuario o rol que será el administrador de clave de AWS KMS. Si es necesario crear un nuevo usuario o rol para este propósito, créelo ahora. Para obtener más información, consulte Identidades de IAM en la documentación de IAM. Esta automatización crea una nueva clave de AWS KMS. 3. Una vez identificado, copie el nombre de recurso de Amazon (ARN) del usuario o rol. Para obtener más información, consulte IAM	Administrador de AWS, AWS general

Tarea	Descripción	Habilidades requeridas
	ARNs en la documentación de IAM. Utilizará este ARN en el siguiente paso.	

Tarea	Descripción	Habilidades requeridas
Implemente la plantilla Stack1 CloudFormation .	1. Abra la CloudFormation consola de AWS en https://console.aws.amazon.com/cloudformation/. 2. En CloudFormation, implemente la `Stack1.yaml` plantilla. Tenga en cuenta los siguientes detalles de implementación: • Proporcione a la pila un nombre claro y descriptivo. Tenga en cuenta el nombre de pila porque necesita este valor en el siguiente paso. • Pegue el ARN del administrador de clave en el único campo de parámetro de Stack1. Este usuario o rol se convierte en el administrador de la clave de AWS KMS creada por la pila. Para obtener más información sobre la implementación de una CloudFormation plantilla, consulte Trabajar con CloudFormation plantillas de AWS en la CloudFormation documentación.	Administrador de AWS, AWS general

Tarea	Descripción	Habilidades requeridas
Implemente la plantilla Stack2 CloudFormation .	En CloudFormation, despliega la `Stack2.yaml` plantilla. Tenga en cuenta los siguientes detalles de implementación: • Proporcione a la pila un nombre claro y descriptivo. • Para el único parámetro de Stack2, introduzca el nombre de la pila que creó en el paso anterior. Esto permite a Stack2 hacer referencia a la nueva clave y rol de AWS KMS implementados por la pila en el paso anterior.	Administrador de AWS, AWS general
Cree un volumen sin cifrar para realizar pruebas.	Cree una EC2 instancia con un volumen de EBS sin cifrar. Para obtener instrucciones, consulte Crear un volumen de Amazon EBS en la EC2 documentación de Amazon. El tipo de instancia no importa y no es necesario acceder a la instancia. Puede crear una instancia t2.micro para permanecer en el nivel gratuito y no necesita crear un par de claves.	Administrador de AWS, AWS general

Tarea	Descripción	Habilidades requeridas
Pruebe la regla de AWS Config.	1. Abra la consola de AWS Config en https://console.aws.amazon.com/config/. En la página Reglas, seleccione la regla encrypted-volumes. 2. Confirme que la nueva instancia de prueba sin cifrar aparezca en la lista de recursos no conformes. Si el volumen no aparece inmediatamente, espere unos minutos y actualice los resultados. La regla AWS Config detecta los cambios en los recursos poco después de crear la instancia y el volumen. 3. Seleccione el recurso y, a continuación, seleccione Corregir. Puede ver el progreso y el estado de la corrección en Systems Manager de la siguiente manera: 1. Abra la consola de AWS Systems Manager en https://console.aws.amazon.com/systems-manager/. 2. En el panel de navegación, elija automatización.	Administrador de AWS, AWS general

Tarea	Descripción	Habilidades requeridas
	3. Seleccione el enlace ID de ejecución para ver los pasos y el estado.	
Configure cuentas o regiones de AWS adicionales.	Según sea necesario para su caso de uso, repita esta epopeya para cualquier otra cuenta o región de AWS.	Administrador de AWS, AWS general

Habilitar el cifrado a nivel de cuenta de los volúmenes de EBS

Tarea	Descripción	Habilidades requeridas
Ejecute el script de habilitación.	1. En un shell de bash, use el comando `cd` para navegar hasta el repositorio clonado. 2. Ingrese el comando siguiente para ejecutar el script `enable-ebs-encryption-for-account` . `./Bash/enable-ebs-encryption-for-account.sh`	Administrador de AWS, AWS general, bash
Confirme si la configuración está actualizada.	1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/. 2. En la parte derecha de la pantalla, en Configuración, seleccione Protección y seguridad de datos.	Administrador de AWS, AWS general

Tarea	Descripción	Habilidades requeridas
	3. En la sección Cifrado de EBS, confirme que Cifrar siempre los volúmenes nuevos de EBS está activada y si la opción Clave de cifrado predeterminada está configurada en el ARN que especificó anteriormente. **Note** Si la configuración Encriptar siempre los nuevos volúmenes de EBS está desactivada o la clave sigue configurada alias/aws/ebs, confirme que ha iniciado sesión en la misma cuenta y región de AWS en la que ejecutó el script de shell y compruebe si hay mensajes de error en el shell.	
Configure cuentas o regiones de AWS adicionales.	Según sea necesario para su caso de uso, repita esta epopeya para cualquier otra cuenta o región de AWS.	Administrador de AWS, AWS general

Impedir la creación de instancias no cifradas

Tarea	Descripción	Habilidades requeridas
Cree una política de control de servicios.	1. Abra la consola de AWS Organizations en la https://console.aws.amazon.com/organizations/v2/. 2. Cree una nueva política de control de servicios. Para obtener más información, consulte Creación, actualización y eliminación de políticas de control de servicios en la documentación de AWS Organizations. 3. Añada el contenido de `DenyUnencryptedEC2.json` a la política y guárdelo. En la primera epopeya, descargó este archivo JSON del GitHub repositorio. 4. Adjunta esta política a la raíz de la organización o a cualquier unidad organizativa necesaria (OUs). Para obtener más información, consulte Asociar y desasociar políticas de control de servicios en la documentación de AWS Organizations.	Administrador de AWS, AWS general

Recursos relacionados

Documentación de servicio de AWS

- CLI de AWS
- AWS Config
- AWS CloudFormation
- Amazon EC2
- AWS KMS
- AWS Organizations
- Automatización de AWS Systems Manager

Otros recursos

- jq manual (sitio web de jq)
- jq download () GitHub

Realice copias de seguridad de los servidores Sun SPARC en el emulador Stromasys Charon-SSP del Nube de AWS

Kevin Yung y Rohit Darji, Amazon Web Services

Luis Ramos, Stromasys

Resumen

Este patrón ofrece cuatro opciones para realizar copias de seguridad de los servidores SPARC de Sun Microsystems tras una migración de un entorno local a la nube de Amazon Web Services ()AWS. Estas opciones de copia de seguridad lo ayudan a implementar un plan de copia de seguridad que cumpla con el objetivo de punto de recuperación (RPO) y el objetivo de tiempo de recuperación (RTO) de su organización, utilice enfoques automatizados y reduzca sus costos operativos generales. El patrón proporciona una descripción general de las cuatro opciones de copia de seguridad y los pasos para implementarlas.

Si utiliza un servidor Sun SPARC alojado como huésped en un emulador Charon-SSP de Stromasys, puede utilizar una de las tres opciones de copia de seguridad siguientes:

- Opción de copia de seguridad 1: cinta virtual Stromasys: utilice la función de cinta virtual Charon-SSP para configurar una instalación de copia de seguridad en el servidor Sun SPARC y archivar los archivos de copia de seguridad en Amazon Simple Storage Service (Amazon S3) mediante la automatización.AWS Systems Manager
- Opción de copia de seguridad 2: instantánea de Stromasys: utilice la característica de instantáneas de Charon-SSP para configurar una función de copia de seguridad para los servidores invitados Sun SPARC en Charon-SSP.
- Opción de copia de seguridad 3: instantánea del volumen de Amazon Elastic Block Store (Amazon EBS): si aloja el emulador Charon-SSP en Amazon Elastic Compute Cloud (Amazon EC2), puede utilizar una instantánea de volumen de Amazon EBS para crear copias de seguridad para un sistema de archivos Sun SPARC.

Si utiliza un servidor Sun SPARC alojado como huésped en un emulador Charon-SSP en Amazon EC2, puede utilizar la opción de copia de seguridad siguiente:

- Opción de respaldo 4: biblioteca de cintas AWS Storage Gateway virtuales (VTL): utilice una aplicación de respaldo con un Storage Gateway VTL Tape Gateway para realizar copias de seguridad de los servidores Sun SPARC.

Si utiliza un servidor Sun SPARC alojado como una zona de marca en un servidor Sun SPARC, puede utilizar las opciones de copia de seguridad 1, 2 y 4.

Stromasys proporciona software y servicios para emular los sistemas críticos antiguos SPARC, Alpha, VAX y PA-RISC. Para obtener más información sobre cómo migrar a la emulación de Stromasys, consulte Realojar SPARC, Alpha u otros sistemas heredados Nube de AWS con Stromasys en el blog. AWS AWS

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- Servidores Sun SPARC existentes.
- Licencias para Charon-SSP existentes. Las licencias para Charon-SSP están disponibles en Stromasys AWS Marketplace y las licencias para el entorno virtual (VE) de Stromasys están disponibles en Stromasys. Para obtener más información, póngase en contacto con el departamento de ventas de Stromasys.
- Familiaridad con los servidores Sun SPARC y las copias de seguridad de Linux.
- Familiaridad con la tecnología de emulación Charon-SSP. Para obtener más información al respecto, consulte la emulación de servidores antiguos de Stromasys en la documentación de Stromasys.
- Si desea utilizar la función de cinta virtual o las aplicaciones de copia de seguridad para los sistemas de archivos de sus servidores Sun SPARC, debe crear y configurar las instalaciones de copia de seguridad para el sistema de archivos del servidor Sun SPARC.
- Comprensión del RPO y el RTO. Para obtener más información al respecto, consulte los objetivos de recuperación ante desastres del documento técnico sobre el pilar de la confiabilidad en la documentación de Well-Architected Framework AWS .
- Para usar la opción 4 de copia de seguridad, debe tener lo siguiente:
  - Aplicación de backup basada en software que admite una Puerta de enlace de cinta Storage Gateway VTL. Para obtener más información al respecto, consulte Trabajar con dispositivos VTL en la documentación. AWS Storage Gateway
  - Bacula Director o una aplicación de copia de seguridad similar, instalada y configurada. Para obtener información, consulte la documentación de Bacula Director.

En la siguiente tabla se proporciona información sobre las cuatro opciones de copia de seguridad de este patrón.

Opciones de copia de seguridad	¿Es coherente ante bloqueos?	¿Es coherente en cuanto a las aplicaciones?	¿Solución de dispositivo de copia de seguridad virtual?	Casos de uso típicos
Opción 1: cinta virtual Stromasys	Sí Puede automatizar las instantáneas del sistema de archivos Sun SPARC para hacer copias de seguridad de los datos en una cinta virtual. Por ejemplo, puede utilizar instantáneas de UFS o ZFS.	Sí Esta opción de copia de seguridad requiere un script automatizado para vaciar las transacciones en curso, configurar un modo sin conexión temporal o de solo lectura durante la instantánea del sistema de archivos o realizar un volcado de datos de la aplicación. Es posible que también necesite tiempo de inactividad de la aplicación o modo de solo lectura.	Sí	Realice copias de seguridad de los sistemas de archivos del servidor Sun SPARC con archivos .tar o .zip Copia de seguridad de los datos de la aplicación

Opción 2: instantánea de Stromasys	Sí Debe configurar el Administrador Charon-SSP o utilizar un argumento de startup desde la línea de comandos para habilitar esta característica. También debe ejecutar un comando de Linux para solicitar al emulador Charon-SSP que guarde el estado del servidor invitado Sun SPARC en un archivo de instantánea. ⚠ Important Debe apagar el servidor invitado Sun SPARC.	Sí Esta opción de copia de seguridad crea una instantánea del servidor invitado emulado, incluidos sus discos virtuales y su volcado de memoria. ⚠ Important Debe apagar el servidor invitado Sun SPARC durante la instantánea.	No	Instantánea del servidor Sun SPARC Copia de seguridad de los datos de la aplicación

Opción 3: instantánea de volumen de Amazon EBS	Sí Puede utilizarla AWS Backup para automatizar la instantánea de Amazon EBS.	Sí Esta opción de copia de seguridad requiere un script automatizado para vaciar las transacciones en curso y configurar una parada temporal o de solo lectura de la instancia de Amazon EC2 durante la instantánea del volumen de Amazon EBS. **Important** Esta opción de copia de seguridad puede requerir un tiempo de inactividad de la aplicación o un modo	No	Instantánea de los sistemas de archivos del servidor Sun SPARC Copia de seguridad de los datos de la aplicación

de solo lectura para lograr la coherencia de la aplicación.

AWS Storage Gateway Opción 4: VTL	Sí Puede realizar automáticamente una copia de seguridad de los datos de copia de seguridad del sistema de archivos Sun SPARC en la VTL mediante un agente de copia de seguridad.	Sí Esta opción de copia de seguridad requiere un script automatizado para vaciar las transacciones en curso, configurar un modo sin conexión temporal o de solo lectura durante la instantánea del sistema de archivos o realizar un volcado de datos de la aplicación. **Important** Esta opción de copia de seguridad puede requerir un tiempo de inactividad de la aplicació	Sí	Una amplia flota de copias de seguridad del sistema de archivos del servidor Sun SPARC Copia de seguridad de los datos de la aplicación

n o un modo de solo lectura.

Limitaciones

- Puede utilizar los enfoques de este patrón para hacer copias de seguridad de servidores Sun SPARC individuales, pero también puede utilizar estas opciones de copia de seguridad para datos compartidos si tiene aplicaciones que se ejecutan en un clúster.

Tools (Herramientas)

Opción de copia de seguridad 1: cinta virtual Stromasys

- El emulador Charon-SSP de Stromasys crea la réplica virtual del hardware SPARC original dentro de un sistema informático estándar de 64 bits compatible con x86. Ejecuta el código binario SPARC original, incluidos los sistemas operativos (OSs) como SunOS o Solaris, sus productos en capas y sus aplicaciones.
- Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona una capacidad informática de tamaño variable que se utiliza para crear y alojar los sistemas de software.
- Amazon Elastic File System (Amazon EFS) proporciona un sistema de archivos set-and-forget elástico, simple Servicios de AWS y sin servidor para su uso con recursos locales.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet.
- AWS Systems Manager La automatización simplifica las tareas comunes de mantenimiento e implementación de las instancias de Amazon EC2 y AWS otros recursos.

Opción de copia de seguridad 2: instantánea de Stromasys

- El emulador Charon-SSP de Stromasys crea la réplica virtual del hardware SPARC original dentro de un sistema informático estándar de 64 bits compatible con x86. Ejecuta el código binario SPARC original, incluidos SunOS o Solaris, OSs sus productos en capas y sus aplicaciones.

- Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona una capacidad informática de tamaño variable que se utiliza para crear y alojar los sistemas de software.
- Amazon Elastic File System (Amazon EFS) proporciona un sistema de archivos set-and-forget elástico, simple Servicios de AWS y sin servidor para su uso con recursos locales.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet.
- AWS Systems Manager La automatización simplifica las tareas comunes de mantenimiento e implementación de las instancias de Amazon EC2 y AWS otros recursos.

Opción de backup 3: instantánea del volumen de Amazon EBS

- El emulador Stromasys Charon-SSP crea la réplica virtual del hardware SPARC original en un sistema informático estándar de 64 bits compatible con x86. Ejecuta el código binario SPARC original, incluidos SunOS o Solaris, OSs sus productos en capas y sus aplicaciones.
- AWS Backupes un servicio de protección de datos totalmente gestionado que facilita la centralización y la automatización Servicios de AWS, tanto en la nube como en las instalaciones.
- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento a nivel de bloque para su uso con las instancias de Amazon EC2.
- Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona una capacidad informática de tamaño variable que se utiliza para crear y alojar los sistemas de software.

Opción de backup 4: AWS Storage GatewayVTL

- El emulador Charon-SSP de Stromasys crea la réplica virtual del hardware SPARC original dentro de un sistema informático estándar de 64 bits compatible con x86. Ejecuta el código binario SPARC original, incluidos SunOS o Solaris, OSs sus productos en capas y sus aplicaciones.
- Bacula es un sistema de copia de seguridad informática de código abierto y de nivel empresarial. Para obtener más información sobre si su aplicación de respaldo actual es compatible con Tape Gateway, consulte Aplicaciones de respaldo de terceros compatibles con Tape Gateway en la documentación. AWS Storage Gateway
- Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona una capacidad informática de tamaño variable que se utiliza para crear y alojar los sistemas de software.

- Amazon Relational Database Service (Amazon RDS) para MySQL admite instancias de base de datos que ejecutan varias versiones de MySQL.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet.
- AWS Storage Gatewayconecta un dispositivo de software local con un almacenamiento en la nube para proporcionar una integración perfecta con las funciones de seguridad de datos entre el entorno de TI local y la infraestructura de almacenamiento. AWS

Epics

Opción de copia de seguridad 1: crear una copia de seguridad en cinta virtual de Stromasys

Tarea	Descripción	Habilidades requeridas
Cree un sistema de archivos compartidos Amazon EFS para el almacenamiento de archivos en cinta virtual.	Inicie sesión Consola de administración de AWS o utilice AWS Command Line Interface (AWS CLI) para crear un sistema de archivos Amazon EFS. Para obtener más información, consulte Crear un sistema de archivos de Amazon EFS en la documentación de Amazon EFS.	Arquitecto de la nube
Configure el host Linux para montar el sistema de archivos compartidos.	Instale el controlador Amazon EFS en la instancia Linux Amazon EC2 y configure el sistema operativo Linux para montar el sistema de archivos compartidos Amazon EFS durante el startup. Para obtener más información al respecto, consulte Montaje de sistemas de archivos	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	mediante el asistente de montaje de Amazon EFS en la documentación de Amazon EFS.	
Instale el emulador Charon-SSP.	Instale el emulador Charon-SSP en la instancia Linux de Amazon EC2. Para obtener más información al respecto, consulte Configuración de una Nube de AWS instancia para Charon-SSP en la documentación de Stromasys.	DevOps ingeniero
Cree un contenedor de archivos de cinta virtual en el sistema de archivos compartido para cada servidor huésped Sun SPARC.	Ejecute el comando `touch <vtape-container-name>` para crear un contenedor de archivos de cinta virtual en el sistema de archivos compartido para cada servidor huésped Sun SPARC implementado en el emulador Charon-SSP.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Configure Charon-SSP Manager para crear dispositivos de cinta virtuales para los servidores invitados SPARC de Sun.	Inicie sesión en Charon-SSP Manager, cree dispositivos de cinta virtuales y configúrelos para que utilicen los archivos contenedores de cintas virtuales de cada servidor huésped Sun SPARC. Para obtener más información al respecto, consulte la guía del usuario de Charon-SSP 5.2 para Linux en la documentación de Stromasys.	DevOps ingeniero
Valide que el dispositivo de cinta virtual esté disponible en los servidores invitados Sun SPARC.	Inicie sesión en cada servidor huésped Sun SPARC y ejecute el comando `mt -f /dev/rmt/1` para validar que el dispositivo de cinta virtual esté configurado en el sistema operativo.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Cree un manual de procedimientos de Systems Manager Automation.	Desarrolle el manual de procedimientos de automatización de Systems Manager y configure ventanas y asociaciones de mantenimiento en Systems Manager para programar el proceso de copia de seguridad. Para obtener más información al respecto, consulte Tutoriales de automatización y Configuración de ventanas de mantenimiento en la AWS Systems Manager documentación.	Arquitecto de la nube
Configure Systems Manager Automation para archivar los archivos de contenedores de cintas virtuales rotados.	Utilice el ejemplo de código de la opción Back 1 de la sección Información adicional para desarrollar un manual de automatización de Systems Manager para archivar los archivos de contenedores de cintas virtuales rotados en Amazon S3.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Implemente el manual de procedimientos de automatización de Systems Manager para archivar y programar.	Implemente el manual de procedimientos de automatización de Systems Manager y prográmelo para que se ejecute automáticamente en Systems Manager. Para obtener más información, consulte Configuración de la automatización en la documentación de Systems Manager.	Arquitecto de la nube

Opción de copia de seguridad 2: crear una instantánea de Stromasys

Tarea	Descripción	Habilidades requeridas
Cree un sistema de archivos compartidos Amazon EFS para el almacenamiento de archivos en cinta virtual.	Inicie sesión Consola de administración de AWS o utilice el AWS CLI para crear un sistema de archivos Amazon EFS. Para obtener más información, consulte Crear un sistema de archivos de Amazon EFS en la documentación de Amazon EFS.	Arquitecto de la nube
Configure el host Linux para montar el sistema de archivos compartidos.	Instale el controlador Amazon EFS en la instancia Linux Amazon EC2 y configure el sistema operativo Linux para montar el sistema de archivos	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	compartidos Amazon EFS durante el inicio. Para obtener más información al respecto, consulte Montaje de sistemas de archivos mediante el asistente de montaje de Amazon EFS en la documentación de Amazon EFS.	
Instale el emulador Charon-SSP.	Instale el emulador Charon-SSP en la instancia Linux de Amazon EC2. Para obtener más información al respecto, consulte Configuración de una Nube de AWS instancia para Charon-SSP en la documentación de Stromasys.	DevOps ingeniero
Configure los servidores invitados SPARC de Sun para que se inicien con la opción de instantánea.	Utilice el administrador Charon-SSP para configurar la opción de instantáneas para cada servidor huésped Sun SPARC. Para obtener más información al respecto, consulte la guía del usuario de Charon-SSP 5.2 para Linux en la documentación de Stromasys.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Cree un manual de procedimientos de Systems Manager Automation.	Utilice el ejemplo de código de la Opción de copia de seguridad 2 de la sección Información adicional para desarrollar un manual de procedimientos de automatización de Systems Manager para ejecutar de forma remota el comando snapshot en un servidor huésped Sun SPARC durante un período de mantenimiento.	Arquitecto de la nube
Implemente el manual de procedimientos de automatización de Systems Manager y configure la asociación a los hosts Linux de Amazon EC2.	Desarrolle el manual de procedimientos de automatización de Systems Manager y configure ventanas y asociaciones de mantenimiento en Systems Manager para programar el proceso de copia de seguridad. Para obtener más información al respecto, consulte los tutoriales de automatización y la configuración de las ventanas de mantenimiento en la AWS Systems Manager documentación.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Archive las instantáneas en un almacenamiento a largo plazo.	Utilice el código de ejemplo del manual de la sección de información adicional para desarrollar un manual de automatización de Systems Manager para archivar archivos de instantáneas en Amazon S3.	Arquitecto de la nube

Opción de copia de seguridad 3: crear una instantánea de volumen de Amazon EBS

Tarea	Descripción	Habilidades requeridas
Instale el emulador Charon-SSP.	Instale el emulador Charon-SSP en la instancia Linux de Amazon EC2. Para obtener más información al respecto, consulte Configuración de una Nube de AWS instancia para Charon-SSP en la documentación de Stromasys.	DevOps ingeniero
Cree volúmenes de Amazon EBS para los servidores invitados de Sun SPRAC.	Inicie sesión en Consola de administración de AWS, abra la consola de Amazon EBS y, a continuación, cree volúmenes de Amazon EBS para los servidores invitados de Sun SPRAC. Para obtener más información al respecto, consulte Configuración de una Nube de	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	AWS instancia para Charon-SSP en la documentación de Stromasys.	
Adjunte los volúmenes de Amazon EBS a la instancia Linux de Amazon EC2.	En la consola Amazon EC2, conecte los volúmenes de Amazon EBS a la instancia de Amazon EC2 Linux. Para obtener más informaci ón, consulte Adjuntar un volumen de Amazon EBS a una instancia en la documenta ción de Amazon EC2.	AWS DevOps
Mapee los volúmenes de Amazon EBS como unidades SCSI en el emulador Charon-SSP.	Configure Charon-SSP Manager para mapear los volúmenes de Amazon EBS como unidades SCSI en los servidores invitados Sun SPARC. Para obtener más informaci ón al respecto, consulte la sección Configuración del almacenamiento SCSI en la guía de Charon-SSP 5.2 para Linux en la documentación de Stromasys.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Configure la AWS Backup programación para la captura instantánea de los volúmenes de Amazon EBS.	Configure AWS Backup políticas y programas para realizar instantáneas de los volúmenes de Amazon EBS. Para obtener más información al respecto, consulte el AWS Backup tutorial sobre la copia de seguridad y restauración de Amazon EBS en la documentación del Centro de AWS desarrolladores.	AWS DevOps

Opción de Backup 4: Crear una AWS Storage Gateway VTL

Tarea	Descripción	Habilidades requeridas
Cree un dispositivo de Puerta de enlace de cinta.	Inicie sesión en Consola de administración de AWS, abra la AWS Storage Gateway consola y, a continuación, cree un dispositivo Tape Gateway en una VPC. Para obtener más información al respecto, consulte Crear una puerta de enlace en la AWS Storage Gateway documentación.	Arquitecto de la nube
Creación de una instancia de base de datos de Amazon RDS para el catálogo de Bacula.	Abra la consola de Amazon RDS y cree una instancia de base de datos de Amazon RDS para MySQL.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Para obtener más información al respecto, consulte Creación de una instancia de base de datos MySQL y conexión a una base de datos en una instancia de base de datos MySQL en la documentación de Amazon RDS.	
Implemente el controlador de aplicaciones de copia de seguridad en la VPC.	Instale Bacula en la instancia Amazon EC2, implemente el controlador de aplicaciones de respaldo y, a continuación, configure el almacenamiento de respaldo para que se conecte al dispositivo Tape Gateway. Puede usar el ejemplo de configuración del daemon de almacenamiento de Bacula Director que se encuentra en el archivo `Bacula-storage-daemon-config.txt` (adjunto). Para obtener más información, consulte la documentación de Bacula.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Configure la aplicación de copia de seguridad en los servidores invitados Sun SPARC.	Configure un segundo cliente para instalar y configurar la aplicación de copia de seguridad en los servidore s invitados de Sun SPARC utilizando el ejemplo de configuración de Bacula que se incluye en el archivo `SUN-SPARC-Guest-Bacula-Config.txt` (adjunto).	DevOps ingeniero
Configure la configuración y la programación de la copia de seguridad.	Configure la configuración y los horarios de las copias de seguridad en el controlador de la aplicación de copia de seguridad mediante el ejemplo de configuración de Bacula Director que se encuentra en el archivo `Bacula-Di rectory-Config.txt` (adjunto). Para obtener más información, consulte la documentación de Bacula.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Valide que la configuración y los programas de copia de seguridad sean correctos.	Siga las instrucciones de la documentación de Bacula para realizar las pruebas de validación y copia de seguridad de su configuración en los servidores invitados Sun SPARC. Por ejemplo, puede utilizar los siguientes comandos para validar los archivos de configuración: • `bacula-dir -t -c bacula-dir.conf` • `bacula-fd -t -c bacula-fd.conf` • `bacula-sd -t -c bacula-sd.conf`	DevOps ingeniero

Recursos relacionados

- SPARC virtual de Charon con licencia VE
- SPARC virtual de Charon
- Uso de servicios en la nube y almacenamiento de objetos con Bacula Enterprise Edition
- Objetivos de recuperación de desastres (DR)
- Soluciones de emulación de sistemas heredados de Charon

Información adicional

Opción de copia de seguridad 1: crear una cinta virtual de Stromasys

Puede utilizar el siguiente código de ejemplo del manual de procedimientos de automatización de Systems Manager para iniciar automáticamente la copia de seguridad y, a continuación, cambiar las cintas:

```
...
# example backup script saved in SUN SPARC Server
 #!/usr/bin/bash
 mt -f  rewind
 tar -cvf
 mt -f  offline
...
         mainSteps:
         - action: aws:runShellScript
           name:
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
               # Validate tape backup container file exists
               if [ ! -f {{TapeBackupContainerFile}} ]; then
                 logger -s -p local3.warning "Tape backup container file is not exists
 - {{TapeBackupContainerFile}}, create a new one"
                 touch {{TapeBackupContainerFile}}
               fi
         - action: aws:runShellScript
           name: startBackup
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
               user={{BACKUP_USER}}
               keypair={{KEYPAIR_PATH}}
               server={{SUN_SPARC_IP}}
               backup_script={{BACKUP_SCRIPT}}
               ssh -i $keypair $user@$server -c "/usr/bin/bash $backup_script"
         - action: aws:runShellScript
           name: swapVirtualDiskContainer
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
```

```
            - |
              mv {{TapeBackupContainerFile}} {{TapeBackupContainerFile}}.$(date +%s)
              touch {{TapeBackupContainerFile}}
        - action: aws:runShellScript
          name: uploadBackupArchiveToS3
          inputs:
            onFailure: Abort
            timeoutSeconds: "1200"
            runCommand:
            - |
              aws s3 cp {{TapeBackupContainerFile}} s3://{{BACKUP_BUCKET}}/
{{SUN_SPARC_IP}}/$(date '+%Y-%m-%d')/
 ...
```

Opción de copia de seguridad 2: crear una instantánea de Stromasys

Puede utilizar el siguiente código de ejemplo del manual de procedimientos de automatización de Systems Manager para iniciar automáticamente la copia de seguridad.

```
     ...

        mainSteps:
        - action: aws:runShellScript
          name: startSnapshot
          inputs:
            onFailure: Abort
            timeoutSeconds: "1200"
            runCommand:
            - |
              # You may consider some graceful stop of the application before taking a
 snapshot
              # Query SSP PID by configuration file
              # Example: ps ax | grep ssp-4 | grep Solaris10.cfg | awk '{print $1"
 "$5}' | grep ssp4 | cut -f1 -d" "
              pid=`ps ax | grep ssp-4 | grep {{SSP_GUEST_CONFIG_FILE}} | awk '{print
 $1" "$5}' | grep ssp4 | cut -f1 -d" "`
              if [ -n "${pid}" ]; then
                kill -SIGTSTP ${pid}
              else
                echo "No PID found for SPARC guest with config
 {{SSP_GUEST_CONFIG_FILE}}"
                exit 1
              fi
```

```
         - action: aws:runShellScript
           name: startBackup
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
               # upload snapshot and virtual disk files into S3
               aws s3 sync {{SNAPSHOT_FOLDER}} s3://{{BACKUP_BUCKET}}/$(date '+%Y-%m-
%d')/
               aws s3 cp {{VIRTUAL_DISK_FILE}} s3://{{BACKUP_BUCKET}}/$(date '+%Y-%m-
%d')/
         - action: aws:runShellScript
           name: restratSPARCGuest
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
               /opt/charon-ssp/ssp-4u/ssp4u -f {{SSP_GUEST_CONFIG_FILE}} -d -a
 {{SPARC_GUEST_NAME}} --snapshot {{SNAPSHOT_FOLDER}}
 ...
```

Opción de backup 4:AWS Storage GatewayVTL

Si utiliza zonas no globales de Solaris para ejecutar servidores Sun SPARC antiguos virtualizados, el enfoque de la aplicación de copia de seguridad se puede aplicar a las zonas no globales que se ejecutan en los servidores Sun SPARC (por ejemplo, el cliente de copia de seguridad puede ejecutarse dentro de las zonas no globales). Sin embargo, el cliente de copia de seguridad también se puede ejecutar en el host de Solaris y tomar instantáneas de las zonas no globales. A continuación, se puede hacer una copia de seguridad de las instantáneas en una cinta.

El siguiente ejemplo de configuración añade el sistema de archivos que aloja las zonas no globales de Solaris a la configuración de copia de seguridad del host de Solaris:

```
FileSet {
   Name = "Branded Zones"
   Include {
     Options {
       signature = MD5
     }
```

```
      File = /zones
    }
  }
```

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Realice copias de seguridad y archive datos en Amazon S3 con Veeam Backup & Replication

Jeanna James, Anthony Fiore (AWS) y William Quigley, Amazon Web Services

Resumen

Este patrón detalla el proceso de envío de copias de seguridad creadas por Veeam Backup & Replication a las clases de almacenamiento de objetos compatibles con Amazon Simple Storage Service (Amazon S3) mediante la capacidad de repositorio de copias de seguridad escalable de Veeam.

Veeam admite múltiples clases de almacenamiento de Amazon S3 para adaptarse mejor a sus necesidades específicas. Puede elegir el tipo de almacenamiento en función del acceso a los datos, la resiliencia y los requisitos de costo de sus datos de copia de seguridad o archivado. Por ejemplo, puede almacenar los datos que no planea usar durante 30 días o más en Amazon S3 de acceso poco frecuente (IA) a un menor costo. Si planea archivar datos durante 90 días o más, puede usar S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive con el nivel de archivado de Veeam. También puede usar el Bloqueo de objetos de S3 para hacer que las copias de seguridad sean inmutables en Amazon S3.

En este patrón no se describe cómo configurar Veeam Backup & Replication con una puerta de enlace de cinta en AWS Storage Gateway. Para obtener información sobre este tema, consulte Veeam Backup & Replication using AWS VTL Gateway - Deployment Guide en el sitio web de Veeam.

> Advertencia: este escenario requiere usuarios AWS Identity and Access Management (de IAM) con acceso programático y credenciales de larga duración, lo que supone un riesgo para la seguridad. Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten. Las claves de acceso se pueden actualizar si es necesario. Para obtener más informaci ón, consulte Actualización de claves de acceso en la Guía de usuario de IAM.

Requisitos previos y limitaciones

Requisitos previos

- Veeam Backup & Replication, que incluye Veeam Availability Suite o Veeam Backup Essentials, instalado (puede registrarse para obtener una prueba gratuita)
- Licencia Veeam Backup & Replication con funcionalidad Enterprise o Enterprise Plus, que incluye Veeam Universal License (VUL)
- Un usuario de IAM activo con acceso a un bucket de Amazon S3
- Un usuario de IAM activo con acceso a Amazon Elastic Compute Cloud (Amazon EC2) y Amazon Virtual Private Cloud (Amazon VPC), si utiliza el nivel de archivado
- Conectividad de red, desde local hasta Servicios de AWS con ancho de banda disponible para respaldar y restaurar el tráfico a través de una conexión pública a Internet o una interfaz virtual AWS Direct Connect pública (VIF)
- Se abrieron los siguientes puertos de red y puntos de conexión para garantizar una comunicación adecuada con los repositorios de almacenamiento de objetos:
  - Almacenamiento Amazon S3 — TCP — puerto 443: se utiliza para comunicarse con el almacenamiento de Amazon S3.
  - Almacenamiento de Amazon S3 (puntos de enlace en la nube) `*.amazonaws.com` para Regiones de AWS y las AWS GovCloud (US) Regions regiones de China: se utiliza `*.amazonaws.com.cn` para comunicarse con el almacenamiento de Amazon S3. Para obtener una lista completa de los puntos de conexión, consulte los puntos de enlace de Amazon S3 en la AWS documentación.
  - Almacenamiento en Amazon S3 — TCP HTTP — puerto 80: se utiliza para verificar el estado del certificado. Tenga en cuenta que los puntos finales de verificación de certificados (la lista de revocación de certificados (CRL) URLs y los servidores del Protocolo de estado de certificados en línea (OCSP) están sujetos a cambios. Encontrará la lista real de direcciones en el propio certificado.
  - Almacenamiento de Amazon S3 (puntos de conexión de verificación de certificados), `*.amazontrust.com`: se utiliza para verificar el estado del certificado. Tenga en cuenta que los puntos finales de verificación de certificados (servidores CRL y OCSP) están sujetos a cambios. URLs Encontrará la lista real de direcciones en el propio certificado.

Limitaciones

- Veeam no admite las políticas de ciclo de vida de S3 en ningún bucket de S3 que se utilice como repositorio de almacenamiento de objetos de Veeam. Estas incluyen políticas con transiciones de clases de almacenamiento de Amazon S3 y reglas de caducidad del ciclo de vida de S3. Veeam

debe ser la única entidad que administre estos objetos. La activación de las políticas de ciclo de vida de S3 puede tener resultados inesperados, incluida la pérdida de datos.

Versiones de producto

- Veeam Backup & Replication v9.5 Update 4 o posterior (solo nivel de copia de seguridad o de capacidad)
- Veeam Backup & Replication v10 o posterior (solo nivel de copia de seguridad o de capacidad y Bloqueo de objetos de S3)
- Veeam Backup & Replication v11 o posterior (copia de seguridad o nivel de capacidad, archivo o nivel de archivo y Bloqueo de objetos de S3)
- Veeam Backup & Replication v12 o posterior (nivel de rendimiento, copia de seguridad o nivel de capacidad, archivo o nivel de archivo y Bloqueo de objetos de S3)
- S3 Standard
- S3 Standard-IA
- S3 One Zone-IA
- S3 Glacier Flexible Retrieval (solo v11 y versiones posteriores)
- S3 Glacier Deep Archive (solo v11 y versiones posteriores)
- S3 Glacier Instant Retrieval (solo v12 y versiones posteriores)

Arquitectura

Pila de tecnología de origen

- Instalación en las instalaciones de Veeam Backup & Replication con conectividad desde un servidor de copia de seguridad de Veeam o un servidor gateway de Veeam a Amazon S3

Pila de tecnología de destino

- Amazon S3
- Amazon VPC y Amazon EC2 (si se utiliza el nivel de archivado)

Arquitectura de destino: SOBR

El siguiente diagrama muestra la arquitectura del repositorio de copias de seguridad escalable horizontalmente (SOBR).

El software Veeam Backup and Replication protege los datos de errores lógicos, como fallas del sistema, errores de aplicaciones o eliminaciones accidentales. En este diagrama, las copias de seguridad se ejecutan primero en las instalaciones y una copia secundaria se envía directamente a Amazon S3. Una copia de seguridad representa una point-in-time copia de los datos.

El flujo de trabajo consta de tres componentes principales necesarios para organizar o copiar las copias de seguridad en Amazon S3 y un componente opcional:

- Veeam Backup & Replication (1): el servidor de copia de seguridad responsable de coordinar, controlar y administrar la infraestructura de respaldo, la configuración, los trabajos, las tareas de recuperación y otros procesos.
- Servidor de puerta de enlace Veeam (no se muestra en el diagrama): un servidor de puerta de enlace en las instalaciones opcional que se requiere si el servidor de respaldo de Veeam no tiene conectividad saliente con Amazon S3.
- Repositorio de copia de seguridad escalable horizontalmente (2): sistema de repositorio con soporte de escalado horizontal para el almacenamiento de datos en varios niveles. El repositorio de copias de seguridad escalable horizontalmente consta de uno o más repositorios de copias de seguridad que proporcionan un acceso rápido a los datos y se pueden ampliar con los repositorios de almacenamiento de objetos de Amazon S3 para el almacenamiento a largo plazo (nivel de capacidad) y el archivado (nivel de archivo). Veeam utiliza el repositorio de copia de seguridad escalable horizontalmente para organizar los datos automáticamente entre el almacenamiento de objetos local (nivel de rendimiento) y el almacenamiento de objetos de Amazon S3 (niveles de capacidad y archivo).

> **Note**
>
> A partir de Veeam Backup & Replication v12.2, la función Direct to S3 Glacier hace que el nivel de capacidad S3 sea opcional. Un SOBR se puede configurar con un nivel de rendimiento y un nivel de archivo de S3 Glacier. Esta configuración resulta útil para los usuarios que tienen inversiones importantes en almacenamiento local (en las instalaciones) para el nivel de capacidad y que solo necesitan conservar los archivos a largo plazo en la nube. Para más información, consulte la documentación de Veeam Backup & Replication.

- Amazon S3 (3): servicio de almacenamiento de AWS objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento.

Arquitectura de destino: DTO

El siguiente diagrama muestra la arquitectura direct-to-object (DTO).

En este diagrama, los datos de las copias de seguridad van directamente a Amazon S3 sin almacenarse primero en las instalaciones. Las copias secundarias se pueden almacenar en S3 Glacier.

Automatización y escala

Puede automatizar la creación de recursos de IAM y depósitos de S3 mediante las CloudFormation plantillas que se proporcionan en el repositorio. VeeamHub GitHub Las plantillas incluyen opciones estándar e inmutables.

Tools (Herramientas)

Herramientas y Servicios de AWS

- Veeam Backup & Replication es una solución de Veeam para proteger, hacer copias de seguridad, replicar y restaurar sus cargas de trabajo físicas y virtuales.
- CloudFormationle ayuda a modelar y configurar sus AWS recursos, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Puede gestionar y aprovisionar pilas en múltiples Cuentas de AWS y Regiones de AWS.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática escalable en el Nube de AWS. Puede utilizar Amazon EC2 para lanzar tantos o tan pocos servidores virtuales como necesite, y puede ampliarlos de forma horizontal o horizontal.
- AWS Identity and Access Management (IAM) es un servicio web para controlar de forma segura el acceso a Servicios de AWS. Con IAM, puede gestionar de forma centralizada los usuarios, las credenciales de seguridad, como las claves de acceso, y los permisos que controlan a qué AWS recursos pueden acceder los usuarios y las aplicaciones.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web.
- Amazon S3 Glacier (S3 Glacier) es un servicio seguro y duradero para archivar datos a bajo costo y realizar copias de seguridad a largo plazo.
- Amazon Virtual Private Cloud (Amazon VPC) proporciona una sección aislada de forma lógica en la Nube de AWS que puede lanzar AWS los recursos en una red virtual que haya definido. Esta red virtual es muy similar a la red tradicional que usaría en su propio centro de datos, pero con los beneficios que supone utilizar la infraestructura escalable de AWS.

Código

Utilice las CloudFormation plantillas que se proporcionan en el VeeamHub GitHub repositorio para crear automáticamente los recursos de IAM y los depósitos de S3 para este patrón. Si prefiere crear estos recursos manualmente, siga los pasos de la sección Epics.

Prácticas recomendadas

De acuerdo con las prácticas recomendadas de IAM, le recomendamos encarecidamente que cambie periódicamente las credenciales de usuario de IAM a largo plazo, como el usuario de IAM que utiliza para escribir copias de seguridad de Veeam Backup & Replication en Amazon S3. Para obtener más información, consulte Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Configurar el almacenamiento de Amazon S3 en su cuenta

Tarea	Descripción	Habilidades requeridas
Cree un usuario de IAM.	Siga las instrucciones de la documentación de IAM para crear un usuario de IAM. Este usuario no debería tener acceso a la AWS consola y tendrá que crear una clave de acceso para este usuario. Veeam usa esta entidad	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	para autenticarse y leer y escribir en sus buckets de S3. AWS Debe conceder el privilegio mínimo (es decir, conceder solo los permisos necesarios para realizar una tarea) para que el usuario no tenga más autoridad de la que necesita. Para ver, por ejemplo, las políticas de IAM que debe adjuntar a su usuario de Veeam IAM, consulte la sección Información adicional. **Note** Como alternativa, puede usar las CloudFormation plantillas proporcionadas en el VeeamHub GitHub repositorio para crear un usuario de IAM y un bucket de S3 para este patrón.	

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	1. Inicie sesión en la consola Amazon S3 Consola de administración de AWS y ábrala. 2. Si aún no tiene un depósito de S3 existente para usarlo como almacenamiento de destino, elija Crear depósito y especifique el nombre del depósito y la configuración del depósito. Región de AWS • Le recomendamos que habilite la opción Bloquear el acceso público para el bucket de S3 y que configure las políticas de acceso y permisos de usuario para cumplir con los requisitos de su organización. Para ver un ejemplo, consulte la documentación de Amazon S3. • Le recomendamos que habilite Bloqueo de objetos de S3, incluso si no tiene intención de usarlo de inmediato. Esta configuración solo se puede habilitar en el momento de crear el bucket de S3.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte Crear un bucket en la documentación de Amazon S3.	

Añada Amazon S3 y S3 Glacier Flexible Retrieval (o S3 Glacier Deep Archive) a Veeam Backup & Replication

Tarea	Descripción	Habilidades requeridas
Inicie el asistente para el nuevo repositorio de objetos.	Antes de configurar el almacenamiento de objetos y los repositorios de backup escalables en Veeam, debe añadir los repositorios de almacenamiento Amazon S3 y S3 Glacier que desee utilizar para los niveles de capacidad y archivo. En la próxima épica, conectará estos repositor ios de almacenamiento a su repositorio copia de seguridad escalable horizontalmente. 1. En la consola de Veeam, abra la vista Infraestructura de copia de seguridad. 2. En el panel de inventario, elija el nodo Repositorios de copia de seguridad y, a continuación, elija Añadir repositorio. 3. En el cuadro de diálogo Añadir repositorio de	Administrador de AWS, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	copia de seguridad, elija Almacenamiento de objetos, Amazon S3.	

Tarea	Descripción	Habilidades requeridas
Añada almacenamiento de Amazon S3 al nivel de capacidad.	1. En el cuadro de diálogo Amazon Cloud Storage Services, elija Amazon S3. 2. En el paso Nombre del asistente, especifique el nombre del almacenamiento del objeto y una breve descripción, como el creador y la fecha de creación. 3. En el paso Cuenta del asistente, especifique la cuenta de almacenamiento de objetos. • En Credenciales, elija el usuario de IAM que creó en la primera epopeya para acceder a su almacenamiento de objetos de Amazon S3. • Para la región de AWS, elija Región de AWS la ubicación del bucket de S3. 4. En el paso Bucket del asistente, especifiq ue la configuración de almacenamiento de objetos. • En la región del centro de datos, Región de AWS elija la ubicación del depósito de S3.	Administrador de AWS, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	• Para Bucket, elija el bucket de S3 que creó en la primera épica. • En Carpeta, cree o seleccione una carpeta en la nube a la que asignar su repositorio de almacenamiento de objetos. • Si quiere activar la inmutabilidad, seleccion e Hacer que las copias de seguridad recientes sean inmutables durante X días y establezca el período de tiempo durante el cual deben estar bloqueadas las copias de seguridad. Tenga en cuenta que habilitar la inmutabil idad se traduce en un aumento de los costos debido al aumento del número de llamadas a la API a Amazon S3 desde Veeam. 5. En el paso de resumen del asistente, revise la información de configura ción y, a continuación, seleccione Finalizar.	

Tarea	Descripción	Habilidades requeridas
Añada el almacenamiento de S3 Glacier al nivel de archivo.	Si desea crear un nivel de archivo, utilice los permisos de IAM que se detallan en la sección Información adicional. 1. Inicie el asistente para el nuevo repositorio de objetos tal y como se describió anteriormente. 2. En el cuadro de diálogo Amazon Cloud Storage Services, elija Amazon S3 Glacier. 3. En el paso Nombre del asistente, especifique el nombre del almacenam iento del objeto y una breve descripción, como el creador y la fecha de creación. 4. En el paso Cuenta del asistente, especifique la cuenta de almacenamiento de objetos. • Para las credenciales, elija el usuario de IAM que creó en la primera epopeya para acceder a su almacenamiento de objetos de S3 Glacier. • Para la región de AWS, elija Región de AWS la ubicación del bucket de S3.	Administrador de AWS, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	5. En el paso Bucket del asistente, especifiq ue la configuración de almacenamiento de objetos. • En Región del centro de datos, elija la Región de AWS. • En Bucket, elija un bucket de S3 para almacenar los datos de copia de seguridad. Puede ser el mismo bucket que utilizó para el nivel de capacidad. • En Carpeta, cree o seleccione una carpeta en la nube a la que asignar su repositorio de almacenamiento de objetos. • Si quiere habilitar la inmutabilidad, seleccione Hacer que las copias de seguridad recientes sean inmutables durante toda su política de retención . Tenga en cuenta que habilitar la inmutabil idad se traduce en un aumento de los costos debido al aumento del número de llamadas a la API a Amazon S3 desde Veeam.	

Tarea	Descripción	Habilidades requeridas
	• Si quiere usar S3 Glacier Deep Archive como clase de almacenamiento de archivos, elija Usar la clase de almacenamiento Deep Archive. 6. En el paso Proxy Appliance del asistente, configure la instancia auxiliar que se utiliza para transferir los datos de Amazon S3 a S3 Glacier. Puede usar la configuración predeterminada o configurar cada configuración manualmente. Para configurar los ajustes manualmente: • Elija Personalizar. • Como tipo de EC2 instancia, elija el tipo de instancia para el dispositivo proxy en función de sus requisitos de velocidad y costo para transferir los archivos de respaldo al nivel de archivo de su repositorio de respaldo escalable. • En Amazon VPC, elija la VPC de la instancia de destino. • En Subredes, elija la subred del dispositivo proxy.	

Tarea	Descripción	Habilidades requeridas
	• Para Grupos de seguridad, elija el grupo de seguridad que desea asociar al dispositivo proxy. • En Puerto redirector, especifique el puerto TCP para enrutar las solicitud es entre el dispositivo proxy y los componentes de la infraestructura de copia de seguridad. • Elija Aceptar para confirmar la configura ción. 7. En el paso de resumen del asistente, revise la información de configura ción y, a continuación, seleccione Finalizar.	

Cómo añadir repositorios de copia de seguridad escalables horizontalmente

Tarea	Descripción	Habilidades requeridas
Inicie el asistente de nuevo repositorio de copia de seguridad escalable horizonta lmente.	1. En la consola de Veeam, abra la vista Infraestructura de copia de seguridad. 2. En el panel de inventario, seleccione Repositorios de escalado horizontal y, a continuación, seleccion	Propietario de la aplicación, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	e Añadir repositorio de escalado horizontal.	

Tarea	Descripción	Habilidades requeridas
Añada un repositorio de copias de seguridad escalable horizontalmente y configure los niveles de capacidad y archivo.	1. En el paso Nombre del asistente, especifique el nombre y una breve descripción del repositor io de copias de seguridad escalable horizontalmente. 2. Si es necesario, añada extensiones de rendimien to. También puede utilizar su repositorio de backup local de Veeam existente como nivel de rendimiento. A partir de la versión 12 de Veeam, puede añadir un bucket de S3 como medida de rendimiento para los backups direct-to-object (DTO), sin tener en cuenta el nivel de rendimiento local. 3. Elija Avanzado y especifiq ue opciones adicional es para el repositorio de copias de seguridad escalable horizontalmente. • Seleccione Utilizar archivos de copia de seguridad por máquina para crear un archivo de copia de seguridad independiente para cada máquina y escribir estos archivos en el repositorio de copias	Propietario de la aplicación, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	de seguridad en varios flujos de forma simultáne a. Se recomienda esta opción para una mejor utilización de los recursos de almacenamiento y procesamiento. • Seleccione Realizar una copia de seguridad completa cuando la extensión requerida esté desconectada para crear un archivo de copia de seguridad completo en caso de que una extensión que contiene puntos de restaurac ión para una copia de seguridad incremental quede sin conexión. Esta opción requiere espacio libre en el repositorio de copias de seguridad ampliable para alojar un archivo de copia de seguridad completo. 4. En el paso de políticas del asistente, especifique la política de ubicación de las copias de seguridad para el repositorio. • Elija la localidad de datos para almacenar juntos los archivos de copia	

Tarea	Descripción	Habilidades requeridas
	de seguridad completos e incrementales que pertenezcan a la misma cadena y con el mismo grado de rendimiento. Puede almacenar los archivos que pertenece n a una nueva cadena de copia de seguridad en el mismo nivel de rendimiento o en otro (a menos que utilice un dispositivo de almacenam iento deduplicado como medida de rendimiento). • Elija Rendimiento para almacenar archivos de copia de seguridad completos e increment ales con distintos niveles de rendimiento. Esta opción requiere una conexión de red rápida y fiable. Si elige Rendimien to, puede restringir los tipos de archivos de copia de seguridad que desea almacenar en cada nivel de rendimien to. Por ejemplo, puede almacenar archivos de copia de seguridad completos en una extensión y archivos de copia de seguridad	

Tarea	Descripción	Habilidades requeridas
	incrementales en otras extensiones. Para elegir los tipos de archivos: • Elija Personalizar. • En el cuadro de diálogo Configuración de ubicación de copias de seguridad, elija una extensión de rendimiento y, a continuación, elija Editar. • Elija el tipo de archivos de copia de seguridad que desee almacenar en la extensión. 5. En el paso Nivel de capacidad del asistente, configure el nivel de almacenamiento a largo plazo que desea adjuntar al repositorio de copias de seguridad escalable horizontalmente. • Elija Ampliar la capacidad del repositorio de copias de seguridad escalable horizontalmente con almacenamiento de objetos. Para el repositorio de almacenamiento de objetos, elija el almacenamiento de Amazon S3 para el nivel	

Tarea	Descripción	Habilidades requeridas
	de capacidad que agregó en la épica anterior. • Elija Ventana para seleccionar una ventana de tiempo para mover o copiar datos. • Seleccione Copiar las copias de seguridad en el almacenamiento de objetos tan pronto como se creen para copiar todos los archivos de copia de seguridad creados recientemente o solo en la medida de su capacidad. • Seleccione Mover las copias de seguridad al almacenamiento de objetos a medida que pasen del período de restauraciones operativa s para transferir las cadenas de copias de seguridad inactivas en la medida de su capacidad. En el campo Mover archivos de copia de seguridad con una antigüedad superior a X días, especifique la duración a partir de la cual deben descargar se los archivos de copia	

Tarea	Descripción	Habilidades requeridas
	de seguridad. (Para eliminar las cadenas de copia de seguridad inactivas el día en que se crearon, especifique 0 días). También puede elegir Anular para mover los archivos de copia de seguridad antes, si el repositorio de copias de seguridad escalable horizontalmente ha alcanzado el umbral que ha especificado. • Elija Cifrar los datos cargados en el almacenamiento de objetos y especifique una contraseña para cifrar todos los datos y sus metadatos para su descarga. Elija Agregar o Gestionar contraseñ as para especificar una nueva contraseña 6. En el paso Nivel de capacidad del asistente , configure el nivel de almacenamiento a largo plazo que desea adjuntar al repositorio de copias de seguridad escalable horizontalmente. (Este paso no aparece si omitió	

Tarea	Descripción	Habilidades requeridas
	añadir almacenamiento en Amazon S3 Glacier). • Elija Archivar las copias de seguridad completas de GFS en el almacenamiento de objetos. Para el repositorio de almacenamiento de objetos, elige el almacenamiento de Amazon Glacier que añadiste en la epopeya anterior. • En Copias de seguridad de Archive GFS que tengan más de N días, elija un intervalo de tiempo para mover los archivos a la extensión de archivado. (Para archivar las cadenas de copias de seguridad inactivas el día en que se crearon, especifique 0 días). 7. En el paso de Resumen del asistente, revise la configuración del repositorio de copias de seguridad escalable horizontalmente y, a continuación, seleccione Finalizar.	

Recursos relacionados

- Creación de un usuario de IAM en su Cuenta de AWS (documentación de IAM)
- Creación de un bucket (documentación de Amazon S3)
- Bloquear el acceso público al almacenamiento de Amazon S3 (documentación de Amazon S3)
- Uso del Bloqueo de objetos de S3 (documentación de Amazon S3)
- Documentación técnica de Veeam
- Cómo crear una política de IAM segura para la conexión a S3 Object Storage (documentación de Veeam)

Información adicional

Las siguientes secciones proporcionan ejemplos de políticas de IAM que puede utilizar al crear un usuario de IAM en la sección Epics de este patrón.

Política de IAM para el nivel de capacidad

> **Note**
>
> Cambie el nombre de los buckets de S3 en la política de ejemplo de `<yourbucketname>` por el nombre del bucket de S3 que desee utilizar para las copias de seguridad de los niveles de capacidad de Veeam. Tenga en cuenta también que la política debe restringirse a los recursos específicos utilizados por Veeam (lo que se indica en la `Resource` especificación de la siguiente política) y que la primera parte de la política inhabilita el cifrado del lado del cliente, como se explica en la entrada del AWS blog Prevenir el cifrado involuntario de objetos de Amazon S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RestrictSSECObjectUploads",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<your-bucket-name>/*",
            "Condition": {
```

```
                "Null": {
                    "s3:x-amz-server-side-encryption-customer-algorithm": "false"
                }
            }
        },
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:GetObjectVersion",
                "s3:ListBucketVersions",
                "s3:ListBucket",
                "s3:PutObjectLegalHold",
                "s3:GetBucketVersioning",
                "s3:GetObjectLegalHold",
                "s3:GetBucketObjectLockConfiguration",
                "s3:PutObject*",
                "s3:GetObject*",
                "s3:GetEncryptionConfiguration",
                "s3:PutObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:DeleteObject*",
                "s3:DeleteObjectVersion",
                "s3:GetBucketLocation"

            ],
            "Resource": [
                "arn:aws:s3:::<yourbucketname>",
                "arn:aws:s3:::<yourbucketname>/*"
            ]
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Política de IAM para el nivel de archivo

> **Note**
>
> Cambie el nombre de los buckets de S3 en la política de ejemplo de `<yourbucketname>` por el nombre del bucket de S3 que desee utilizar para las copias de seguridad del nivel de archivo de Veeam.

Para usar su VPC, subred y grupos de seguridad existentes:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:GetObject",
                "s3:RestoreObject",
                "s3:ListBucket",
                "s3:AbortMultipartUpload",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetBucketObjectLockConfiguration",
                "s3:PutObjectRetention",
                "s3:GetObjectVersion",
                "s3:PutObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:DeleteObjectVersion",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket-name>",
                "arn:aws:s3:::<bucket-name>/*"
            ]
        }
    ]
}

{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2Permissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:CreateKeyPair",
                "ec2:DescribeKeyPairs",
                "ec2:RunInstances",
                "ec2:DeleteKeyPair",
                "ec2:DescribeVpcAttribute",
                "ec2:CreateTags",
                "ec2:DescribeSubnets",
                "ec2:TerminateInstances",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeVpcs"
            ],
            "Resource": "arn:aws:ec2:<region>:<account-id>:*"
        }
    ]
}
```

Para crear nuevos grupos de VPC, subred y grupos de seguridad:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:GetObject",
                "s3:RestoreObject",
                "s3:ListBucket",
                "s3:AbortMultipartUpload",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetBucketObjectLockConfiguration",
```

```
                "s3:PutObjectRetention",
                "s3:GetObjectVersion",
                "s3:PutObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:DeleteObjectVersion",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket-name>",
                "arn:aws:s3:::<bucket-name>/*"
            ]
        }
    ]
}

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2Permissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:CreateKeyPair",
                "ec2:DescribeKeyPairs",
                "ec2:RunInstances",
                "ec2:DeleteKeyPair",
                "ec2:DescribeVpcAttribute",
                "ec2:CreateTags",
                "ec2:DescribeSubnets",
                "ec2:TerminateInstances",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeVpcs",
                "ec2:CreateVpc",
                "ec2:CreateSubnet",
                "ec2:DescribeAvailabilityZones",
                "ec2:CreateRoute",
                "ec2:CreateInternetGateway",
                "ec2:AttachInternetGateway",
                "ec2:ModifyVpcAttribute",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:AuthorizeSecurityGroupIngress",
```

```
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:DescribeRouteTables",
                "ec2:DescribeInstanceTypes"
            ],
            "Resource": "*"
        }
    ]
}
```

Copie datos de un bucket de Amazon S3 a otra cuenta o región mediante el AWS CLI

Appasaheb Bagali y Purushotham G K, Amazon Web Services

Resumen

Este patrón describe cómo migrar datos desde un bucket de Amazon Simple Storage Service (Amazon S3) de origen de AWS una cuenta a un bucket de Amazon S3 de destino de AWS otra cuenta, ya sea en la Región de AWS misma región o en una diferente.

El bucket Amazon S3 de origen permite el acceso AWS Identity and Access Management (IAM) mediante una política de recursos adjunta. Un usuario de la cuenta de destino debe asumir un rol que tenga permisos `PutObject` y `GetObject`para el bucket de origen. Por último, ejecuta `copy` `sync` comandos para transferir datos del bucket Amazon S3 de origen al bucket Amazon S3 de destino.

Las cuentas son propietarias de los objetos que cargan en los buckets de Amazon S3. Si copia objetos entre cuentas y regiones, otorga a la cuenta de destino la propiedad de los objetos copiados. Para cambiar la propiedad de un objeto, cambie su lista de control de acceso (ACL) a `bucket-owner-full-control`. Sin embargo, le recomendamos que conceda permisos programáticos para varias cuentas a la cuenta de destino, ya que ACLs puede resultar difícil administrarlos para varios objetos.

> **Warning**
>
> En este escenario, se requieren usuarios de IAM con acceso programático y credenciales de larga duración, lo que supone un riesgo de seguridad. Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten. Las claves de acceso se pueden actualizar si es necesario. Para obtener más información, consulte Actualización de las claves de acceso en la documentación de IAM.

Requisitos previos y limitaciones

Requisitos previos

- Dos activos Cuentas de AWS iguales o diferentes. Regiones de AWS

- Un bucket de Amazon S3 existente en la cuenta de origen.
- Si su bucket de Amazon S3 de origen o destino tiene activado el cifrado por defecto, debe modificar los permisos de la clave AWS Key Management Service (AWS KMS). Para obtener más información, consulte el artículo de AWS Re:post sobre este tema.
- Familiaridad con los permisos entre cuentas.

Limitaciones

- Este patrón cubre una migración única. Para los escenarios que requieren la migración continua y automática de nuevos objetos de un bucket de origen a un bucket de destino, puede utilizar Amazon S3 Batch Replication.
- Este patrón utiliza credenciales de sesión (`AccessKeyIdSecretAccessKey`, y`SessionToken`) que son temporales y no persistentes. La marca de tiempo de caducidad de la salida indica cuándo caducan estas credenciales. El rol se configura con la duración máxima de la sesión. El trabajo de copia se cancelará si la sesión caduca.

Arquitectura

Tools (Herramientas)

- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar Servicios de AWS mediante los comandos de su consola de línea de comandos.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Prácticas recomendadas

- Prácticas recomendadas de seguridad en IAM (documentación de IAM)
- Aplicar permisos con privilegios mínimos (documentación de IAM)

Epics

Cree un usuario y un rol de IAM en el destino Cuenta de AWS

Tarea	Descripción	Habilidades requeridas
Crear un usuario de IAM para conseguir la clave de acceso.	1. Inicie sesión en Consola de administración de AWS y cree un usuario de IAM que tenga acceso mediante programación. Para obtener instrucciones detallada s, consulte Creación de usuarios de IAM en la documentación de IAM. No es necesario adjuntar ninguna política para este usuario. 2. Genere una clave de acceso y una clave secreta para este usuario. Para obtener instrucciones, consulte Cuenta de AWS las claves de acceso en la AWS documentación.	AWS DevOps
Crear una política de IAM basada en identidades.	Cree una política de IAM basada en la identidad denominada `S3MigrationPolicy` mediante los siguientes permisos. Modifique los nombres de los buckets de origen y destino según su caso de uso. Esta política basada en la identidad permite al usuario que asume esta	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	función acceder al depósito de origen y al depósito de destino. Para obtener instrucciones detalladas, consulte Creación de políticas de IAM en la documentación de IAM. { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:ListBucket", "s3:ListObjectsV2", "s3:GetObject", "s3:GetObjectTagging", "s3:GetObjectVersion", "s3:GetObjectVersionTagging"], "Resource": ["arn:aws:s3:::amazon-s3-demo-source-bucket", "arn:aws:s3:::amazon-	

Tarea	Descripción	Habilidades requeridas

	s3-demo-source-bucket/*"
	            ]
	        },
	        {
	            "Effect": "Allow",
	            "Action": [
	"s3:ListBucket",
	"s3:PutObject",
	"s3:PutObjectAcl",
	"s3:PutObjectTagging",
	"s3:GetObjectTagging",
	"s3:ListObjectsV2",
	"s3:GetObjectVersion",
	"s3:GetObjectVersionTagging"
	            ],
	            "Resource": [
	"arn:aws:s3:::amazon-s3-demo-destination-bucket",
	"arn:aws:s3:::amazon-s3-demo-destination-bucket/*"
	            ]
	        }
	    ]	

Tarea	Descripción	Habilidades requeridas
	} }	

Tarea	Descripción	Habilidades requeridas
Crear un rol de IAM.	Cree un rol de IAM denominado `S3MigrationRole` mediante la siguiente política de confianza. Modifique el nombre de recurso de Amazon (ARN) del nombre de usuario o el rol de IAM de destino en la política de confianza según el caso de uso. Esta política de confianza permite que el recién creado usuario de IAM asuma `S3MigrationRole` . Adjunte el creado `S3MigrationPolicy` anteriormente. Para conocer los pasos detallados, consulte Crear una función para delegar permisos a un usuario de IAM en la documentación de IAM. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::<destination_account>:user/<user_name>" }, "Action": "sts:AssumeRole",`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	<pre>"Conditio
	n": {}
	}
	]
	}</pre>	

Cree y adjunte la política de bucket de Amazon S3 a la cuenta de origen

Tarea	Descripción	Habilidades requeridas
Cree y adjunte una política de bucket de Amazon S3.	1. Inicie sesión en su cuenta Consola de administración de AWS de origen y abra la consola de Amazon S3. 2. Elija el bucket de Amazon S3 de origen y, a continuación, elija Permisos. 3. En Política de bucket, elija Editar. 4. Pegue la siguiente política de bucket. Asegúrese de incluir el Cuenta de AWS ID de la cuenta de destino y configure la plantilla de política de bucket de acuerdo con sus requisitos. Esta política basada en recursos permite al rol de destino acceder `S3MigrationRole` a los objetos de Amazon S3 de la cuenta de origen. <pre>{</pre>	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	"Version": "2012-10-17", "Statement": [{ "Sid": "DelegateS3Access", "Effect": "Allow", "Principal": {"AWS": "arn:aws:iam::<destination_account>:role/<RoleName>"}, "Action": ["s3:ListBucket", "s3:GetObject", "s3:ListObjectsV2", "s3:GetObjectTagging", "s3:GetObjectVersion", "s3:GetObjectVersionTagging"], "Resource": ["arn:aws:s3:::amazon-s3-demo-source-bucket/*", "arn:aws:s3:::amazon-s3-demo-source-bucket"] }	

Tarea	Descripción	Habilidades requeridas
	] } 5. Seleccione Save.	

Configurar el bucket Amazon S3 de destino

Tarea	Descripción	Habilidades requeridas
Cree un bucket de Amazon S3 de destino.	1. Inicie sesión en la cuenta Consola de administración de AWS de destino y abra la consola de Amazon S3. 2. Elija Crear bucket. 3. Cree un bucket de Amazon S3 según sus necesidades. Para obtener más información, consulte Crear un bucket en la documentación de Amazon S3.	Administrador de la nube

Copie los datos al bucket de Amazon S3 de destino

Tarea	Descripción	Habilidades requeridas
Configure el AWS CLI con las credenciales de usuario recién creadas.	1. Instale la última versión de AWS CLI. Para obtener instrucciones, consulte Instalación o actualización de la última versión de AWS CLI en la AWS CLI documentación. 2. Ejecute `$ aws configure` y actualice	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	AWS CLI con la clave de AWS acceso del usuario de IAM que creó. Para obtener más información, consulte los ajustes de configuración y del archivo de credenciales en la AWS CLI documentación.	

Tarea	Descripción	Habilidades requeridas
Asuma la función de migración de Amazon S3.	1. Use el AWS CLI para asumir`S3MigrationRole` : `aws sts assume-role \ --role-arn "arn:aws:iam::<destination_account>:role/S3MigrationRole" \ --role-session-name AWSCLI-Session` **Note** Este comando genera varios datos. Dentro del bloque de credenciales, necesita las `AccessKeyId` , `SecretAccessKey` , y `SessionToken` . En este ejemplo se utilizan las variables de entorno `RoleAccessKeyID` , `RoleSecretKey` , y `RoleSessionToken` . : Las credenciales de sesión (`AccessKeyId` `SecretAcc`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	`essKey` , `ySessionToken`) son temporales y no persistentes. La marca de tiempo de caducidad del resultado indica cuándo caducan estas credencia les. El rol se configura con la duración máxima de la sesión. Si las credenciales caducan, debe `sts:AssumeRole` volver a llamar para obtener nuevas credenciales temporales.
	2. Cree tres variables de entorno para asumir el rol de IAM. Estas variables de entorno se completan con el siguiente resultado:
	`# Linux`
	`export AWS_ACCES S_KEY_ID=<RoleAcce ssKeyID from command output>`
	`export AWS_SECRE T_ACCESS_KEY=<Role SecretKey from command output>`	

Tarea	Descripción	Habilidades requeridas

	`export AWS_SESSI ON_TOKEN=<RoleSess ionToken from command output>`
	`# Windows`
	`set AWS_ACCES S_KEY_ID=<RoleAcce ssKeyID from command output>`
	`set AWS_SECRE T_ACCESS_KEY=<Role SecretKey from command output>`
	`set AWS_SESSI ON_TOKEN=<RoleSess ionToken from command output>`
	3. Verifique que ha asumido el rol de IAM mediante la ejecución del siguiente comando:
	`aws sts get-caller-identity`
	Para obtener más informaci ón, consulte ¿Cómo se utiliza AWS CLI para asumir una función de IAM?	

Tarea	Descripción	Habilidades requeridas

Copie y sincronice los datos del depósito de origen con el depósito de destino.	Cuando haya asumido el rol, `S3MigrationRole` puede copiar los datos mediante el comando copy (`cp`) o synchronize (`sync`).
	
	Copiar:
	
	`aws s3 cp s3://amazon-s3-demo-source-bucket/ \ s3://amazon-s3-demo-destination-bucket/ \ --recursive --source-region SOURCE-REGION-NAME --region DESTINATION-REGION-NAME`
	
	Sincronizar:
	
	`aws s3 sync s3://amazon-s3-demo-source-bucket/ \ s3://amazon-s3-demo-destination-bucket/ \ --source-region SOURCE-REGION-NAME --region DESTINATION-REGION-NAME`
		Administrador de la nube

Resolución de problemas

Problema	Solución
Se produjo un error (`AccessDenied `) al llamar a la operación `ListObjects`	1. Asegúrese de haber asumido el rol `S3MigrationRole` . 2. Ejecute `aws sts get-caller-identit` y para comprobar el rol utilizado. Si el resultado no muestra el ARN de`S3Migrationrole` , vuelva a asumir la función de IAM y vuelva a intentarlo.

Recursos relacionados

- Creación de un bucket de Amazon S3 (documentación de Amazon S3)
- Políticas de bucket y políticas de usuario de Amazon S3 (documentación de Amazon S3)
- Identidades de IAM (usuarios, grupos y roles) (documentación de IAM)
- comando cp (AWS CLI documentación)
- comando sync (AWS CLI documentación)

Habilite el archivado de DB2 registros directamente en Amazon S3 en una base de datos IBM Db2

Ambarish Satarkar, Amazon Web Services

Resumen

Este patrón describe cómo usar Amazon Simple Storage Service (Amazon S3) como almacenamiento de catálogos para los registros de archivos que genera IBM Db2, sin usar un área de almacenamiento provisional.

Puede especificar el almacenamiento DB2REMOTO en Amazon S3 para los parámetros de configuración de los métodos de archivado de registros logarchmeth1 y logarchmeth2. Puede usar el parámetro `logarchmeth1` para especificar el destino principal de los registros que se archivan desde la ruta de registro actual. Con esta capacidad, puede archivar y recuperar registros de transacciones desde y hacia Amazon S3 directamente, sin necesidad de utilizar un área de almacenamiento provisional.

Amazon S3 almacena los datos que se cargan en él en al menos tres dispositivos en una sola Región de AWS. Millones de clientes de todos los tamaños y sectores utilizan Amazon S3 para almacenar copias de seguridad empresariales debido a su alta disponibilidad, opciones de almacenamiento flexibles, políticas de ciclo de vida y seguridad.

Requisitos previos y limitaciones

Requisitos previos

- Cuenta de AWS Un activo.
- Base de datos IBM Db2 que se ejecuta en una instancia de Amazon Elastic Compute Cloud (Amazon EC2).
- AWS Command Line Interface (AWS CLI) instalado
- libcurl y libxml2 instalados en la instancia de Db2. EC2

Limitaciones

- Solo Db2 11.5.7 o posterior permite archivar registros directamente en el almacenamiento de Amazon S3.

- Algunas Servicios de AWS no están disponibles en todas. Regiones de AWS Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.
- En todas las configuraciones, existen las siguientes limitaciones para Amazon S3:
  - AWS Key Management Service (AWS KMS) no es compatible.
  - AWS No se admiten las credenciales basadas en roles AWS Identity and Access Management ((IAM) o basadas en tokens (AWS Security Token Service (AWS STS)).

Versiones de producto

- AWS CLI versión 2 o posterior
- IBM Db2 11.5.7 o posterior
- SUSE Linux Enterprise Server (SLES) 11 o posterior
- Red Hat Enterprise Linux (RHEL) 6 o posterior
- Windows Server 2008 R2, 2012 (R2), 2016 o 2019

Arquitectura

En el siguiente diagrama se muestran los componentes y el flujo de trabajo de este patrón.

La arquitectura de Nube de AWS incluye lo siguiente:

- Nube privada virtual (VPC): una sección aislada lógicamente de la que Nube de AWS se lanzan los recursos.
- Zona de disponibilidad: proporciona alta disponibilidad al ejecutar la carga de trabajo LUW de Db2 (Linux, Unix, Windows) en un centro de datos aislado dentro de la Región de AWS.
- Subred pública: proporciona acceso RDP (protocolo de escritorio remoto) para los administradores y conectividad a Internet a través de una puerta de enlace de NAT.
- Subred privada: aloja la base de datos LUW de Db2. La instancia LUW de Db2 se configura con el parámetro `LOGARCHMETH1`. El parámetro escribe los archivos de registro de la base de datos directamente en una ruta de Amazon S3 a través del punto de conexión de la puerta de enlace.

Lo siguiente Servicios de AWS proporciona soporte:

- Amazon S3: sirve como ubicación de almacenamiento escalable y duradera para los archivos de registro de Db2.
- Amazon Elastic File System (Amazon EFS): proporciona un sistema de archivos compartido y totalmente administrado que Db2 puede utilizar para copias de seguridad y almacenamiento provisional de bases de datos. Db2 también puede utilizar Amazon EFS como punto de montaje para los archivos de registro antes de archivarlos en Amazon S3.
- Amazon CloudWatch: recopila y monitorea métricas, registros y eventos de Db2 y las EC2 instancias subyacentes. Puede utilizarlos CloudWatch para crear alarmas, paneles y respuestas automatizadas a problemas de rendimiento o disponibilidad.

Automatización y escala

- Este patrón proporciona una solución totalmente automatizada para almacenar las copias de seguridad de los archivos de registro de Db2.
- Puede usar el mismo bucket de Amazon S3 para habilitar el archivado de registros de varias bases de datos de Db2.

Tools (Herramientas)

Servicios de AWS

- Amazon le CloudWatch ayuda a supervisar las métricas de sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar Servicios de AWS mediante comandos en su shell de línea de comandos.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática escalable en el Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Elastic File System (Amazon EFS) lo ayuda a crear y configurar sistemas de archivos compartidos en la Nube de AWS.
- AWS IAM Identity Centerle ayuda a gestionar de forma centralizada el acceso mediante inicio de sesión único (SSO) a todas sus aplicaciones Cuentas de AWS y a las de la nube.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Otras herramientas

- libcurl es una biblioteca gratuita de transferencia de URL del lado del cliente.
- libxml2 es un kit de herramientas y analizador XML C gratuito.

Prácticas recomendadas

- Siga el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Configuración Servicios de AWS

Tarea	Descripción	Habilidades requeridas

Configure el AWS CLI.	Para descargar e instalar el AWS CLI, utilice los siguientes comandos:
	`i) curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"`
	`ii) unzip awscliv2.zip`
	`iii) sudo ./aws/install`
		Administrador de sistemas de AWS; administrador de AWS

Configure la AWS CLI.	Para configurar el AWS CLI, utilice los siguientes comandos:	Administrador de sistemas de AWS; administrador de AWS

Tarea	Descripción	Habilidades requeridas

	`$ aws configure`
	`AWS Access Key ID`
	` [None]:**********`
	`**********`
	`AWS Secret Access Key`
	` [None]: *********`
	`**********`
	`Default region name`
	` [None]: < aws region >`
	`Default output format`
	` [None]: text`	

Tarea	Descripción	Habilidades requeridas

Cree un usuario de IAM.	Para crear un usuario de IAM para usarlo más adelante en la conexión de base de datos de Db2 con Amazon S3, utilice el siguiente comando:
	
	`aws iam create-user --user-name <unique username>`
	
	A continuación, se muestra un ejemplo del comando:
	
	`aws iam create-user --user-name db_backup_user`
	
	Warning
	En este escenario, se requieren usuarios de IAM con acceso programático y credenciales de larga duración, lo que supone un riesgo de seguridad. Para mitigar este riesgo, le recomendamos que brinde a estos usuarios únicament e los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten. Las
		Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	claves de acceso se pueden actualizar si es necesario. Para obtener más información, consulte las credenciales de seguridad de AWS y la sección Administrar las claves de acceso para los usuarios de IAM en la documentación de IAM.	

Cree un bucket de Amazon S3.	Para crear un bucket de Amazon S3 a fin de almacenar la copia de seguridad de la base de datos, utilice el siguiente comando:
	`aws s3api create-bucket --bucket <unique bucket name> --region <aws region>`
	A continuación, se muestra un comando de ejemplo:
	`aws s3api create-bucket --bucket myfirstbucket --region af-south-1`
		Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
Autorice el usuario de IAM.	Para autorizar el usuario de IAM recién creado a tener permisos de Amazon S3, siga estos pasos: 1. Para generar un nuevo archivo de políticas de IAM `db2bucket.json` para el bucket de Amazon S3, utilice el siguiente comando: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "ListObjectsInBucket", "Effect": "Allow", "Action": "s3:ListBucket", "Resource": [ "arn:aws:s3:::myfirstbucket" ] }, { "Sid": "AllObjectActions", "Effect": "Allow", "Action": [` Administrador de sistemas de AWS; administrador de AWS

Tarea	Descripción	Habilidades requeridas

	<pre>"s3:PutObject",
	
	"s3:GetObject",
	
	"s3:DeleteObject"
	],
	"Resource
	": [
	
	"arn:aws:s3:::myfi
	rstbucket/*"
	]
	}
	]
	}</pre>
	2. Cree una política de IAM basada en el archivo `db2bucket.json` . El resultado de JSON muestra el nombre de recurso de Amazon (ARN) para la política: `"Arn": "arn:aws:iam::111122223333:policy/db2s3policy"` .
	
	<pre>aws iam create-policy
	\
	--policy-name
	db2s3policy \
	--policy-
	document file://db
	2bucket.json</pre>
	3. Adjunte la política de IAM al usuario de IAM con el ARN de la política.	

Tarea	Descripción	Habilidades requeridas
	`aws iam attach-user-policy --user-name db_backup_user --policy-arn "arn:aws:iam::111122223333:policy/db2s3policy"`	

Tarea	Descripción	Habilidades requeridas

Cree una clave de acceso.	Para generar una clave de acceso para acceder mediante programación a Amazon S3 desde la DB2 instancia, utilice el siguiente comando:
	
	`aws iam create-access-key --user-name <username>`
	
	A continuación, se muestra un ejemplo del comando:
	
	`aws iam create-access-key --user-name db_backup_user`
	
	Warning
	En este escenario, se requieren usuarios de IAM con acceso programático y credenciales de larga duración, lo que supone un riesgo de seguridad. Para mitigar este riesgo, le recomendamos que brinde a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten. Las
		Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	claves de acceso se pueden actualizar si es necesario. Para obtener más información, consulte las credenciales de seguridad de AWS y la sección Administrar las claves de acceso para los usuarios de IAM en la documentación de IAM.	
Cree un almacén de claves PKCS.	Para crear un almacén de claves PKCS para almacenar la clave y crear una clave de acceso secreta para transferir los datos a Amazon S3, utilice el siguiente comando: `gsk8capicmd_64 -keydb -create -db "/db2/db2<sid>/.keystore/db6-s3.p12" -pw "<password>" -type pkcs12 -stash`	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
Configure DB2 para usar el almacén de claves.	DB2 Para configurar el uso del almacén de claves con los `keystore_type` parámetro s `keystore_location` y, utilice los siguientes comandos: `db2 "update dbm cfg using keystore_location /db2/db2<sid>/.keystore/db6-s3.p12 keystore_type pkcs12"`	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas

Cree un alias DB2 de acceso al almacenamiento.	Un alias de acceso al almacenamiento específico el bucket de Amazon S3 que se utilizará. También proporciona los detalles de la conexión, como el nombre de usuario y la contraseña, que se almacenan en el almacén de claves local en un formato cifrado. Para obtener más información, consulte el comando CATALOG STORAGE ACCESS en la documentación de IBM Db2.
	
	Para crear el alias de acceso al almacenamiento, use la siguiente sintaxis:
	
	`db2 "catalog storage access alias <alias_name> vendor S3 server <S3 endpoint> user '<access_key>' password '<secret_access_key>' container '<bucket_name>'"`
	
	A continuación se muestra un ejemplo:
	
	`db2 "catalog storage access alias DB2BKPS3 vendor S3 server s3.us-west-2.amazonaws.com user '********' password`
		Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	`'*****************` `****' container` `'myfirstbucket'"`	

Actualice la ubicación de logarchmeth1 en y reinicie DB2 DB2

Tarea	Descripción	Habilidades requeridas

Actualice la ubicación `LOGARCHMETH1` .	Para usar el alias de acceso al almacenamiento que definió anteriormente, actualice los parámetros de la base de datos `LOGARCHMETH1` y utilice el siguiente comando:
	`db2 update db cfg for <DBNAME> using LOGARCHMETH1 'DB2REMOTE://<storage_alias_name>//<sub folder>'`
	Para separar los registros de otros archivos, especifique un subdirectorio (es decir, el prefijo del bucket de Amazon S3) `TESTDB_LOGS` en el que guardar los registros del bucket de S3.
	A continuación se muestra un ejemplo:
	`db2 update db cfg for ABC using LOGARCHME`
		Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	`TH1 'DB2REMOTE://DB2BK PS3//TESTDB_LOGS/'` Debería ver el siguiente mensaje: `DB20000I The UPDATE DATABASE CONFIGURATION command completed successfu lly.`	
Reiniciar DB2.	Reinicie la DB2 instancia después de volver a configura rla para el archivado de registros. Sin embargo, si anteriormente `LOGARCHMETH1` estaba configurado en cualquier ubicación del sistema de archivos, no es necesario reiniciarlo.	Administrador AWS, administr ador de sistemas AWS

Comprobación de la ruta del registro del archivo en Amazon S3 y db2diag.log

Tarea	Descripción	Habilidades requeridas
Compruebe el registro de archivos en Amazon S3.	En este punto, la base de datos está completamente configurada para archivar los registros de transacciones directamente en el almacenam iento de Amazon S3. Para confirmar la configuración, comience a ejecutar actividad es transaccionales en la	Administrador AWS, administr ador de sistemas AWS

Tarea	Descripción	Habilidades requeridas
	base de datos para empezar a consumir (y archivar) el espacio de registro. A continuación, compruebe los registros de archivos en Amazon S3.	

Tarea	Descripción	Habilidades requeridas
Compruebe la configuración del registro de archivos en `db2diag.log` .	Tras comprobar el registro de archivos en Amazon S3, busque el siguiente mensaje en el registro DB2 de diagnósticodb2diag.log : `MESSAGE : ADM1846I Completed archive for log file "S0000079.LOG" to Completed archive for log file S0000080.LOG to DB2REMOTE://<AWS S3 Bucket Name>/<SID>/log1/db2<sid>/<SID>/NODE0000/LOGSTREAM0000/C0000001/ from /db2/<SID>/log_dir/NODE0000/LOGSTREAM0000/. MESSAGE : ADM1846I Completed archive for log file "S0000080.LOG" to Completed archive for log file S0000081.LOG to DB2REMOTE://<AWS S3 Bucket Name> /<SID>/log1/db2<sid>/<SID>/NODE0000/LOGSTREAM0000/C0000001/ from /db2/<SID>/log_dir/NODE0000/LOGSTREAM0000/.`	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	Este mensaje confirma que los archivos del registro de DB2 transacciones cerradas se están archivando en el almacenamiento (remoto) de Amazon S3.	

Recursos relacionados

AWS documentación de servicio

- AWS credenciales de seguridad (documentación de IAM)
- Concesión del privilegio mínimo (documentación de IAM)
- Administración de claves de acceso para usuarios de IAM (documentación de IAM)
- Prácticas recomendadas de seguridad en IAM (documentación de IAM)

Recursos de IBM

- Base de datos IBM Db2
- logarchmeth1: parámetro de configuración del método de archivado de registros principal
- logarchmeth2: parámetro de configuración del método de archivado de registros secundario
- Almacenamiento remoto

Migre datos de un entorno Hadoop local a Amazon S3 con DistCp AWS PrivateLink para Amazon S3

Jason Owens, Andrés Cantor, Jeff Klopfenstein, Bruno Rocha Oliveira y Samuel Schmidt, Amazon Web Services

Resumen

Este patrón demuestra cómo migrar prácticamente cualquier cantidad de datos desde un entorno Apache Hadoop local a la nube de Amazon Web Services (AWS) mediante la herramienta de código abierto Apache con DistCpAWS for PrivateLink Amazon Simple Storage Service (Amazon S3). En lugar de utilizar la Internet pública o una solución proxy para migrar los datos, puede utilizar AWS PrivateLink para Amazon S3 para migrar los datos a Amazon S3 a través de una conexión de red privada entre su centro de datos local y una Amazon Virtual Private Cloud (Amazon VPC). Si usa entradas de DNS en Amazon Route 53 o añade entradas en el archivo /etc/hosts en todos los nodos del clúster de Hadoop en las instalaciones, se le redirigirá automáticamente al punto de conexión de interfaz correcto.

Esta guía proporciona instrucciones de uso DistCp para migrar datos a la nube de AWS. DistCp es la herramienta más utilizada, pero hay otras herramientas de migración disponibles. Por ejemplo, puede usar herramientas de AWS sin conexión, como AWS Snowball o AWS Snowmobile, o herramientas de AWS en línea, como AWS Storage Gateway o AWS. DataSync Además, puede utilizar otras herramientas de código abierto, como Apache. NiFi

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa con una conexión de red privada entre el centro de datos en las instalaciones y la nube de AWS
- Hadoop, instalado in situ con DistCp
- Un usuario de Hadoop con acceso a los datos de migración en el sistema de archivos distribuido de Hadoop (HDFS)
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada
- Permisos para colocar objetos en un bucket de S3

Limitaciones

Las limitaciones de la nube privada virtual (VPC) se aplican a AWS PrivateLink para Amazon S3. Para obtener más información, consulte las propiedades y limitaciones de los puntos de conexión de la interfaz y PrivateLink las cuotas de AWS (PrivateLink documentación de AWS).

AWS PrivateLink para Amazon S3 no admite lo siguiente:

- Puntos de conexión del estándar federal de procesamiento de información (FIPS)
- Puntos de conexión del sitio web
- Puntos de enlace global heredado

Arquitectura

Pila de tecnología de origen

- Clúster de Hadoop con instalado DistCp

Pila de tecnología de destino

- Amazon S3
- Amazon VPC

Arquitectura de destino

El diagrama muestra cómo el administrador de Hadoop copia datos desde un entorno local DistCp a través de una conexión de red privada, como AWS Direct Connect, a Amazon S3 a través de un punto de enlace de la interfaz Amazon S3.

Tools (Herramientas)

Servicios de AWS

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Otras herramientas

- Apache Hadoop DistCp (copia distribuida) es una herramienta que se utiliza para copiar grandes clústeres e intracústeres. DistCp utiliza Apache MapReduce para la distribución, la gestión y recuperación de errores y la elaboración de informes.

Epics

Migración de datos a la nube de AWS

Tarea	Descripción	Habilidades requeridas
Cree un punto de conexión para AWS PrivateLink para Amazon S3.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon VPC. 2. En el panel de navegación, elija Endpoints (puntos de conexión) y, a continuación, elija Create Endpoint (Crear punto de enlace). 3. En Service category, seleccione AWS services. 4. En el campo de búsqueda, escriba s3 y, a continuac ión, pulse Intro. 5. En los resultados de la búsqueda, elija com.amazo naws. Nombre del servicio < your-aws-region >.s3 donde el valor de la columna Tipo es Interfaz.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	6. En VPC, elija su VPC. En Subredes, elija sus subredes. 7. En Grupo de seguridad , elija o cree un grupo de seguridad que permita TCP 443. 8. Añada etiquetas en función de sus necesidades y, a continuación, seleccione Crear punto de conexión.	
Compruebe los puntos de conexión y busque las entradas de DNS.	1. Abra la consola de Amazon VPC, elija Puntos de conexión y, a continuac ión, seleccione el punto de conexión que creó anteriormente. 2. En la pestaña Detalles, busque la primera entrada de DNS en nombres de DNS. Esta es la entrada de DNS regional. Al usar este nombre de DNS, las solicitudes alternan entre las entradas de DNS específicas de las zonas de disponibilidad. 3. Seleccione la pestaña Subredes. Puede encontrar la dirección de la interfaz de red elástica del punto de conexión en cada zona de disponibilidad.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

Compruebe las reglas del firewall y las configuraciones de enrutamiento.	Para confirmar que las reglas del firewall están abiertas y que la red está configurada correctamente, use Telnet para probar el punto de conexión en el puerto 443. Por ejemplo:
	`$ telnet vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com 443`
	`Trying 10.104.88.6...`
	`Connected to vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com.`
	`...`
	`$ telnet vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com 443`
	`Trying 10.104.71.141...`
	`Connected to vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com.`
	Note
	Si usa la entrada regional, una prueba
		Administrador de red, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	correcta mostrará que el DNS alterna entre las dos direcciones IP que puede ver en la pestaña Subredes del punto de conexión seleccionado en la consola de Amazon VPC.	

Tarea	Descripción	Habilidades requeridas
Configure la resolución de nombres.	Debe configurar la resolución de nombres para permitir que Hadoop acceda al punto de conexión de la interfaz Amazon S3. No puede usar el nombre del punto de conexión como tal. En su lugar, debe resolver `<your-bucket-name>.s3.<your-aws-region>.amazonaws.com` o `*.s3.<your-aws-region>.amazonaws.com`. Para obtener más información sobre esta limitación de nombres, consulte Presentación del cliente Hadoop S3A (sitio web de Hadoop). Elija una de las siguientes opciones de configuración: • Use el DNS en las instalaciones para resolver la dirección IP privada del punto de conexión. Puede anular el comportamiento de todos los buckets o de algunos de ellos. Para obtener más información, consulte «Opción 2: acceder a Amazon S3 mediante zonas de política de respuesta del sistema de nombres de dominio	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	(DNS RPZ)» en Acceso híbrido seguro a Amazon S3 mediante AWS PrivateLink (entrada del blog de AWS). • Configure el DNS en las instalaciones para reenviar el tráfico de forma condicional a los puntos de conexión entrantes de la resolución en la VPC. El tráfico se reenvía a Route 53. Para obtener más información, consulte la sección «Opción 3: reenviar solicitudes de DNS desde locales mediante los puntos de enlace entrantes de Amazon Route 53 Resolver» en Acceso híbrido seguro a Amazon S3 mediante AWS (entrada del blog de PrivateLink AWS). • Edite el archivo /etc/hosts en todos los nodos de su clúster de Hadoop. Esta es una solución temporal para realizar pruebas, y no se recomienda su uso en producción. Para editar el archivo /etc/hosts, añada una entrada para `<your-bucket-name>.s3.<your-aws-region>.amazonaws.com`	

Tarea	Descripción	Habilidades requeridas
	o `s3.<your-aws-region>.amazonaws.com` . El archivo /etc/hosts no puede tener varias direcciones IP para una entrada. Debe elegir una única dirección IP de una de las zonas de disponibilidad, que luego se convertirá en un único punto de error.	

Tarea	Descripción	Habilidades requeridas
Configure la autenticación para Amazon S3.	Para autenticarse en Amazon S3 a través de Hadoop, le recomendamos que exporte las credenciales de rol temporales al entorno de Hadoop. Para obtener más información, consulte Autenticación con S3 (sitio web de Hadoop). En trabajos de larga duración, puede crear un usuario y asignar una política con permisos para colocar datos únicament e en un bucket de S3. La clave de acceso y la clave secreta se pueden almacenar en Hadoop, y solo pueden acceder a ellas el propio DistCp trabajo y el administr ador de Hadoop. Para obtener más información sobre el almacenamiento de secretos, consulte Almacenamiento de secretos con los proveedores de credenciales de Hadoop (sitio web de Hadoop). Para obtener más información sobre otros métodos de autenticación, consulte Cómo obtener credenciales de un rol de IAM para su uso con acceso de CLI a una cuenta de AWS en la documentación de AWS IAM Identity Center	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	(sucesor de AWS Single Sign-On).
	
	Para usar credenciales temporales, añada las credenciales temporales a su archivo de credencia les o ejecute los siguientes comandos para exportar las credenciales a su entorno:
	
	`export AWS_SESSI ON_TOKEN=SECRET-SE SSION-TOKEN`
	`export AWS_ACCES S_KEY_ID=SESSION-A CCESS-KEY`
	`export AWS_SECRE T_ACCESS_KEY=SESSION- SECRET-KEY`
	
	Si tiene una combinación de clave de acceso y clave secreta tradicional, ejecute los siguientes comandos:
	
	`export AWS_ACCES S_KEY_ID=my.aws.key`
	`export AWS_SECRE T_ACCESS_KEY=my.se cret.key`
	
	Note
	Si utiliza una combinación de clave de acceso y clave	

Tarea	Descripción	Habilidades requeridas
	secreta, cambie el proveedor de credenciales en los DistCp comandos de a. `"org.apache.hadoop.fs.s3a.TemporaryAWSCredentialsProvider" "org.apache.hadoop.fs.s3a.SimpleAWSCredentialsProvider"`	

Tarea	Descripción	Habilidades requeridas
Transfiera datos mediante DistCp.	Para usarlo DistCp para transferir datos, ejecute los siguientes comandos: `hadoop distcp -Dfs.s3a.aws.credentials.provider=\"org.apache.hadoop.fs.s3a.TemporaryAWSCredentialsProvider" \ -Dfs.s3a.access.key="${AWS_ACCESS_KEY_ID}" \ -Dfs.s3a.secret.key="${AWS_SECRET_ACCESS_KEY}" \ -Dfs.s3a.session.token="${AWS_SESSION_TOKEN}" \ -Dfs.s3a.path.style.access=true \ -Dfs.s3a.connection.ssl.enabled=true \ -Dfs.s3a.endpoint=s3.<your-aws-region>.amazonaws.com \ hdfs:///user/root/ s3a://<your-bucket-name>` **Note** La región de AWS del punto de conexión no se detecta automáticamente cuando se utiliza el DistCp	Ingeniero de migraciones; administrador de AWS

Tarea	Descripción	Habilidades requeridas
	comando con AWS PrivateLink para Amazon S3. Hadoop 3.3.2 y las versiones posteriores resuelven este problema habilitando la opción de establecer de forma explícita la región de AWS del bucket de S3. Para obtener más informaci ón, consulte S3A para añadir la opción fs.s3a.endpoint.region y establecer la región de AWS (sitio web de Hadoop). Para obtener más informaci ón sobre otros proveedores de S3A, consulte Configuración general de cliente S3A (sitio web de Hadoop). Por ejemplo, si usa el cifrado, puede añadir la siguiente opción a la serie de comandos anteriores en función del tipo de cifrado: `-Dfs.s3a.server-si de-encryption-algo rithm=AES-256 [or SSE-C or SSE-KMS]`	

Tarea	Descripción	Habilidades requeridas
	Note Para usar el punto de conexión de la interfaz con S3A, debe crear una entrada de alias de DNS para el nombre regional de S3 (por ejemplo, `s3.<your-aws-region>.amazonaws.com`) en el punto de conexión de la interfaz. Consulte la sección Configurar autenticación para Amazon S3 para obtener más instrucciones. Esta solución alternativa es necesaria para Hadoop 3.3.2 y versiones anteriores. Las versiones futuras de S3A no requieren de esta solución alternativa. Si tiene problemas de firma con Amazon S3, añada una opción para usar Signature Version 4 (SigV4):	

Tarea	Descripción	Habilidades requeridas
	`-Dmapreduce.map.java.opts="-Dcom.amazonaws.services.s3.enableV4=true"`	

Más patrones

- Acceda Servicios de AWS desde IBM z/OS instalando el AWS CLI
- Archivar automáticamente los elementos en Amazon S3 con DynamoDB TTL
- Realice copias de seguridad automáticas de las bases de datos de SAP HANA mediante Systems Manager y EventBridge
- Copia de seguridad y archivo de datos de mainframe en Amazon S3 mediante BMC AMI Cloud Data
- Cree una canalización de servicios de ETL para cargar datos de forma incremental desde Amazon S3 a Amazon Redshift mediante AWS Glue
- Configure el registro de invocación de modelos en Amazon Bedrock mediante AWS CloudFormation
- Convierta y desempaquete datos EBCDIC a ASCII en AWS mediante Python
- Convierta VARCHAR2 (1) el tipo de datos de Oracle en un tipo de datos booleano para Amazon Aurora PostgreSQL
- Cree una definición de tareas de Amazon ECS y monte un sistema de archivos en EC2 las instancias mediante Amazon EFS
- Entregue registros de DynamoDB a Amazon S3 mediante Kinesis Data Streams y Firehose con AWS CDK
- Implementación de un sistema de archivos de Lustre para un procesamiento de datos de alto rendimiento mediante Terraform y DRA
- Costos de almacenamiento estimados para una tabla de Amazon DynamoDB
- Identifique los buckets públicos de Amazon S3 AWS Organizations mediante Security Hub (CSPM)
- Migre un servidor SFTP local para utilizar AWS AWS Transfer for SFTP
- Migración de una tabla particionada de Oracle a PostgreSQL mediante AWS DMS
- Migración de datos de Microsoft Azure Blob a Amazon S3 mediante Rclone
- Migración de valores CLOB de Oracle a filas individuales en PostgreSQL en AWS
- Migre sistemas de archivos compartidos en una migración AWS grande
- Migre pequeños conjuntos de datos del entorno local a Amazon S3 mediante AWS SFTP
- Mover los archivos de mainframe directamente a Amazon S3 mediante Transfer Family
- Elimine EC2 las entradas de Amazon en el mismo Cuenta de AWS AWS Managed Microsoft AD formulario mediante AWS Lambda la automatización

- Ejecutar cargas de trabajo con estado y almacenamiento de datos persistente mediante Amazon EFS en Amazon EKS con AWS Fargate
- Importación correcta de un bucket de S3 como CloudFormation pila de AWS
- Sincronice los datos entre los sistemas de archivos de Amazon EFS en distintas regiones de AWS mediante AWS DataSync
- Vea los detalles de la instantánea de EBS de su cuenta u organización de AWS

Herramientas para desarrolladores

Temas

- DevOps
- infraestructura
- Aplicaciones web y móviles

DevOps

Temas

- Acelere MLOps con las plantillas Backstage y de autoservicio de Amazon AI SageMaker
- Automatice las operaciones de AWS infraestructura con Amazon Bedrock
- Automatice CloudFront las actualizaciones cuando cambien los puntos finales del equilibrador de carga mediante Terraform
- Automatice las CodeGuru revisiones de Amazon para aplicaciones de AWS CDK Python mediante GitHub Actions
- Automatice la implementación de lagos de Supply Chain datos en una configuración de múltiples repositorios
- Automatice la evaluación de recursos de AWS
- Instalar sistemas SAP automáticamente mediante herramientas de código abierto
- Automatice la implementación de productos y la cartera de AWS Service Catalog mediante AWS CDK
- Automatice la gestión dinámica de canalizaciones para implementar soluciones de hotfix en entornos de Gitflow mediante el uso y AWS Service Catalog AWS CodePipeline
- Automatice la eliminación de AWS CloudFormation pilas y recursos asociados
- Automatización de la ingesta y visualización de métricas personalizadas de Amazon MWAA en Amazon Managed Grafana mediante Terraform
- Adjunte automáticamente una política gestionada por AWS para Systems Manager a los perfiles de EC2 instancia mediante Cloud Custodian y AWS CDK
- Cree CI/CD canalizaciones y clústeres de Amazon ECS de forma automática para microservicios mediante AWS CDK
- Cree e inserte imágenes de Docker en Amazon ECR mediante GitHub Actions y Terraform
- Cree y pruebe aplicaciones iOS con AWS CodeCommit CodePipeline, AWS y AWS Device Farm
- Configure autenticación TLS mutua para aplicaciones ejecutadas en Amazon EKS
- Automatice la creación de recursos de Amazon WorkSpaces Applications mediante AWS CloudFormation
- Crear un analizador de registros personalizado para Amazon ECS mediante un enrutador de registros Firelens
- Cree un marco de orquestación de recursos basado en API con GitHub Actions y Terragrunt

- Cree solicitudes de cambios automatizadas para la AWS infraestructura gestionada por Terraform mediante Actions GitHub
- Crear automáticamente canalizaciones de CI dinámicas para proyectos de Java y Python
- Despliega canarios de CloudWatch Synthetics con Terraform
- Implemente una ChatOps solución para gestionar los resultados de los escaneos SAST mediante Amazon Q Developer en aplicaciones de chat, acciones personalizadas y CloudFormation
- Implementación de sistemas de agentes en Amazon Bedrock con el marco CrewAI mediante Terraform
- Implemente un trabajo de AWS Glue con una canalización de CodePipeline CI/CD de AWS
- Implemente código en varias regiones de AWS mediante AWS CodePipeline CodeCommit, AWS y AWS CodeBuild
- Implemente cargas de trabajo desde DevOps canalizaciones de Azure a clústeres privados de Amazon EKS
- Ejecución de consultas SQL en Amazon Redshift mediante Terraform
- Exportación de etiquetas para una lista de instancias de Amazon EC2 a un archivo CSV
- Exportar los informes de AWS Backup de toda la organización en AWS Organizations como un archivo CSV
- Genere una CloudFormation plantilla de AWS que contenga las reglas administradas por AWS Config mediante Troposphere
- Otorgue a las instancias de SageMaker notebook acceso temporal a un CodeCommit repositorio de otra cuenta de AWS
- Implemente una estrategia GitHub de ramificación de Flow para entornos de cuentas múltiples DevOps
- Implementa una estrategia de ramificación de Gitflow para entornos de múltiples cuentas DevOps
- Implemente una estrategia de ramificación troncal para entornos de cuentas múltiples DevOps
- Implemente un escaneo Checkov personalizado y centralizado para aplicar la política antes de implementar AWS la infraestructura
- Implementación de diagnósticos y solución de problemas de Kubernetes con tecnología de IA con la integración de K8sGPT y Amazon Bedrock
- Detecta automáticamente los cambios e inicia diferentes CodePipeline canalizaciones para un monorepo en CodeCommit
- Integre un repositorio de Bitbucket con AWS Amplify mediante AWS CloudFormation

- Lance un CodeBuild proyecto en todas las cuentas de AWS mediante Step Functions y una función de proxy Lambda
- Administración de la conmutación por error de multi-AZ para clústeres de EMR mediante el Controlador de recuperación de aplicaciones
- Gestione blue/green las implementaciones de microservicios en varias cuentas y regiones mediante los servicios de código de AWS y las claves multirregionales de AWS KMS
- Supervise los repositorios de Amazon ECR en busca de permisos comodín mediante AWS y AWS Config CloudFormation
- Optimice las implementaciones sin servidor con varias cuentas mediante los flujos de trabajo y Actions AWS CDK GitHub
- AWS Service Catalog Aprovisione productos en función de AWS CloudFormation plantillas mediante GitHub acciones
- Aprovisionamiento de roles de IAM con privilegio mínimo mediante la implementación de una solución de máquina expendedora de roles
- Publica CloudWatch las métricas de Amazon en un archivo CSV
- Elimine EC2 las entradas de Amazon Cuentas de AWS de un lado a otro AWS Managed Microsoft AD mediante AWS Lambda la automatización
- Elimine EC2 las entradas de Amazon en el mismo Cuenta de AWS AWS Managed Microsoft AD formulario mediante AWS Lambda la automatización
- Ejecute pruebas unitarias para trabajos ETL de Python AWS Glue utilizando el marco pytest
- Configure una CI/CD canalización mediante AWS CodePipeline y AWS CDK
- Configuración del registro centralizado a escala empresarial mediante Terraform
- Configure el end-to-end cifrado para aplicaciones en Amazon EKS mediante cert-manager y Let's Encrypt
- Simplificación de la implementación de aplicaciones multiusuario de Amazon EKS mediante Flux
- Simplificación del desarrollo y la implementación de los bots de Amazon Lex mediante un flujo de trabajo automatizado
- Coordine la dependencia de los recursos y la ejecución de tareas mediante la construcción AWS Fargate WaitCondition hook
- Utilice repositorios de código fuente de Git de terceros en AWS CodePipeline
- Cree una CI/CD canalización para validar las configuraciones de Terraform mediante AWS CodePipeline
- Más patrones

Acelere MLOps con las plantillas Backstage y de autoservicio de Amazon AI SageMaker

Ashish Bhatt, Shashank Hirematt y Shivanshu Suryakar, de Amazon Web Services

Resumen

Las organizaciones que utilizan sistemas de operaciones de aprendizaje automático (MLOps) se enfrentan a importantes desafíos a la hora de escalar, estandarizar y proteger su infraestructura de aprendizaje automático. Este patrón presenta un enfoque transformador que combina Backstage, un portal para desarrolladores de código abierto, con Amazon SageMaker AI y módulos reforzados de infraestructura como código (IaC) para mejorar la forma en que sus equipos de ciencia de datos pueden desarrollar, implementar y gestionar los flujos de trabajo de aprendizaje automático.

Los módulos de IaC para este patrón se proporcionan en el repositorio de módulos. GitHub AWS AIOps Estos módulos ofrecen plantillas prediseñadas para configurar la infraestructura de ML y crear entornos de ML coherentes. Sin embargo, los científicos de datos a menudo tienen dificultades para usar estas plantillas directamente porque requieren tener experiencia en infraestructura. Al añadir un portal para desarrolladores como Backstage, los científicos de datos pueden implementar entornos de ML estandarizados de forma sencilla sin necesidad de comprender los detalles de la infraestructura subyacente.

Al utilizar Backstage como plataforma de autoservicio e integrar plantillas de SageMaker IA preconfiguradas, puede:

- Acelerar la rentabilidad de sus iniciativas de ML.
- Garantizar una seguridad y una gobernanza coherentes.
- Proporcionar a los científicos de datos entornos estandarizados y que cumplan con las normas.
- Reducir los gastos operativos y la complejidad de la infraestructura.

Este patrón proporciona una solución que aborda los desafíos críticos MLOps y también proporciona un marco escalable y repetible que permite la innovación y, al mismo tiempo, mantiene los estándares organizacionales.

Público objetivo

Este patrón está dirigido a una amplia audiencia relacionada con el ML, la arquitectura de nube y la ingeniería de plataformas dentro de una organización. Esto incluye:

- Ingenieros de ML que desean estandarizar y automatizar las implementaciones de flujos de trabajo de ML.
- Científicos de datos que desean obtener acceso de autoservicio a entornos de ML preconfigurados y que cumplan con las normas.
- Ingenieros de plataformas que se encargan de crear y mantener las plataformas internas para desarrolladores y la infraestructura compartida.
- Arquitectos de nube que diseñan soluciones de nube escalables, seguras y rentables para MLOps.
- DevOps ingenieros interesados en extender las prácticas de integración continua y entrega continua (CI/CD) al aprovisionamiento de infraestructuras y flujos de trabajo de aprendizaje automático.
- Gerentes y directores técnicos que supervisan las iniciativas de ML y desean mejorar la productividad del equipo, la gobernanza y el tiempo de comercialización.

Para obtener más información sobre MLOps los desafíos, los MLOps módulos de SageMaker IA y cómo la solución proporcionada por este patrón puede satisfacer las necesidades de sus equipos de aprendizaje automático, consulte la sección de información adicional.

Requisitos previos y limitaciones

Requisitos previos

- AWS Identity and Access Management Funciones y permisos (IAM) para aprovisionar recursos en su Cuenta de AWS
- Comprensión de los conceptos de Amazon SageMaker Studio, SageMaker Projects, SageMaker Pipelines y SageMaker Model Registry
- Comprensión de los principios de IaC y experiencia con herramientas como AWS Cloud Development Kit (AWS CDK)

Limitaciones

- Cobertura limitada de plantillas. Actualmente, la solución solo admite los AIOps módulos SageMaker relacionados con la IA de la solución más ampliaAIOps . Otros módulos, como Ray en Amazon Elastic Kubernetes Service (Amazon EKS), MLflow Apache Airflow y el ajuste de precisión para Amazon Bedrock, aún no están disponibles como plantillas de Backstage.
- Ajustes predeterminados no configurables. Las plantillas utilizan configuraciones predeterminadas fijas de los módulos sin personalización. AIOps SageMaker No puede modificar los tipos de

instancias, los tamaños de almacenamiento, las configuraciones de red ni las políticas de seguridad mediante la interfaz Backstage, lo que limita la flexibilidad en casos de uso específicos.

- solo admite AWS. La plataforma está diseñada exclusivamente para AWS despliegues y no admite escenarios multinube. Organizations que utilizan servicios en la nube de forma externa Nube de AWS no pueden usar estas plantillas para sus necesidades de infraestructura de aprendizaje automático.
- Administración de credenciales manual Debe proporcionar sus AWS credenciales de forma manual para cada implementación. Esta solución no proporciona la integración con los proveedores de identidad corporativa ni la rotación automática de credenciales. AWS IAM Identity Center
- Administración del ciclo de vida limitado. Las plantillas carecen de funciones integrales de gestión del ciclo de vida de los recursos, como políticas de limpieza automatizadas, recomendaciones de optimización de costes y detección de desviaciones en la infraestructura. Debe gestionar y supervisar manualmente los recursos implementados tras su creación.

Arquitectura

El siguiente diagrama muestra la arquitectura de la solución para un portal de desarrolladores unificado que estandariza y acelera la implementación de la infraestructura de aprendizaje automático con SageMaker IA en todos los entornos.

En esta arquitectura:

1. AWS los planes de modernización de aplicaciones proporcionan la configuración de la infraestructura con un clúster de Amazon EKS como base para el marco Cloud Native Operational Excellence (CNOE). Esta solución integral aborda los complejos desafíos de administración de la infraestructura nativa en la nube al proporcionar una plataforma de desarrollador interna (IDP) escalable. Los esquemas ofrecen un enfoque estructurado para configurar una infraestructura sólida y flexible que pueda adaptarse a las cambiantes necesidades organizativas.
2. El marco de código abierto CNOE consolida las DevOps herramientas y resuelve la fragmentación del ecosistema mediante un enfoque unificado de ingeniería de plataformas. Al reunir herramientas y tecnologías dispares, simplifica el complejo panorama del desarrollo nativo en la nube para que sus equipos puedan centrarse en la innovación en lugar de en la gestión de la cadena de herramientas. El marco proporciona una metodología estandarizada para seleccionar, integrar y gestionar las herramientas de desarrollo.

3. Con CNOE, Backstage se implementa como una out-of-the-box solución dentro del clúster de Amazon EKS. Backstage incluye una autenticación sólida a través de Keycloak y flujos de trabajo de implementación integrales a través de Argo CD. Esta plataforma integrada crea un entorno centralizado para gestionar los procesos de desarrollo y proporciona un único lugar para que los equipos accedan, implementen y supervisen su infraestructura y aplicaciones en varios entornos.
4. Un GitHub repositorio contiene plantillas de AIOps software preconfiguradas que cubren todo SageMaker el ciclo de vida de la IA. Estas plantillas abordan las necesidades críticas de infraestructura de aprendizaje automático, como el aprovisionamiento de SageMaker Studio, la formación de modelos, los procesos de inferencia y la supervisión de modelos. Estas plantillas lo ayudan a acelerar sus iniciativas de ML y a garantizar la coherencia entre los distintos proyectos y equipos.
5. GitHub Actions implementa un flujo de trabajo automatizado que activa de forma dinámica el aprovisionamiento de recursos mediante la utilidad Seed-Farmer. Este enfoque integra el catálogo de Backstage con el repositorio de AIOps módulos y crea un proceso de despliegue de infraestructura simplificado. La automatización reduce las intervenciones manuales, minimiza los errores humanos y garantiza que la infraestructura se cree de forma rápida y coherente en los distintos entornos.
6. AWS CDK lo ayuda a definir y aprovisionar la infraestructura como código, y garantiza una implementación de recursos repetible, segura y compatible en todas las Cuentas de AWS especificadas. Este enfoque proporciona el máximo control con una intervención manual mínima, de modo que puede crear plantillas de infraestructura estandarizadas que se puedan replicar y auditar fácilmente y con versiones que pueda controlar.

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir y aprovisionar la Nube de AWS infraestructura en código.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar AWS Kubernetes sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.
- Amazon SageMaker AI es un servicio de aprendizaje automático gestionado que le ayuda a crear y entrenar modelos de aprendizaje automático y, a continuación, implementarlos en un entorno hospedado listo para la producción.

Otras herramientas

- Backstage es un marco de código abierto que lo ayuda a crear portales internos para desarrolladores.
- GitHub Actions es una CI/CD plataforma que automatiza los flujos de trabajo de desarrollo de software, incluidas tareas como la creación, las pruebas y la implementación de código.

Repositorios de código

Este patrón utiliza código y plantillas de los siguientes GitHub repositorios:

- AIOps plataforma interna para desarrolladores (IDP) con repositorio Backstage
- SageMaker Módulos relacionados con la IA del repositorio de módulos AWS AIOps
- Ingeniería moderna en el repositorio AWS

Implementación

Esta implementación utiliza un patrón de implementación de nivel de producción para Backstage del repositorio Ingeniería moderna en AWS. Este enfoque simplifica considerablemente el proceso de configuración e incorpora las AWS mejores prácticas de seguridad y escalabilidad.

La sección Epics de este patrón describe el enfoque de implementación. Para obtener instrucciones de step-by-step implementación detalladas, consulte la guía de implementación completa disponible en la plataforma AIOps interna para desarrolladores (IDP) con el repositorio Backstage. La implementación incluye:

- Implementación inicial de la plataforma de Backstage
- Integración de plantillas de SageMaker software con Backstage
- Consumo y mantenimiento de plantillas de Backstage

La guía de implementación también incluye instrucciones para el mantenimiento continuo, solución de problemas y escalado de la plataforma.

Prácticas recomendadas

Siga estas mejores prácticas para garantizar la seguridad, la gobernanza y la excelencia operativa en sus implementaciones de MLOps infraestructura.

Administración de plantillas

- Nunca realice cambios importantes en las plantillas activas.
- Pruebe siempre las actualizaciones minuciosamente antes de implementarlas en la producción.
- Mantenga versiones de plantillas claras y bien documentadas.

Seguridad

- Fije GitHub las acciones a algoritmos de hash seguros y específicos (SHAs) para ayudar a prevenir los ataques a la cadena de suministro.
- Use roles de IAM con privilegios mínimos y permisos granulares.
- Guarde las credenciales confidenciales en GitHub Secrets y AWS Secrets Manager.
- Nunca codifique las credenciales de forma rígida en las plantillas.

Gobernanza y seguimiento

- Implemente estándares integrales de etiquetado de recursos.
- Permita un seguimiento preciso de los costos y la supervisión del cumplimiento.
- Mantenga registros de auditoría claros para detectar los cambios en la infraestructura.

Esta guía proporciona una base sólida para implementar estas mejores prácticas mediante el uso de los módulos Backstage, SageMaker AI e IaC.

Epics

Configure su entorno de ML

Tarea	Descripción	Habilidades requeridas
Implementación de Backstage.	En este paso, se utilizan los planos del AWS repositor io Modern Engineering on para crear una infraestr uctura sólida y escalable que integre múltiples component es a fin de crear un IDP	Ingeniería de plataformas

Tarea	Descripción	Habilidades requeridas
	centralizado Servicios de AWS para los flujos de trabajo de aprendizaje automático. Siga las instrucciones de la sección de implementación de Backstage de la guía de implementación para clonar el repositorio, instalar las dependencias, iniciar la AWS CDK configuración de las variables de entorno e implementar la plataforma Backstage. La infraestructura utiliza Amazon EKS como plataforma de orquestación de contenedores para implementar componentes de IDP. La arquitectura de Amazon EKS incluye configuraciones de red seguras para establecer patrones estrictos de acceso y aislamiento de la red. La plataforma se integra con los mecanismos de autenticación para que pueda proteger el acceso de los usuarios a todos los servicios y entornos.	

Tarea	Descripción	Habilidades requeridas
Configura tus plantillas de IA. SageMaker	En este paso, se utilizan los scripts de la plataforma GitHub AIOps interna para desarrolladores (IDP) con el repositorio de Backstage. Siga las instrucciones de la sección de configuración de SageMaker plantillas de la guía de implementación para clonar el repositorio, configurar los requisitos previos y ejecutar el script de configuración. Este proceso crea un repositorio que contiene las plantillas de SageMaker IA necesarias para la integración con Backstage.	Ingeniería de plataformas

Tarea	Descripción	Habilidades requeridas
Integre las plantillas de SageMaker IA con Backstage.	Siga las instrucciones de la sección de integración de SageMaker plantillas de la guía de implementación para registrar sus plantillas de SageMaker IA. Este paso integra los AIOps módulos (plantillas de SageMaker IA del último paso) en su implementación de Backstage para que pueda satisfacer sus necesidades de infraestructura de aprendiza je automático de manera autónoma.	Ingeniería de plataformas

Tarea	Descripción	Habilidades requeridas
Usa las plantillas de SageMaker IA de Backstage.	Siga las instrucciones de la sección Uso de SageMaker plantillas de la guía de implementación para acceder al portal de Backstage y crear el entorno de aprendizaje automático en SageMaker Studio. En el portal de Backstage , puedes seleccionar entre las plantillas de SageMaker IA disponibles, incluidas opciones para entornos de SageMaker Studio, SageMaker libretas, plantilla s de SageMaker proyectos personalizadas y procesos de implementación de modelos. Tras proporcionar los parámetros de configura ción, la plataforma crea repositorios dedicados automáticamente y aprovisio na los AWS recursos a través GitHub de Actions y Seed-Farmer. Puede supervisa r el progreso mediante los registros de GitHub acciones y el catálogo de componentes de Backstage.	Científico de datos, ingeniero de datos, desarrollador

Administración de las plantillas para la gobernanza y el cumplimiento

Tarea	Descripción	Habilidades requeridas
Actualice las plantillas de SageMaker IA.	Para actualizar una plantilla de SageMaker IA en Backstage, sigue estos pasos. 1. Modifique el contenido de la plantilla: a. Realice los cambios necesarios en el archivo `template.yaml` o edite los archivos del directorio `skeleton/` . b. Pruebe los nuevos parámetros, acciones o estructuras de archivos de forma local o en un entorno de desarrollo. 2. Pruebe los cambios: a. Utilice la interfaz de usuario o la CLI (`@backstage/create-app`) de Backstage para estructurar un componente de prueba mediante la plantilla actualizada. b. Confirme que todos los pasos se ejecuten correctamente y que el código generado cumpla con sus expectativas. 3. Confirme y envíe los cambios.	Ingeniería de plataformas

Tarea	Descripción	Habilidades requeridas
	a. Envíe los cambios al repositorio de Git donde se almacena la plantilla. Si la plantilla está registrada en una rama específica (por ejemplo, `main`), las actualizaciones se reflejarán automáticamente. b. Si utiliza el control de versiones (consulte el siguiente paso), asegúrese de que se haya actualizado la versión o etiqueta correcta.	

Tarea	Descripción	Habilidades requeridas

Cree y administre varias versiones de una plantilla.	Para realizar cambios o mejoras importantes, es posible que desees crear varias versiones de una plantilla de SageMaker IA.
	
	1. Use etiquetas o ramas de Git para cada versión; por ejemplo:
	
	`git checkout -b v2.0.0`
	`git push origin v2.0.0`
	
	2. (Opcional pero recomendado) Registre cada versión por separado.
	
	En Backstage, puede registrar diferentes versiones de una plantilla como entidades independientes en el catálogo, donde cada entidad apunta a una rama o etiqueta específica. Por ejemplo (para un archivo `.yaml`):
	
	`metadata:`
	`name: node-service-template-v2`
	`description: Node.js service template - Version 2`
	`spec:`
	`type: template`
	`lifecycle: experimental`
		Ingeniería de plataformas

Tarea	Descripción	Habilidades requeridas
	`version: '2.0.0'` 3. Comunique los cambios con claridad mantenien do un archivo `CHANGELOG .md` en el repositorio de plantillas. En este archivo, se documenta qué características o cambios se introdujeron en cada versión de la plantilla. 4. Si es necesario, desactive las versiones anteriores de la plantilla: a. Márquela como obsoleta en la descripción de la plantilla. b. Elimine la versión del catálogo si ya no es necesaria.	

Amplíe su entorno de ML

Tarea	Descripción	Habilidades requeridas
Amplía la cobertura de plantillas más allá de la SageMaker IA.	La solución actual solo implementa AIOps plantilla s SageMaker relacionadas con la IA. Puede ampliar el entorno de aprendiza je automático añadiendo AIOps módulos e integrando plantillas de software personali zadas para aplicaciones	Ingeniería de plataformas

Tarea	Descripción	Habilidades requeridas
	Servicios de AWS y aplicaciones adicionales. Puede crear estos elementos mediante la interfaz de diseño de plantillas de Backstage; solo tiene que implementar acciones de scaffolder personalizadas o mantener los repositorios de plantillas con metadatos estándar. La plataforma admite el control de versiones de plantillas, el uso compartido entre equipos y los flujos de trabajo de validación para garantizar la coherencia. Para obtener más información, consulte la documentación de Backstage. También puede implementar patrones de herencia de plantillas para crear versiones especializadas de plantillas base. Esta extensibilidad le permite administrar diversos AWS recursos y aplicaciones además de la SageMaker IA, al tiempo que conserva la experiencia simplificada de los desarrolladores y mantiene los estándares de su organización.	

Tarea	Descripción	Habilidades requeridas
Utilice la inyección dinámica de parámetros.	Las plantillas actuales utilizan configuraciones predeterminadas sin personalización y ejecutan la CLI de Seed-Farmer para implementar recursos con variables predeterminadas. Puede ampliar la configuración predeterminada mediante la inyección dinámica de parámetros para las configuraciones específicas del módulo.	Ingeniería de plataformas
Mejore la seguridad y conformidad.	Para mejorar la seguridad en la creación de los recursos de AWS, puede habilitar la integración del control de acceso basado en roles (RBAC) con el inicio de sesión único (SSO), SAML, OpenID Connect (OIDC) y políticas como la aplicación del código.	Ingeniería de plataformas
Añada una limpieza de recursos automatizada.	Puede habilitar características para políticas de limpieza automatizadas y, además, añadir funciones de detección y corrección de desviaciones en la infraestructura.	Ingeniería de plataformas

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Elimine la infraestructura de Backstage y los recursos de SageMaker IA.	Cuando haya terminado de usar su entorno de aprendizaje automático, siga las instrucciones de la sección Limpieza y administración de recursos de la guía de implementación para eliminar la infraestructura de Backstage y eliminar los recursos de SageMaker IA de su entorno de aprendizaje automático.	Ingeniería de plataformas

Resolución de problemas

Problema	Solución
AWS CDK errores de arranque	Compruebe AWS las credenciales y la configuración de la región.
Problemas de acceso al clúster de Amazon EKS	Compruebe la configuración de kubectl y los permisos de IAM.
Problemas de conectividad del equilibrador de carga de aplicación	Asegúrese de que los grupos de seguridad permitan el tráfico entrante en el puerto 80/443.
GitHub problemas de integración	Verifique los permisos de los GitHub tokens y el acceso a la organización.
SageMaker Fallos de implementación de la IA	Compruebe las cuotas de Servicio de AWS y los permisos de IAM.

Recursos relacionados

- Ingeniería de plataformas (en la guía Cloud Adoption Framework de AWS : perspectiva de las plataformas)
- Documentación de Amazon SageMaker AI
- Plantillas de software de Backstage (sitio web de Backstage)
- AIOps repositorio de módulos (colección de módulos iAC reutilizables para ML)
- AIOps plataforma interna para desarrolladores (IDP) con repositorio Backstage
- Ingeniería moderna en el repositorio AWS
- Sitio web de excelencia operativa nativa en la nube (CNOE)

Información adicional

Retos empresariales.

Las organizaciones que se embarcan en sus MLOps iniciativas o las amplían con frecuencia se enfrentan a los siguientes desafíos empresariales y técnicos:

- Entornos incoherentes. La falta de entornos de desarrollo e implementación estandarizados dificulta la colaboración y aumenta los riesgos de implementación.
- Gastos generales de aprovisionamiento manual. La configuración manual de una infraestructura de aprendizaje automático con SageMaker Studio, los depósitos de Amazon Simple Storage Service (Amazon S3), las funciones de IAM y las canalizaciones lleva mucho tiempo CI/CD y es propensa a errores, y desvía a los científicos de datos de su tarea principal de desarrollar modelos.
- Falta de capacidad de descubrimiento y reutilización. La falta de un catálogo centralizado dificulta la búsqueda de los modelos, conjuntos de datos y canalizaciones de ML existentes. Esto lleva a que el trabajo sea redundante y a que se pierdan oportunidades de reutilización.
- Gobernanza y cumplimiento complejos. Garantizar que los proyectos de ML cumplan con las políticas de seguridad organizacionales, las normas de privacidad de datos y los estándares de cumplimiento como la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA) y el Reglamento General de Protección de Datos (GDPR) puede ser un desafío sin barreras de protección automatizadas.
- Reduzca el tiempo para generar valor. El efecto acumulativo de estos desafíos se traduce en ciclos de vida prolongados de los proyectos de ML y retrasa la obtención del valor empresarial derivado de las inversiones en ML.

- Riesgos de seguridad. Las configuraciones incoherentes y los procesos manuales pueden introducir vulnerabilidades de seguridad que dificultan la aplicación de los privilegios mínimos y el aislamiento de la red.

Estos problemas prolongan los ciclos de desarrollo, aumentan la sobrecarga operativa e introducen riesgos de seguridad. La naturaleza iterativa del ML requiere flujos de trabajo repetibles y una colaboración eficiente.

Gartner prevé que para 2026, el 80 % de las organizaciones de ingeniería de software contarán con equipos de plataformas. (Consulte Platform Engineering Empowers Developers to be Better, Faster, Happier [Cómo la ingeniería de plataformas permite a los desarrolladores ser mejores, más rápidos y más felices] en el sitio webde Gartner). Esta predicción destaca cómo un IDP puede acelerar la entrega de software. Como IDP, Backstage ayuda a restablecer el orden en una infraestructura compleja para que los equipos puedan entregar código de alta calidad de forma rápida y segura. La integración de Backstage con AIOps módulos reforzados le ayuda a pasar de la solución de problemas reactiva a la prevención proactiva.

MLOps SageMaker módulos

Los AIOps módulos del GitHub repositorio utilizados para este patrón proporcionan una base valiosa para la estandarización AWS mediante la MLOps IaC reforzada y reutilizable. Estos módulos resumen las mejores prácticas para el aprovisionamiento de SageMaker proyectos, canalizaciones y recursos de red y almacenamiento asociados, con el objetivo de reducir la complejidad y acelerar la configuración de los entornos de aprendizaje automático. Puede usar estas plantillas para varios casos de MLOps uso a fin de establecer patrones de implementación consistentes y seguros que fomenten un enfoque más gobernado y eficiente de los flujos de trabajo de aprendizaje automático.

El uso directo de AIOps los módulos suele requerir que los equipos de plataformas implementen y administren estas plantillas de IaC, lo que puede suponer un desafío para los científicos de datos que desean un acceso de autoservicio. Para descubrir y comprender las plantillas disponibles, configurar los parámetros necesarios y activar su implementación, es posible que sea necesario navegar por las Servicio de AWS consolas o interactuar directamente con las herramientas de la iAc. Esto puede generar fricciones, aumentar la carga cognitiva de los científicos de datos que prefieren centrarse en tareas de ML y, si estas plantillas no se gestionan a través de una interfaz centralizada y fácil de usar, puede provocar una parametrización incoherente o desviarse de los estándares de la organización. La integración de estos potentes AIOps módulos con un IDP como Backstage ayuda a abordar estos desafíos, ya que proporciona una experiencia de autoservicio optimizada, una mayor

capacidad de detección y controles de gobierno más sólidos para utilizar estos componentes básicos estandarizados. MLOps

Backstage como IDP

Una plataforma interna para desarrolladores (IDP) es una capa de autoservicio creada por equipos de plataformas para simplificar y estandarizar la forma en que los desarrolladores crean, implementan y administran las aplicaciones. Abstrae la complejidad de la infraestructura y proporciona a los desarrolladores acceso fácil a las herramientas, entornos y servicios a través de una interfaz unificada.

El objetivo principal de un IDP es mejorar la experiencia y la productividad de los desarrolladores mediante las siguientes acciones:

- Habilitar el autoservicio para tareas como la creación e implementación de servicios.
- Promover la coherencia y el cumplimiento mediante plantillas estándar.
- Integrar herramientas en todo el ciclo de vida del desarrollo (CI/CD, supervisión y documentación).

Backstage es un portal para desarrolladores de código abierto creado por Spotify y que ahora forma parte de Cloud Native Computing Foundation (CNCF). Ayuda a las organizaciones a crear su propio IDP, ya que proporciona una plataforma centralizada y ampliable para administrar los componentes, las herramientas y la documentación del software. Con Backstage, los desarrolladores pueden hacer lo siguiente:

- Descubrir y gestionar todos los servicios internos a través de un catálogo de software.
- Crear nuevos proyectos mediante plantillas predefinidas a través del complemento scaffolder.
- Acceda a herramientas integradas, como CI/CD canalizaciones, paneles de Kubernetes y sistemas de monitoreo, desde un solo lugar.
- Mantenga una documentación coherente y basada en rebajas en todo momento. TechDocs

Preguntas frecuentes

¿Cuál es la diferencia entre usar esta plantilla de Backstage y desplegar SageMaker Studio manualmente a través de la consola? SageMaker

La plantilla Backstage ofrece varias ventajas en comparación con el despliegue manual de la AWS consola, como las configuraciones estandarizadas que siguen las mejores prácticas de la

organización, el despliegue automatizado del iAC con Seed-Farmer y las políticas de seguridad integradas y las medidas de cumplimiento AWS CDK, y la integración mediante los flujos de trabajo de los desarrolladores de la organización. GitHub La plantilla también crea implementaciones reproducibles con control de versiones, lo que facilita la replicación de los entornos en diferentes etapas (desarrollo, puesta en marcha, producción) y mantiene la coherencia entre los equipos. Además, la plantilla incluye funciones de limpieza automatizadas y se integra con el sistema de gestión de identidades de su organización a través de Backstage. El despliegue manual a través de la consola requiere una AWS amplia experiencia y no proporciona el control de versiones ni el mismo nivel de estandarización y gobernanza que ofrece la plantilla. Por estas razones, las implementaciones de consola son más adecuadas para realizar experimentos puntuales que los entornos de producción de ML.

¿Qué es Seed-Farmer y por qué lo utiliza esta solución?

Seed-Farmer es una herramienta de organización de AWS despliegues que gestiona los módulos de infraestructura mediante el. AWS CDK Este patrón utiliza Seed-Farmer porque proporciona componentes de infraestructura estandarizados y reutilizables que están diseñados específicamente para las AI/ML cargas de trabajo, gestiona Servicios de AWS automáticamente las complejas dependencias entre ellos y garantiza despliegues consistentes en diferentes entornos.

¿Necesito instalar el para usar estas plantillas? AWS CLI

No, no es necesario que lo instales AWS CLI en tu ordenador. Las plantillas se ejecutan íntegramente a través de GitHub Actions en la nube. AWS Las credenciales (clave de acceso, clave secreta y token de sesión) se proporcionan a través de la interfaz de Backstage y el despliegue se realiza automáticamente en el entorno de GitHub Actions.

¿Cuánto tiempo se tarda en implementar un entorno de SageMaker Studio?

Una implementación típica de SageMaker Studio tarda entre 15 y 25 minutos en completarse. Esto incluye el AWS CDK arranque (de 2 a 3 minutos), la configuración de la cadena de herramientas de Seed-Farmer (de 3 a 5 minutos) y la creación de recursos (de 10 a 15 minutos). El tiempo exacto depende de su configuración de red Región de AWS y de la complejidad de la misma.

¿Puedo implementar varios SageMaker entornos en el mismo Cuenta de AWS?

Sí, puede. Cada implementación crea recursos con nombres únicos en función del nombre del componente que proporcione en la plantilla. Sin embargo, tenga en cuenta las Servicio de AWS cuotas: cada cuenta puede tener un número limitado de SageMaker dominios por región, así que compruebe sus cuotas antes de crear varios entornos.

Automatice las operaciones de AWS infraestructura con Amazon Bedrock

Ishwar Chauthaiwale y Anand Bukkapatnam Tirumala, Amazon Web Services

Resumen

En las soluciones nativas en la nube, la automatización de las operaciones de infraestructura comunes desempeña un papel fundamental a la hora de mantener entornos eficientes, seguros y rentables. La gestión manual de las operaciones lleva mucho tiempo y es propensa a errores humanos. Además, los miembros del equipo con distintos niveles de AWS experiencia deben realizar estas tareas y, al mismo tiempo, garantizar el cumplimiento de los protocolos de seguridad. Este patrón demuestra cómo usar Amazon Bedrock para automatizar las operaciones de AWS infraestructura comunes mediante el procesamiento del lenguaje natural (NLP).

Este patrón puede ayudar a las organizaciones a desarrollar código reutilizable, modular y seguro para implementar una infraestructura basada en IA generativa en varios entornos. Al centrarse en la infraestructura como código (IaC) y en la automatización, ofrece DevOps beneficios clave, como el control de versiones, las implementaciones coherentes, la reducción de los errores, el aprovisionamiento más rápido y la mejora de la colaboración.

El patrón implementa una arquitectura segura que permite a los equipos gestionar las operaciones relacionadas con aspectos clave, entre los que se incluyen: Servicios de AWS

- Administración del control de versiones para un bucket de Amazon Simple Storage Service (Amazon S3)
- Creación de instantáneas de Amazon Relational Database Service (Amazon RDS)
- Administración de instancias de Amazon Elastic Compute Cloud (Amazon EC2)

La arquitectura emplea puntos finales de Amazon Virtual Private Cloud (Amazon VPC) y redes privadas para una comunicación segura, con AWS Lambda funciones que funcionan como ejecutores de tareas dentro de subredes privadas. Amazon S3 proporciona administración de datos e implementa funciones y permisos integrales AWS Identity and Access Management (IAM) para garantizar los controles de acceso adecuados. Esta solución no incluye una característica de historial de chat y el chat no se almacena.

Requisitos previos y limitaciones

- Un activo Cuenta de AWS.

- Deben existir medidas de control de acceso adecuadas para proteger y controlar el acceso. Algunos ejemplos de control de acceso incluyen el uso AWS Systems Manager de modelos básicos de acceso, una función de IAM para la implementación y funciones basadas en servicios, la inhabilitación del acceso público a los buckets de Amazon S3 y la configuración de una cola de espera.
- Una () clave gestionada por el cliente. AWS Key Management ServiceAWS KMS
- AWS Command Line Interface (AWS CLI) versión 2 o posterior, instalada y configurada en el entorno de implementación.
- Instalación y configuración de Terraform AWS Provider, versión 4 o posterior.
- La versión 1.5.7 o posterior de Terraform instalada y configurada.
- Revise y defina los esquemas de OpenAPI para los grupos de acciones del agente en Amazon Bedrock para protegerse del acceso no autorizado y mantener la integridad de los datos.
- El acceso está habilitado en su Cuenta de AWS dispositivo para los modelos Amazon Titan Text Embeddings v2 necesarios y para los modelos de base Claude 3.5 Sonnet o Claude 3 Haiku. Para evitar errores en la implementación, confirme que la implementación de destino es compatible con los modelos requeridos Región de AWS .
- Una nube privada virtual (VPC) configurada que sigue las prácticas recomendadas de AWS Well Architected Framework.
- Revisión completa de la política de IA responsable de Amazon.

Versiones de producto

- Amazon Titan Text Embeddings V2
- Anthropic Claude 3.5 Sonnet or Claude 3 Haiku
- Terraform AWS Provider versión 4 o posterior
- Terraform versión 1.5.7 o posterior

Arquitectura

En el siguiente diagrama se muestran los componentes de la arquitectura y el flujo de trabajo de esta aplicación.

La arquitectura de la solución consta de varias capas que funcionan juntas para procesar las solicitudes en lenguaje natural y ejecutar las operaciones correspondientes AWS :

1. El usuario realiza solicitudes de operaciones a través de la consola de chat de Amazon Bedrock.
2. El chatbot utiliza las bases de conocimiento de Amazon Bedrock para procesar las solicitudes. Implementa el modelo Amazon Titan Text Embeddings v2 para el procesamiento del lenguaje natural.
3. Si la petición del usuario incluye una solicitud de acción, el grupo de acción de Amazon Bedrock utiliza el modelo Anthropic Claude 3 Haiku o Claude 3.5 Sonnet (según su elección) como lógica de ejecución y define las operaciones mediante un esquema OpenAPI.
4. El grupo de acción llega a los puntos de conexión de Amazon VPC mediante una comunicación AWS PrivateLink de servicio segura.
5. Se accede a la AWS Lambda función a través de los puntos de conexión de Amazon VPC para los servicios de Amazon Bedrock.
6. Las funciones de Lambda son el motor de ejecución principal. Según la solicitud, la función de Lambda llama a la API para realizar acciones en los Servicios de AWS. La función de Lambda también gestiona el enrutamiento y la ejecución de las operaciones.
7. Se Servicios de AWS realizan la solicitud de obtención de la API de la función Lambda y las operaciones correspondientes.
8. La función de Lambda calcula una carga útil de salida que Amazon Bedrock entiende.
9. Esta carga útil se envía a Amazon Bedrock mediante una comunicación PrivateLink de servicio segura. El modelo de lenguaje de gran tamaño (LLM) que usa Amazon Bedrock comprende esta carga útil y la convierte en un formato comprensible para las personas.
10. A continuación, el resultado se muestra al usuario en la consola de chat de Amazon Bedrock.

La solución permite las siguientes operaciones principales:

- Amazon S3: permite habilitar el control de versiones en bucket.
- Amazon RDS: permite crear instantáneas de bases de datos para realizar copias de seguridad.
- Amazon EC2: permite enumerar las instancias y controlar el inicio y la parada de estas.

Tools (Herramientas)

Servicios de AWS

- Amazon Bedrock es un servicio totalmente gestionado que pone a su disposición modelos básicos de alto rendimiento (FMs) de las principales empresas emergentes de IA y Amazon a través de una API unificada.

- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar Servicios de AWS mediante comandos en su consola de línea de comandos.
- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon OpenSearch Serverless es una configuración sin servidor bajo demanda para Amazon OpenSearch Service.
- AWS PrivateLinkle ayuda a crear conexiones unidireccionales y privadas desde sus nubes privadas virtuales (VPCs) a servicios externos a la VPC.
- Amazon Relational Database Service (Amazon RDS) lo ayuda a configurar, utilizar y escalar una base de datos relacional en la Nube de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Systems Manager lo ayuda a administrar las aplicaciones y la infraestructura que se ejecutan en la Nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo necesario para detectar y resolver problemas operativos y le ayuda a administrar sus AWS recursos de forma segura y a escala.
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Otras herramientas

- Git es un sistema de control de versiones distribuido y de código abierto.
- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.

Repositorio de código

El código de este patrón está disponible en el repositorio aws-samples/. GitHub infra-ops-orchestrator

Prácticas recomendadas

- Supervise los registros de ejecución de Lambda con regularidad. Para obtener más información, consulte Supervisión y solución de problemas de funciones de Lambda. Para obtener más información sobre las prácticas recomendadas, consulte Prácticas recomendadas para trabajar con funciones. AWS Lambda
- Revise las configuraciones de seguridad periódicamente para garantizar la conformidad con los requisitos de su organización. Para más información, consulte Prácticas recomendadas de seguridad.
- Siga el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Implementar la solución

Tarea	Descripción	Habilidades requeridas

Clonar el repositorio.	Para clonar un repositorio en su máquina local, ejecute el siguiente comando:
	`git clone "git@github.com:aws-samples/infra-ops-orchestrator.git"`
	`cd infra-ops-orchestrator`
		AWS DevOps, DevOps ingeniero

Edite las variables de entorno.	Edite el archivo `terraform.tfvars` en el directorio raíz del repositorio clonado. Revise los marcadores de posición	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	indicados por `[XXXXX]` y actualícelos según su entorno.	

Cree la infraestructura.	Para crear la infraestructura, ejecute los comandos siguientes:
	`terraform init`
	`terraform plan`
	Revise el plan de ejecución detenidamente. Si los cambios planificados son aceptables, ejecute el comando siguiente:
	`terraform apply --auto-approve`
		AWS DevOps, DevOps ingeniero

Acceso a la solución

Tarea	Descripción	Habilidades requeridas
Acceda a la solución.	Tras una implementación correcta, siga estos pasos para utilizar la interfaz basada en el chat: 1. Para acceder a Infrastructure Orchestrator Assistant, inicie sesión en el rol de Consola de administración de AWS uso de un IAM con los permisos de Amazon	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Bedrock y abra la consola de Amazon Bedrock en. https://console.aws.amazon.com/bedrock/ En el panel de navegación de la izquierda, seleccione Agentes. A continuación, elija el Asistente orquestador de infraestructuras en la sección Agentes. 2. Asegúrese de que los recursos de destino existan en su AWS entorno para las siguientes sugerencias y, a continuación, pruebe estas operaciones de ejemplo: • Cree una copia de seguridad de una instancia de Amazon RDS solicitando lo siguiente: Crea una instantánea de la instancia de RDS [instance-name]. • Para habilitar el control de versiones en un bucket de Amazon S3, solicite lo siguiente: Habilita el control de versiones para el bucket [nombre del depósito]. • Enumere las instancias de Amazon EC2 solicitando lo siguiente: Enumera	

Tarea	Descripción	Habilidades requeridas
	todas las instancias de EC2. • Para iniciar o detener una instancia de Amazon EC2, solicite lo siguiente : Inicia una instancia de EC2 [instance-id] o Detén la instancia EC2 [instance -id]. Nota: Sustituya los valores entre paréntesis por los nombres de los recursos reales o IDs de su AWS entorno.	

Eliminar recursos

Tarea	Descripción	Habilidades requeridas

Elimine los recursos creados.	Para eliminar toda la infraestr uctura creada por este patrón, ejecute el comando siguiente:
	
	`terraform plan -destroy`
	
	Revise el plan de eliminaci ón detenidamente. Si las eliminaciones planificadas son aceptables, ejecute el comando siguiente:
	
	`terraform destroy`
		AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Nota: Este comando eliminará de forma permanente todos los recursos creados por este patrón. El comando solicitar á una confirmación antes de eliminar cualquier recurso.	

Resolución de problemas

Problema	Solución
Comportamiento del agente	Para obtener información sobre este problema, consulte Prueba y solución de problemas del comportamiento de los agentes en la documentación de Amazon Bedrock.
Problemas de la red de Lambda	Para obtener información sobre estos problemas, consulte Solución de problemas de red en Lambda en la documentación de Lambda.
Permisos de IAM	Para obtener información sobre estos problemas, consulte Solución de problemas de IAM en la documentación de IAM.

Recursos relacionados

- Creación de una instantánea de base de datos para una instancia de base de datos Single-AZ para Amazon RDS
- Definición de los esquemas de OpenAPI para los grupos de acciones del agente en Amazon Bedrock
- Habilitar el control de versiones en buckets
- Cómo funciona Amazon Bedrock Agents

- Recuperación de datos y generación de respuestas de IA con bases de conocimientos de Amazon Bedrock
- Acceda de forma segura a Services Over AWS PrivateLink
- Detención e iniciación de una instancia de Amazon EC2
- Utilice grupos de acciones para definir las acciones que debe realizar su agente

Automatice CloudFront las actualizaciones cuando cambien los puntos finales del equilibrador de carga mediante Terraform

Tamilselvan P, Mohan Annam y Naveen Suthar, Amazon Web Services

Resumen

Cuando los usuarios de Amazon Elastic Kubernetes Service (Amazon EKS) eliminan y vuelven a instalar su configuración de entrada mediante gráficos de Helm, se crea un nuevo equilibrador de carga de aplicación (ALB). Esto crea un problema porque Amazon CloudFront sigue haciendo referencia al registro DNS anterior de la ALB. Como resultado, no se podrá acceder a los servicios destinados a este punto de conexiön. (Para más información sobre este flujo de trabajo problemático, consulte Información adicional).

Para resolver este problema, este patrón describe el uso de una AWS Lambda función personalizada que se desarrolló con Python. Esta función Lambda detecta automáticamente cuando se crea un nuevo ALB mediante las reglas de Amazon. EventBridge A continuación AWS SDK para Python (Boto3), la función actualiza la CloudFront configuración con la nueva dirección DNS del ALB, lo que garantiza que el tráfico se dirija al punto final correcto.

Esta solución automatizada mantiene la continuidad del servicio sin enrutamiento ni latencia adicionales. El proceso ayuda a garantizar que CloudFront siempre haga referencia al punto final DNS del ALB correcto, incluso cuando la infraestructura subyacente cambie.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.
- Ejemplo de aplicación web para pruebas y validaciones que se implementa en Amazon EKS mediante Helm. Para más información, consulte Implementación de aplicaciones con Helm en Amazon EKS en la documentación de Amazon EKS.
- Configure CloudFront para enrutar las llamadas a un ALB creado por un controlador de ingreso Helm. Para obtener más información, consulte Instalar el controlador de AWS Load Balancer con Helm en la documentación de Amazon EKS y Restringir el acceso a los balanceadores de carga de aplicaciones en la documentación. CloudFront
- Terraform se instala y configura en un espacio de trabajo local.

Limitaciones

- Algunos Servicios de AWS no están disponibles en todos. Regiones de AWS Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- Terraform, versión 1.0.0 o posterior
- La versión 4.20 o posterior del Proveedor de AWS para Terraform

Arquitectura

En el siguiente diagrama se muestran los componentes de la arquitectura y el flujo de trabajo de esta aplicación.

Esta solución realiza los pasos que se indican a continuación:

1. El controlador de entrada de Amazon EKS crea un nuevo equilibrador de carga de aplicación (ALB) cada vez que se reinicia o implementa Helm.
2. EventBridge busca eventos de creación de ALB.
3. El evento de creación de ALB activa la función de Lambda.
4. La función Lambda se implementó en base a Python 3.9 y utiliza la API boto3 para realizar llamadas. Servicios de AWS La función Lambda actualiza la CloudFront entrada con el nombre DNS más reciente del balanceador de carga, que se recibe de los eventos de creación del balanceador de carga.

Tools (Herramientas)

Servicios de AWS

- Amazon CloudFront acelera la distribución de tu contenido web al distribuirlo a través de una red mundial de centros de datos, lo que reduce la latencia y mejora el rendimiento.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar AWS Kubernetes sin necesidad de instalar o mantener su propio plano de control o nodos de Kubernetes.

- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, AWS Lambda funciones, puntos finales de invocación HTTP que utilizan destinos de API o buses de eventos en otros. Cuentas de AWS
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS SDK para Python (Boto3)es un kit de desarrollo de software que le ayuda a integrar su aplicación, biblioteca o script de Python con Servicios de AWS.

Otras herramientas

- Python es un lenguaje de programación informático de uso general.
- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.

Repositorio de código

El código de este patrón está disponible en el GitHub aws-cloudfront-automation-terraform repositorio -samples.

Epics

Configuración de la estación de trabajo local

Tarea	Descripción	Habilidades requeridas
Instalar y configurar la CLI de Git.	Para instalar y configura r la interfaz de la línea de comandos (CLI) de Git en su estación de trabajo local, siga las instrucciones de Introducc ión a la instalación de Git en la documentación de Git.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Cree la carpeta del proyecto y añada los archivos.	1. Ve al GitHub repositorio del patrón y pulsa el botón Código. 2. En el cuadro de diálogo Clone (Clonar), seleccione la pestaña HTTPS. En Clone using the web URL (Clonar mediante la URL web), copie la URL que se muestra. 3. En el equipo local, cree una carpeta. Póngale el nombre del proyecto. 4. Abra un terminal en la máquina local y vaya a la carpeta. 5. Para clonar el repositorio de Git de este patrón, ejecute el siguiente comando: `git clone https://github.com/aws-samples/aws-cloudfront-automation-terraform-samples` 6. Una vez clonado el repositorio, utilice el siguiente comando para ir al directorio clonado: `cd <directory name>/cloudfront-update` Abra el proyecto en un entorno de desarrollo	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	integrado (IDE) de su elección.	

Aprovisionamiento de la arquitectura de destino mediante la configuración de Terraform

Tarea	Descripción	Habilidades requeridas

Implemente la solución.	Para implementar recursos en el objetivo Cuenta de AWS, siga los siguientes pasos:
	1. Vaya a la carpeta `cloudfront-update` .
	2. Actualice el archivo `terraform.tfvars` con `cloudfront_distribution_id` .
	3. Para configurarlo Región de AWS para su AWS perfil, ejecute el siguiente comando:
	`export AWS_REGION={{ REGION }}`
	4. Ejecute el comando siguiente para inicializar Terraform:
	`terraform init`
	5. Ejecute el siguiente comando para validar Terraform:
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	`terraform validate`
	6. Ejecute el siguiente comando para crear un plan de ejecución de Terraform:
	`terraform plan`
	7. Ejecute el siguiente comando para aplicar las acciones desde `terraform plan`:
	`terraform apply`	

Verifique la implementación

Tarea	Descripción	Habilidades requeridas
Valide la implementación.	1. Inicia sesión Consola de administración de AWS y abre la CloudFront consola de Amazon en la https://console.aws.amazon.com/cloudfront/v4/home. 2. En el panel de navegació n izquierdo, seleccion a Distribuciones y, a continuación, abre la distribución. CloudFront 3. En la pestaña Origins (Orígenes), compruebe que el nombre y la asignación	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	de origen tengan el registro DNS de ALB actualizado.	

Limpieza de la infraestructura

Tarea	Descripción	Habilidades requeridas
Limpie la infraestructura.	Para limpiar la infraestructura que creó anteriormente, realice los siguientes pasos: 1. Ejecute el comando siguiente: `terraform destroy` 2. Para confirmar el comando de eliminación, introduzca `yes`.	DevOps ingeniero

Resolución de problemas

Problema	Solución
Error al validar las credenciales del proveedor	Al ejecutar los comandos `apply` o `destroy` de Terraform desde su equipo local, es posible que se produzca un error similar al siguiente: `Error: configuring Terraform AWS Provider: error validating provider credentials: error calling sts:GetCallerIdentity: operation error STS: GetCallerIdentity, https response error StatusCode: 403, RequestID: 123456a9-fbc1-40ed-b8d8-513d0133ba7f, api error InvalidClientTokenId:`

Problema	Solución
	`The security token included in the request is invalid.` Este error se debe a la caducidad del token de seguridad de las credenciales usadas en la configuración de la máquina local. Para resolver el error, consulte Establecer y ver los ajustes de configuración en la documenta ción AWS Command Line Interface (AWS CLI).

Recursos relacionados

AWS resources

- Restrinja el acceso a los balanceadores de carga de aplicaciones
- Enrute el tráfico de Internet con el AWS Load Balancer Controller

Documentación de Terraform

- AWS Proveedor
- Instalar Terraform
- Estado remoto

Información adicional

Flujo de trabajo problemático

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Cuando el usuario accede a la aplicación, la llamada va a. CloudFront
2. CloudFront enruta las llamadas al Application Load Balancer (ALB) correspondiente.
3. El ALB incluye las direcciones IP de destino, que son las direcciones IP del pod de aplicaciones. A partir de ahí, el ALB proporciona al usuario los resultados esperados.

Sin embargo, este flujo de trabajo tiene un problema. Las implementaciones de aplicaciones se realizan a través de gráficos de Helm. Siempre que hay una implementación o si alguien reinicia Helm, también se vuelve a crear la entrada correspondiente. Como resultado, el controlador del equilibrador de carga externo vuelve a crear el ALB. Además, durante cada recreación, el ALB se vuelve a crear con un nombre de DNS diferente. Debido a esto, CloudFront tendrá una entrada obsoleta en la configuración de origen. Debido a que esta entrada está obsoleta, el usuario no podrá acceder a la aplicación. Este problema provoca un tiempo de inactividad para los usuarios.

Solución alternativa

Otra posible solución es crear un DNS externo para el ALB y, a continuación, apuntarlo al punto final de la zona alojada privada de Amazon Route 53. CloudFront Sin embargo, este enfoque añade otro salto en el flujo de la aplicación, lo que podría provocar la latencia de la aplicación. La solución de la función de Lambda de este patrón no interrumpe el flujo de actual.

Automatice las CodeGuru revisiones de Amazon para aplicaciones de AWS CDK Python mediante GitHub Actions

Vanitha Dontireddy y Sarat Chandra Pothula, Amazon Web Services

Resumen

Nota: A partir del 7 de noviembre de 2025, no podrá crear nuevas asociaciones de repositorios en Amazon CodeGuru Reviewer. Para obtener información sobre los servicios con capacidades similares a las de CodeGuru Reviewer, consulte el cambio de disponibilidad de Amazon CodeGuru Reviewer en la documentación de CodeGuru Reviewer.

Este patrón muestra la integración de las revisiones de código CodeGuru automatizadas de Amazon para aplicaciones de AWS Cloud Development Kit (AWS CDK) Python, orquestadas a través GitHub de acciones. La solución implementa una arquitectura sin servidor definida en Python AWS CDK . Al automatizar el análisis de código experto dentro del proceso de desarrollo, este enfoque puede hacer lo siguiente para los proyectos de AWS CDK Python:

- Mejorar la calidad del código.
- Optimizar los flujos de trabajo.
- Maximizar los beneficios de la informática sin servidor.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.
- AWS Command Line Interface (AWS CLI) versión 2.9.11 o posterior, instalada y configurada.
- Una GitHub cuenta activa y un GitHub repositorio con permisos de flujo de trabajo de lectura y escritura y creación de solicitudes de extracción (PR) mediante GitHub Actions para garantizar que el flujo de trabajo de PR funcione correctamente.
- Una función de OpenID Connect (OIDC) en GitHub Actions para implementar la solución en. Cuenta de AWS Utilice el constructo de AWS CDK para crear el rol.

Limitaciones

- Amazon CodeGuru Profiler admite aplicaciones escritas en todos los lenguajes de máquinas virtuales Java (JVM) (como Scala y Kotlin) y en tiempos de ejecución y Python 3.6 o versiones posteriores.
- Amazon CodeGuru Reviewer solo admite asociaciones con repositorios de código Java y Python de los siguientes proveedores de código fuente: AWS CodeCommit Bitbucket GitHub, GitHub Enterprise Cloud y GitHub Enterprise Server. Además, los repositorios de Amazon Simple Storage Service (Amazon S3) solo se admiten mediante Actions. GitHub
- No existe una forma automatizada de imprimir los resultados durante la canalización de procesos de integración e implementación continuos (CI/CD). En su lugar, este patrón utiliza GitHub las acciones como método alternativo para gestionar y mostrar los resultados.
- Algunas Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

En el siguiente diagrama se muestra la arquitectura para esta solución.

Como se muestra en el diagrama, cuando un desarrollador crea una solicitud de cambios (PR) para su revisión, GitHub Actions activa los siguientes pasos:

1. Suposición de la función de IAM: la canalización utiliza la función de IAM que se especifica en GitHub Secrets para realizar las tareas de despliegue.
2. Análisis de código
   - CodeGuru Reviewer analiza el código almacenado en el bucket de Amazon S3. Identifica los defectos y proporciona recomendaciones para corregirlos y optimizarlos.
   - CodeGuru La seguridad escanea en busca de infracciones y vulnerabilidades de las políticas.
3. Revisión de resultados
   - La canalización imprime un enlace al panel de resultados en la salida de la consola.
   - Si se detectan resultados críticos, la canalización devuelve un error inmediatamente.
   - En el caso de tener resultados de gravedad alta, normal o baja, el proceso continúa al siguiente paso.
4. Aprobación de PR

- El revisor debe aprobar manualmente el PR.
- Si se deniega el PR, se produce un error en la canalización y se detienen los pasos de implementación adicionales.

5. Implementación de CDK: tras la aprobación del PR, comienza el proceso de implementación de CDK. Configura lo siguiente Servicios de AWS y los recursos:
   - CodeGuru Generador de perfiles
   - AWS Lambda función
   - Cola de Amazon Simple Queue Service (Amazon SQS)
6. Generación de datos de creación de perfiles: para generar suficientes datos de creación de perfiles para CodeGuru Profiler:
   - La canalización invoca la función de Lambda varias veces mediante el envío periódico de mensajes a la cola de Amazon SQS.

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir y aprovisionar la Nube de AWS infraestructura en código.
- CDK Toolkit es un kit de desarrollo en la nube de línea de comandos que le ayuda a interactuar con su AWS CDK aplicación.
- Amazon CodeGuru Profiler recopila datos de rendimiento en tiempo de ejecución de sus aplicaciones activas y proporciona recomendaciones que pueden ayudarle a ajustar el rendimiento de las aplicaciones.
- Amazon CodeGuru Reviewer utiliza el análisis de programas y el aprendizaje automático para detectar posibles defectos difíciles de encontrar para los desarrolladores. A continuación, CodeGuru Profiler ofrece sugerencias para mejorar el código de Java y Python.
- Amazon CodeGuru Security es una herramienta de seguridad de aplicaciones estática que utiliza el aprendizaje automático para detectar infracciones y vulnerabilidades de las políticas de seguridad. Proporciona sugerencias para abordar los riesgos de seguridad y genera métricas para que pueda realizar un seguimiento del estado de seguridad de sus aplicaciones.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.

- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

- GitHub Actions es una plataforma de integración y entrega continuas (CI/CD) que está estrechamente integrada con los repositorios. GitHub Puedes usar GitHub Actions para automatizar tu proceso de creación, prueba e implementación.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub amazon-codeguru-suite-cdk-python.

Prácticas recomendadas

- Siga las prácticas recomendadas para desarrollar e implementar una infraestructura en la nube con la AWS CDK.
- Siga las prácticas recomendadas de seguridad de IAM cuando utilice los flujos de trabajo de Servicios de AWS In GitHub Actions, entre las que se incluyen:
  - No guarde las credenciales en el código del repositorio.
  - Obtenga un rol de IAM para recibir credenciales temporales y utilícelas siempre que sea posible.
  - Otorgue el mínimo privilegio al rol de IAM utilizado en los flujos de trabajo de GitHub Actions. Conceda únicamente los permisos necesarios para realizar las acciones en sus flujos de trabajo de GitHub Actions.
  - Supervisa la actividad del rol de IAM que se usa en los flujos de trabajo de GitHub Actions.
  - Cambie periódicamente las credenciales a largo plazo que utilice.

Epics

Configure su entorno

Tarea	Descripción	Habilidades requeridas

Configura las AWS credencia les.	Para exportar las variables que definen la pila Cuenta de AWS y Región de AWS dónde la vas a implementar, ejecuta los siguientes comandos:
	`export CDK_DEFAU LT_ACCOUNT=<12-digit AWS account number>`
	`export CDK_DEFAU LT_REGION=<AWS Region>`
	Las AWS credenciales de la AWS CDK se proporcio nan a través de variables de entorno.
		AWS DevOps, DevOps ingeniero

Clonar el repositorio.	Para clonar un repositorio en su máquina local, ejecute el siguiente comando: `git clone https://g ithub.com/aws-samp les/amazon-codeguru- suite-cdk-python.git`	AWS DevOps, DevOps ingeniero
Instale el kit de herramientas de CDK.	Para confirmar que el Kit de herramientas de CDK está instalado y comprobar la versión, ejecute el siguiente comando:	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	`cdk --version`
	
	Si la versión del kit de herramientas de CDK es anterior a la versión 2.27.0, ejecute el siguiente comando para actualizar a esa versión.
	
	`npm install -g aws-cdk@2.27.0`
	
	Si el kit de herramientas de CDK no está instalado, ejecute el siguiente comando para instalarlo:
	
	`npm install -g aws-cdk@2.27.0 --force`	

Instale las dependencias requeridas.	Ejecute el siguiente comando para instalar las dependencias de proyecto necesarias:
	
	`python -m pip install --upgrade pip`
	`pip install -r requirements.txt`
		AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Arranque el entorno de CDK.	Para arrancar un entorno de AWS CDK, ejecute los siguientes comandos.
	`npm install`
	`npm run cdk bootstrap "aws://${ACCOUNT_NUMBER}/${AWS_REGION}"`
	Tras arrancar correctamente el entorno, debería aparecer el siguiente resultado.
	`# Bootstrapping environment aws://{account}/{region}...`
	`# Environment aws://{account}/{region} bootstrapped`
		AWS DevOps, DevOps ingeniero

Implementación de la aplicación de CDK

Tarea	Descripción	Habilidades requeridas
Sintetiza la AWS CDK aplicación.	Para sintetizar una AWS CDK aplicación, ejecuta el siguiente comando: `cdk synth` Para obtener más información sobre este comando, consulte cdk synthesize en la documentación. AWS CDK	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Implementación de recursos.	Ejecute el siguiente comando para implementar los recursos: `cdk deploy --require-approval never` **Note** El indicador `--require-approval never` significa que el CDK aprobará y ejecutará todos los cambios automáticamente. Esto incluye los cambios que CDK normalmente consideraría que necesitan una revisión manual (como los cambios en la política de IAM o la eliminación de recursos). Asegúrese de que el código y la CI/CD canalización de su CDK estén bien probados y sean seguros antes de utilizar la `--require-approval never` bandera en entornos de producción.	AWS DevOps, DevOps ingeniero

Crea GitHub secretos y un token de acceso personal

Tarea	Descripción	Habilidades requeridas
Cree los secretos necesarios en GitHub.	Para permitir que los flujos de trabajo de GitHub Actions accedan a AWS los recursos de forma segura sin exponer información confidencial del código de tu repositor io, crea secretos. Para crear los secretos de GitHub un repositorio y `ROLE_TO_A SSUME` `CodeGuruR eviewArtifactBucke tName` `AWS_ACCOUNT_ID` , sigue las instrucciones de la documentación de GitHub Actions sobre cómo crear secretos para un repositorio. A continuación, encontrará más información sobre las variables: • `AWS_ACCOUNT_ID` — El Cuenta de AWS ID en el que se ejecuta la canalizac ión. • `CodeGuruReviewArti factBucketName` — El nombre del depósito de S3 en el que se almacenan los artefactos de CodeGuru Reviewer. Este patrón utiliza el nombre de bucket `codeguru-reviewer-`	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`build-artifacts-<ACCOUNT_ID>-<REGION>` . • `AWS_REGION` — El Región de AWS lugar donde se encuentran los recursos. • `ROLE_TO_ASSUME` : nombre del rol de IAM que asume la canalización. Este patrón utiliza el nombre de rol `githubActionsDeployRole` .	

Tarea	Descripción	Habilidades requeridas
Crea un token de acceso GitHub personal.	Para configurar una forma segura de autenticar tus flujos de trabajo de GitHub Actions e interactuar con ellos GitHub, haz lo siguiente: 1. Para crear un token de acceso GitHub personal con acceso de lectura y escritura a tu repositorio, sigue las instrucciones que se indican en la GitHub documentación sobre cómo gestionar tus tokens de acceso personal. 2. Para guardar este token como secreto de repositorio para GitHub Actions, sigue las instrucciones que se indican en la documenta ción de GitHub Actions sobre cómo crear secretos para un repositorio.	AWS DevOps, DevOps ingeniero

Limpieza

Tarea	Descripción	Habilidades requeridas
Eliminación de recursos.	Para limpiar tu aplicación de AWS CDK Python, ejecuta el siguiente comando: `cdk destroy --all`	DevOps ingeniero

Resolución de problemas

Problema	Solución
Muestre el enlace a los resultados del panel.	No hay forma de imprimir los resultados durante el CI/CD oleoducto. En cambio, este patrón utiliza GitHub las acciones como un método alternativo para gestionar y mostrar los resultados.

Recursos relacionados

AWS resources

- AWS Kit Cloud Development
- CodeGuru Documentación de Amazon
- Amazon S3
- AWS Identity and Access Management
- Amazon Simple Queue Service
- ¿Qué es AWS Lambda?

GitHub documentación

- Configuración de OpenID Connect en Amazon Web Services
- GitHub Acciones
- Reutilización de los flujos de trabajo
- Activación de un flujo de trabajo

Automatice la implementación de lagos de Supply Chain datos en una configuración de múltiples repositorios

Keshav Ganesh, Amazon Web Services

Resumen

Este patrón proporciona un enfoque automatizado para implementar y administrar lagos de AWS Supply Chain datos mediante capacidades de integración continua y despliegue continuo () de múltiples repositorios. CI/CD) pipeline. It demonstrates two deployment methods: automated deployment using GitHub Actions workflows, or manual deployment using Terraform directly. Both approaches use Terraform for infrastructure as code (IaC), with the automated method adding GitHub Actions and JFrog Artifactory for enhanced CI/CD

La solución aprovecha Supply Chain y Amazon Simple Storage Service (Amazon S3) para establecer la infraestructura del lago de datos y, al mismo tiempo, utiliza cualquiera de los dos métodos de implementación para automatizar la configuración y la creación de recursos. AWS Lambda Esta automatización elimina los pasos de configuración manual y garantiza la uniformidad de las implementaciones en todos los entornos. Además, Supply Chain elimina la necesidad de contar con una amplia experiencia en extracción, transformación y carga (ETL) y puede proporcionar información y análisis impulsados por Amazon Quick Sight.

Al implementar este patrón, las organizaciones pueden reducir el tiempo de implementación, mantener la infraestructura como código y administrar los lagos de datos de la cadena de suministro mediante un proceso automatizado y controlado por versiones. El enfoque de múltiples repositorios proporciona un control de acceso detallado y permite el despliegue independiente de diferentes componentes. Los equipos pueden elegir el método de implementación que mejor se adapte a sus herramientas y procesos existentes.

Requisitos previos y limitaciones

Requisitos previos

Asegúrese de que lo siguiente esté instalado en su máquina local:

- AWS Command Line Interface (AWS CLI) versión 2
- GitHub CLI
- Python v3.13

- Terraform v1.12 o posterior

Asegúrese de que se cuente con lo siguiente antes de la implementación:

- Un activo Cuenta de AWS.
- Una nube privada virtual (VPC) con dos subredes privadas Cuenta de AWS en Región de AWS la que elija.
- Permisos suficientes para el rol AWS Identity and Access Management (IAM) utilizado para la implementación en los siguientes servicios:
  - Supply Chain — Se prefiere Full Access para implementar sus componentes, como conjuntos de datos y flujos de integración, además de acceder a ellos desde. Consola de administración de AWS
  - Amazon CloudWatch Logs: para crear y administrar grupos de CloudWatch registros.
  - Amazon Elastic Compute Cloud (Amazon EC2): para grupos de seguridad de Amazon EC2 y puntos de conexión de Amazon Virtual Private Cloud (Amazon VPC).
  - Amazon EventBridge : para uso de Supply Chain.
  - IAM: para crear funciones AWS Lambda de servicio.
  - AWS Key Management Service (AWS KMS) — Para acceder al depósito AWS KMS keys de artefactos de Amazon S3 y al depósito Supply Chain provisional de Amazon S3.
  - AWS Lambda — Para crear las funciones Lambda que despliegan los Supply Chain componentes.
  - Amazon S3: para acceder al depósito de artefactos de Amazon S3, al depósito de registro de acceso al servidor y al Supply Chain depósito provisional. Si utiliza la implementación manual, también necesitará permisos para el depósito de artefactos Terraform de Amazon S3.
  - Amazon VPC: para crear y administrar una VPC.

Si prefiere utilizar los flujos de trabajo de GitHub Actions para la implementación, haga lo siguiente:

- Configure OpenID Connect (OIDC) para el rol de IAM con los permisos mencionados anteriormente.
- Cree un rol de IAM con permisos similares para acceder al. Consola de administración de AWS Para obtener más información, consulte Crear un rol para conceder permisos a un usuario de IAM en la documentación de IAM.

Si prefiere realizar una implementación manual, haga lo siguiente:

- Cree un usuario de IAM para que asuma la función de IAM con los permisos mencionados anteriormente. Para obtener más información, consulte Crear un rol para conceder permisos a un usuario de IAM en la documentación de IAM.
- Asuma el rol en su terminal local.

Si prefieres usar los flujos de trabajo de GitHub Actions para la implementación, configura lo siguiente:

- Una cuenta JFrog Artifactory para obtener el nombre de host, el nombre de usuario y el token de acceso al inicio de sesión.
- Una clave de JFrog proyecto y un repositorio para almacenar artefactos.

Limitaciones

- La Supply Chain instancia no admite técnicas complejas de transformación de datos.
- Supply Chain es la más adecuada para los dominios de la cadena de suministro porque proporciona análisis e información integrados. Para cualquier otro dominio, se Supply Chain puede utilizar como almacén de datos como parte de la arquitectura del lago de datos.
- Es posible que sea necesario mejorar las funciones Lambda utilizadas en esta solución para gestionar los reintentos de API y la administración de memoria en una implementación a escala de producción.
- Algunas Servicios de AWS no están disponibles en todos. Regiones de AWS Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

Puedes implementar esta solución mediante flujos de trabajo de GitHub Actions automatizados o manualmente con Terraform.

Despliegue automatizado con Actions GitHub

En el siguiente diagrama, se muestra la opción de despliegue automatizado que utiliza los flujos de trabajo de GitHub Actions. JFrog Artifactory se utiliza para la gestión de artefactos. Almacena

la información y los resultados de los recursos para utilizarlos en una implementación de varios repositorios.

Despliegue manual con Terraform

El siguiente diagrama muestra la opción de despliegue manual a través de Terraform. En lugar de JFrog Artifactory, Amazon S3 se utiliza para la administración de artefactos.

Flujo de trabajo de una implementación

Los diagramas muestran el siguiente flujo de trabajo:

1. Implemente conjuntos de datos de Supply Chain servicios, infraestructura y bases de datos mediante uno de los siguientes métodos de implementación:
   - Implementación automatizada: utiliza los flujos de trabajo de GitHub Actions para organizar todos los pasos de la implementación y utiliza JFrog Artifactory para la gestión de artefactos.
   - Implementación manual: ejecuta los comandos de Terraform directamente para cada paso de la implementación y usa Amazon S3 para la administración de artefactos.
2. Cree los AWS recursos de apoyo necesarios para el funcionamiento del Supply Chain servicio:
   - Puntos de enlace y grupos de seguridad de Amazon VPC
   - AWS KMS keys
   - CloudWatch Registros, grupos de registros
3. Cree e implemente los siguientes recursos de infraestructura:
   - Funciones Lambda que administran (crean, actualizan y eliminan) la instancia de Supply Chain servicio, los espacios de nombres y los conjuntos de datos.
   - Supply Chain organizar un bucket de Amazon S3 para la ingesta de datos
4. Implemente la función Lambda que gestiona los flujos de integración entre el depósito provisional y los conjuntos de datos. Supply Chain Una vez completada la implementación, los pasos restantes del flujo de trabajo gestionan la ingesta y el análisis de los datos.
5. Configure la ingesta de datos de origen en el bucket Supply Chain provisional de Amazon S3.
6. Una vez que se añaden los datos al Supply Chain bucket provisional de Amazon S3, el servicio activa automáticamente el flujo de integración de los Supply Chain conjuntos de datos.
7. Supply Chain se integra con Quick Sight Analytics para crear paneles basados en los datos ingeridos.

Tools (Herramientas)

Servicios de AWS

- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas y aplicaciones Servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar Servicios de AWS mediante los comandos de su consola de línea de comandos.
- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, AWS Lambda funciones, puntos de enlace de invocación HTTP que utilizan destinos de API o buses de eventos en otros. Cuentas de AWS
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS IAM Identity Centerle ayuda a gestionar de forma centralizada el acceso mediante el inicio de sesión único (SSO) a todas sus aplicaciones y a las de la nube. Cuentas de AWS
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Q in Supply Chain es un asistente de IA generativa interactivo que le ayuda a gestionar su cadena de suministro de forma más eficiente mediante el análisis de los datos de su lago de Supply Chain datos.
- Amazon QuickSight es un servicio de inteligencia empresarial (BI) a escala de la nube que lo ayuda a visualizar, analizar y generar informes de sus datos en un único panel.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Supply Chaines una aplicación gestionada basada en la nube que se puede utilizar como almacén de datos en las organizaciones para los dominios de la cadena de suministro, que se puede utilizar para generar información y realizar análisis de los datos ingeridos.

- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS. Un punto de conexión de Amazon VPC es un dispositivo virtual que le ayuda a conectar de forma privada su VPC a una red compatible Servicios de AWS sin necesidad de una pasarela de Internet, un dispositivo NAT, una conexión VPN o una conexión. AWS Direct Connect

Otras herramientas

- GitHub Actions es una plataforma de integración y entrega continuas (CI/CD) que está estrechamente integrada con los repositorios. GitHub Puedes usar GitHub Actions para automatizar tu proceso de creación, prueba e implementación.
- HashiCorp Terraform es una herramienta de infraestructura como código (IaC) que te ayuda a crear y administrar recursos locales y en la nube.
- JFrog Artifactory proporciona end-to-end automatización y administración de archivos binarios y artefactos a través del proceso de entrega de la aplicación.
- Python es un lenguaje de programación informático de uso general. Este patrón usa Python para que el código de la AWS función interactúe con Supply Chain

.

Prácticas recomendadas

- Mantenga la mayor seguridad posible al implementar este patrón. Como se indica en los requisitos previos, asegúrese de tener una nube privada virtual (VPC) con dos subredes privadas en Región de AWS la que Cuenta de AWS elija.
- Utilice claves administradas por el AWS KMS cliente siempre que sea posible y concédales permisos de acceso limitados.
- Para configurar las funciones de IAM con el acceso mínimo necesario para ingerir datos según este patrón, consulte Proteger la ingestión de datos desde los sistemas de origen a Amazon S3 en el repositorio de este patrón.

Epics

(Ambas opciones) Configure una estación de trabajo local

Tarea	Descripción	Habilidades requeridas

Clonar el repositorio.	Para clonar el repositorio de este patrón, ejecute el comando siguiente en la estación de trabajo local:
	`git clone https://github.com/aws-samples/sample-automate-aws-supply-chain-deployment.git`
	`cd ASC-Deployment`
		AWS DevOps

(Opción automatizada) Verifique los requisitos previos para la implementación.	Asegúrese de que se hayan completado los requisitos previos para la implementación automática.	Propietario de la aplicación

(Opción manual) Prepárese para la implementación de los Supply Chain conjuntos de datos.	Para ir al `terraform-deployment` directorio de`ASC-Datasets` , ejecute el siguiente comando:
	`cd ASC-Datasets/terraform-deployment`
	Para asumir el rol ARN que se creó en los requisitos previos, ejecute el siguiente comando:
	`aws sts assume-role --role-arn <enter AWS user role ARN> --role-`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	session-name <your-session-name>
	
	Para configurar y exportar las variables de entorno, ejecute los siguientes comandos:
	
	`# Export Environment variables`
	`export REGION=<Enter deployment region>`
	`export REPO_NAME=<Enter Current ASC Datasets dir name>`
	`export PROJECT_NAME="asc-deployment-poc"`
	`export ACCOUNT_ID=<Enter deployment Account ID>`
	`export ENVIRONMENT="dev"`
	`export LAMBDA_LAYER_TEMP_DIR_TERRAFORM="layerOutput"`
	`export LAMBDA_FUNCTION_TEMP_DIR_TERRAFORM="lambdaOutput"`
	`export AWS_USER_ROLE=<Enter user role ARN for AWS Console access and deployment>`
	`export S3_TERRAFORM_ARTIFACTS_BUCKET_NAME="$PROJECT_NAME-$ACCOUNT_ID-$REGION-terraform-artifacts-$ENVIRONMENT"`	

Tarea	Descripción	Habilidades requeridas

(Opción manual) Prepárese para gestionar los flujos de Supply Chain integración durante la implementación.	Para ir al `terraform-deployment` directorio de`ASC-Integration-Flows` , ejecute el siguiente comando:
	`cd ASC-Integration-Flows/terraform-deployment`
	Para asumir el rol ARN que se creó anteriormente, ejecute el siguiente comando:
	`aws sts assume-role --role-arn <enter AWS user role ARN> --role-session-name <your-session-name>`
	Para configurar y exportar las variables de entorno, ejecute los siguientes comandos:
	`# Export Environment variables`
	`export REGION=<Enter deployment region>`
	`export REPO_NAME=<Enter Current ASC Integration Flows dir name>`
	`export ASC_DATASET_VARS_REPO=<Enter Current ASC Datasets dir name>  #Must be the same directory name`
		Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	used for ASC Datasets deployment export PROJECT_NAME="asc-deployment-poc" export ACCOUNT_ID=<Enter deployment Account ID> export ENVIRONMENT="dev" export LAMBDA_LAYER_TEMP_DIR_TERRAFORM="layerOutput" export LAMBDA_FUNCTION_TEMP_DIR_TERRAFORM="lambdaOutput" export S3_TERRAFORM_ARTIFACTS_BUCKET_NAME="$PROJECT_NAME-$ACCOUNT_ID-$REGION-terraform-artifacts-$ENVIRONMENT"	

(Opción automatizada) Implemente Supply Chain conjuntos de datos mediante los flujos de trabajo de GitHub Actions

Tarea	Descripción	Habilidades requeridas
Copia el `ASC-Datasets` directorio.	Para copiar el `ASC-Datasets` directorio a una nueva ubicación, siga estos pasos: 1. Para ir al `ASC-Datasets` directorio, ejecute el siguiente comando:	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`cd ASC-Datasets`
	2. Para copiar el `ASC-Datasets` directorio a una nueva ubicación, ejecute los siguientes comandos:
	`cp -r ASC-Datasets ../ASC-Datasets-standalone`
	`cd ../ASC-Datasets-standalone`	

Configure el `ASC-Datasets` directorio.	Para configurarlo `ASC-Datasets` como un repositorio independiente en su organización, ejecute los siguientes comandos:
	`git init`
	`git add .`
	`git commit -m "Initial commit: ASC-Datasets standalone repository"`
	`git remote add origin <INSERT_ASC_DATASETS_GITHUB_URL>`
	`git branch -M dev`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

Configure el nombre de la rama en el archivo de flujo de trabajo .github.	Configura el nombre de la rama en el archivo de flujo de trabajo de implement ación, como se muestra en el siguiente ejemplo:
	`on:`
	`workflow_`
	`dispatch:`
	`push:`
	`branches:`
	`- dev`
	`#Change to any other branch preferred for deployment`
		Propietario de la aplicación

Configure GitHub los entornos y configure los valores del entorno.	Para configurar GitHub los entornos de su GitHub organización, siga las instrucci ones de Configuración de GitHub los entornos del repositorio de este patrón. Para configurar los valores del entorno en los archivos de flujo de trabajo, siga las instrucciones de Configurar los valores del entorno en los archivos de flujo de trabajo del repositorio de este patrón.	Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Activa el flujo de trabajo.	Para introducir los cambios en su GitHub organización y activar el flujo de trabajo de implementación, ejecute el siguiente comando: `git push -u origin dev`	AWS DevOps

(Opción automatizada) Implemente flujos de Supply Chain integración mediante flujos de trabajo de GitHub Actions

Tarea	Descripción	Habilidades requeridas

Copia el `ASC-Integration-Flows` directorio.	Para copiar el `ASC-Integration-Flows` directorio a una nueva ubicación, siga estos pasos:
	1. Para ir al `ASC-Integration-Flows` directorio, ejecute el siguiente comando:
	`cd ASC-Integration-Flows`
	2. Para copiar el `ASC-Integration-Flows` directorio a una nueva ubicación, ejecute los siguientes comandos:
	`cp -r ASC-Integration-Flows ../ASC-`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`Integration-Flows-st andalone` `cd ../ASC-In tegration-Flows-st andalone`	

Configure el `ASC-Integ ration-Flows` directorio.	Para configurar el `ASC-Integration-Flows` directorio como un repositorio independiente en su organizac ión, ejecute los siguientes comandos:
	`git init`
	`git add .`
	`git commit -m "Initial commit: ASC-Integ ration-Flows standalon e repository"`
	`git remote add origin <INSERT_ASC_Integr ation_Flows_GITHUB _URL>`
	`git branch -M dev`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

Configure el nombre de la rama en el archivo de flujo de trabajo .github.	Configura el nombre de la rama en el archivo de flujo de trabajo de implementación, como se muestra en el siguiente ejemplo:
	`on:`
	`workflow_`
	`dispatch:`
	`push:`
	`branches:`
	`- dev`
	`#Change to any other branch preferred for deployment`
		Propietario de la aplicación

Configure GitHub los entornos y configure los valores del entorno.	Para configurar GitHub los entornos de su GitHub organización, siga las instrucciones de Configuración de GitHub los entornos del repositorio de este patrón. Para configurar los valores del entorno en los archivos de flujo de trabajo, siga las instrucciones de Configurar los valores del entorno en los archivos de flujo de trabajo del repositorio de este patrón.	Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Activa el flujo de trabajo.	Para introducir los cambios en su GitHub organización y activar el flujo de trabajo de implementación, ejecute el siguiente comando: `git push -u origin dev`	AWS DevOps

(Opción manual) Implemente Supply Chain conjuntos de datos con Terraform

Tarea	Descripción	Habilidades requeridas
Vaya al directorio `terraform-deployment` .	Para ir al `terraform-deployment` directorio de`ASC-Datasets` , ejecute el siguiente comando: `cd ASC-Datasets/terraform-deployment`	AWS DevOps

Configure el bucket Amazon S3 del estado de Terraform.	Para configurar el bucket Amazon S3 del estado de Terraform, utilice el siguiente script:
	`# Setup terraform bucket`
	`chmod +x ../scripts/setup-terraform.sh`
	`../scripts/setup-terraform.sh`
		AWS DevOps

Configure el bucket Amazon S3 de Terraform Artifacts.	Para configurar el bucket Amazon S3 de Terraform	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	Artifacts, utilice el siguiente script:
	
	`# Setup terraform artifacts bucket`
	`chmod +x ../scripts/setup-terraform-artifacts-bucket.sh`
	`../scripts/setup-terraform-artifacts-bucket.sh`	

Configure el backend y la configuración de los proveedores de Terraform.	Para configurar el backend y los proveedores de Terraform, utilice el siguiente script:
	
	`# Setup terraform backend and providers config if they don't exist`
	`chmod +x ../scripts/generate-terraform-config.sh`
	`../scripts/generate-terraform-config.sh`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

Genere un plan de despliegue.	Para generar un plan de despliegue, ejecute los siguientes comandos:
	`# Run terraform init and validate`
	`terraform init`
	`terraform validate`
	
	`# Run terraform plan`
	`terraform plan \`
	`-var-file="tfInputs/$ENVIRONMENT.tfvars" \`
	`-var="project_name=$PROJECT_NAME" \`
	`-var="environment=$ENVIRONMENT" \`
	`-var="user_role=$AWS_USER_ROLE" \`
	`-var="lambda_temp_dir=$LAMBDA_FUNCTION_TEMP_DIR_TERRAFORM" \`
	`-var="layer_temp_dir=$LAMBDA_LAYER_TEMP_DIR_TERRAFORM" \`
	`-parallelism=40 \`
	`-out='tfplan.out'`
		AWS DevOps

Implemente las configura ciones.	Para implementar las configuraciones, ejecute el siguiente comando:
	`# Run terraform apply`
	`terraform apply tfplan.out`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

Actualice otras configuraciones y almacene los resultados.	Para actualizar las políticas AWS KMS clave y almacenar los resultados de las configuraciones aplicadas en el bucket Amazon S3 de Terraform Artifacts, ejecute los siguientes comandos:
	`# Update AWS Supply Chain KMS Key policy with the service's requirements`
	`chmod +x ../scripts/update-asc-kms-policy.sh`
	`../scripts/update-asc-kms-policy.sh`
	`# Update AWS KMS Keys' policy with IAM roles`
	`chmod +x ../scripts/update-kms-policy.sh`
	`../scripts/update-kms-policy.sh`
	`# Create terraform outputs file to be used as input variables`
	`terraform output -json > raw_output.json`
	`jq -r 'to_entries | map( if .value.type == "string" then "\(.key) = \"\(.value.value)\"" else`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`"\(.key) = \(.value.value | tojson)" end ) | .[]' raw_output.json > $REPO_NAME-outputs.tfvars`
	
	`# Upload reformed outputs file to Amazon S3 terraform artifacts bucket (For retrieval from other repositories) aws s3 cp $REPO_NAME-outputs.tfvars s3://$S3_TERRAFORM_ARTIFACTS_BUCKET_NAME/$REPO_NAME-outputs.tfvars rm -f raw_output.json rm -f $REPO_NAME-outputs.tfvars`	

(Opción manual) Implemente flujos Supply Chain de integración de servicios mediante Terraform

Tarea	Descripción	Habilidades requeridas
Vaya al directorio `terraform-deployment` .	Para ir al `terraform-deployment` directorio de`ASC-Integration-Flows` , ejecute el siguiente comando: `cd ASC-Integration-Flows/terraform-deployment`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

Configure el backend y la configuración de los proveedor es de Terraform.	Para configurar las configura ciones del backend y del proveedor de Terraform, utilice el siguiente script:
	`# Setup terraform backend and providers config if they don't exist`
	`chmod +x ../scripts/generate-terraform-config.sh`
	`../scripts/generate-terraform-config.sh`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

Genere un plan de despliegue.	Para generar un plan de despliegue, ejecute los siguientes comandos. Estos comandos inicializan el entorno de Terraform, combinan las variables de configuración `ASC-Datasets` con las configuraciones de Terraform existentes y generan un plan de despliegue.
	`# Run terraform init and validate`
	`terraform init`
	`terraform validate`
	`# Download and merge ASC DATASET tfvars`
	`chmod +x ../scripts/download-vars-through-s3.sh`
	`../scripts/download-vars-through-s3.sh $ASC_DATASET_VARS_REPO`
	`# Run terraform plan`
	`terraform plan \`
	`-var-file="tfInputs/$ENVIRONMENT.tfvars" \`
	`-var="project_name=$PROJECT_NAME" \`
	`-var="environment=$ENVIRONMENT" \`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`-var="lambda_temp_dir= $LAMBDA_FUNCTION_TEMP _DIR_TERRAFORM" \ -var="layer_temp_dir= $LAMBDA_LAYER_TEMP_DIR _TERRAFORM" \ -parallelism=40 \ -out='tfplan.out'`	
Implemente las configura ciones.	Para implementar las configuraciones, ejecute el siguiente comando: `# Run terraform apply terraform apply tfplan.out`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

Actualice otras configuraciones.	Para actualizar las políticas AWS KMS clave y almacenar los resultados de las configuraciones aplicadas en el bucket Amazon S3 de Terraform Artifacts, ejecute los siguientes comandos:
	`# Update AWS KMS Keys' policy with IAM roles`
	`chmod +x ../scripts/update-kms-policy-through-s3.sh`
	`../scripts/update-kms-policy-through-s3.sh $ASC_DATA SET_VARS_REPO`
	`# Create terraform outputs file to be used as input variables`
	`terraform output -json > raw_output.json`
	`jq -r 'to_entries | map( if .value.type == "string" then "\(.key) = \"\(.value.value)\"" else "\(.key) = \(.value.value | tojson)" end ) | .[]' raw_output.json > $REPO_NAME-outputs.tfvars`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`# Upload reformed outputs file to Amazon S3 terraform artifacts bucket (For retrieval from other repositories)`
	`aws s3 cp $REPO_NAME-outputs.tfvars s3://$S3_TERRAFORM_ARTIFACTS_BUCKET_NAME/$REPO_NAME-outputs.tfvars`
	`rm -f raw_output.json`
	`rm -f $REPO_NAME-outputs.tfvars`	

(Ambas opciones) Ingiera datos

Tarea	Descripción	Habilidades requeridas
Cargue archivos CSV de muestra.	Para cargar archivos CSV de muestra para los conjuntos de datos, siga los siguientes pasos: 1. Cree archivos CSV de muestra con datos variados para los conjuntos de datos del calendario y de las líneas de pedidos salientes que se crearon durante la implementación. 2. Obtenga el ID de la Supply Chain instancia del directorio `asc_instance_id` de salidas de Terraform.	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas

	3. Tenga en cuenta el nombre del bucket de Amazon S3 Supply Chain que se creó en la implementación: `aws-supply-chain-data-<Instance_ID>`
	4. Para cargar los archivos mediante el AWS CLI, ejecute los siguientes comandos:
	`# Upload Calendar CSV file`
	`aws s3 cp calendar_sample.csv s3://aws-supply-chain-data-<Instance_ID>/calendar-data/`
	`# Upload Outbound Order Line CSV file`
	`aws s3 cp outbound_order_line_sample.csv s3://aws-supply-chain-data-<Instance_ID>/outbound-order-line-data/`	

(Ambas opciones) Configura el Supply Chain acceso

Tarea	Descripción	Habilidades requeridas
Configura el Supply Chain acceso.	Para configurar el Supply Chain acceso desde Consola de administración de AWS, siga los siguientes pasos:	Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	1. Inicie sesión en Consola de administración de AWS y busque el Supply Chain servicio. 2. Ve a la instancia`asc-deployment-poc-dev-asc-instance` . 3. Este patrón utiliza el Centro de identidad de IAM para gestionar el acceso de los usuarios a la Supply Chain instancia. Para garantizar el acceso completo a esta solución, inicie sesión como administrador de la aplicación.	

(Opción automática) Limpie todos los recursos mediante los flujos de trabajo de GitHub Actions

Tarea	Descripción	Habilidades requeridas
Active el flujo de trabajo de destrucción de los recursos de los flujos de integración.	Active el flujo de trabajo de destrucción `ASC-Integration-Flows` desde la rama de despliegue de su GitHub organización.	AWS DevOps
Active el flujo de trabajo de destrucción de los recursos de conjuntos de datos.	Active el flujo de trabajo de destrucción `ASC-Datasets` desde la rama de despliegue de su GitHub organización.	AWS DevOps

(Opción manual) Limpie los recursos de los flujos de Supply Chain integración con Terraform

Tarea	Descripción	Habilidades requeridas
Vaya al directorio `terraform-deployment` .	Para ir al `terraform-deployment` directorio de`ASC-Integration-Flows` , ejecute el siguiente comando: `cd ASC-Integration-Flows/terraform-deployment`	AWS DevOps

Configure el backend y la configuración de los proveedores de Terraform.	Para configurar el backend y los proveedores de Terraform, utilice el siguiente script:
	`# Setup terraform backend and providers config if they don't exist`
	`chmod +x ../scripts/generate-terraform-config.sh`
	`../scripts/generate-terraform-config.sh`
		AWS DevOps

Genere un plan de destrucción de infraestructura.	Para prepararse para la destrucción controlada de su AWS infraestructura mediante la generación de un plan de desmontaje detallado, ejecute los siguientes comandos. El proceso inicializa Terraform , incorpora configuraciones de Supply Chain conjuntos de datos y crea un plan de	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	destrucción que puede revisar antes de ejecutarlo.
	
	`# Run terraform init and validate`
	`terraform init`
	`terraform validate`
	
	`# Download and merge ASC DATASET tfvars`
	`chmod +x ../scripts/download-vars-through-s3.sh`
	`../scripts/download-vars-through-s3.sh $ASC_DATASET_VARS_REPO`
	
	`# Run terraform plan`
	`terraform plan -destroy \`
	`-var-file="tfInputs/$ENVIRONMENT.tfvars" \`
	`-var="project_name=$PROJECT_NAME" \`
	`-var="environment=$ENVIRONMENT" \`
	`-var="lambda_temp_dir=$LAMBDA_FUNCTION_TEMP_DIR_TERRAFORM" \`
	`-var="layer_temp_dir=$LAMBDA_LAYER_TEMP_DIR_TERRAFORM" \`
	`-parallelism=40 \`
	`-out='tfplan.out'`	

Tarea	Descripción	Habilidades requeridas

Ejecute un plan de destrucción de la infraestructura.	Para ejecutar la destrucción planificada de su infraestructura, ejecute el siguiente comando:
	`# Run terraform apply`
	`terraform apply`
	`tfplan.out`
		AWS DevOps

Elimine las salidas de Terraform del bucket de Amazon S3.	Para eliminar el archivo de resultados que se cargó durante la implementación de `ASC-Integration-Flows`, ejecute el siguiente comando:
	`# Delete the outputs file`
	`aws s3 rm s3://$S3_TERRAFORM_ARTIFACTS_BUCKET_NAME/$REPO_NAME-outputs.tfvars`
		AWS DevOps

(Opción manual) Limpie los recursos de los conjuntos de datos de Supply Chain servicios con Terraform

Tarea	Descripción	Habilidades requeridas
Vaya al directorio `terraform-deployment`.	Para ir al `terraform-deployment` directorio de `ASC-Datasets`, ejecute el siguiente comando:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`cd ASC-Datasets/terraform-deployment`	

Configure el backend y la configuración de los proveedores de Terraform.	Para configurar el backend y los proveedores de Terraform, utilice el siguiente script:
	`# Setup terraform backend and providers config if they don't exist`
	`chmod +x ../scripts/generate-terraform-config.sh`
	`../scripts/generate-terraform-config.sh`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

Genere un plan de destrucción de infraestructura.	Para crear un plan para destruir los recursos del Supply Chain conjunto de datos, ejecute los siguientes comandos:
	
	`# Run terraform init and validate`
	`terraform init`
	`terraform validate`
	
	`# Run terraform plan`
	`terraform plan -destroy \`
	`-var-file="tfInputs/$ENVIRONMENT.tfvars" \`
	`-var="project_name=$PROJECT_NAME" \`
	`-var="environment=$ENVIRONMENT" \`
	`-var="user_role=$AWS_USER_ROLE" \`
	`-var="lambda_temp_dir=$LAMBDA_FUNCTION_TEMP_DIR_TERRAFORM" \`
	`-var="layer_temp_dir=$LAMBDA_LAYER_TEMP_DIR_TERRAFORM" \`
	`-parallelism=40 \`
	`-out='tfplan.out'`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

Depósitos de Amazon S3 vacíos.	Para vaciar todos los depósitos de Amazon S3 (excepto el depósito de registro de acceso al servidor, para el que está configura do`force-destroy`), utilice el siguiente script:
	`# Delete S3 buckets excluding server access logging bucket`
	`chmod +x ../scripts/empty-s3-buckets.sh`
	`../scripts/empty-s3-buckets.sh tfplan.out`
		AWS DevOps

Ejecute un plan de destrucción de la infraestructura.	Para ejecutar la destrucción planificada de la infraestructura de su Supply Chain conjunto de datos mediante el plan generado, ejecute el siguiente comando:
	`# Run terraform apply`
	`terraform apply tfplan.out`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

Elimine las salidas de Terraform del depósito de artefactos de Terraform de Amazon S3.	Para completar el proceso de limpieza, elimine el archivo de resultados que se cargó durante la implementación de `ASC-Datasets` ejecutando el siguiente comando:
	`# Delete the outputs file`
	`aws s3 rm s3://$S3_TERRAFORM_ARTIFACTS_BUCKET_NAME/$REPO_NAME-outputs.tfvars`
		AWS DevOps

Resolución de problemas

Problema	Solución
Un Supply Chain conjunto de datos o un flujo de integración no se implementó correctamente debido a errores Supply Chain internos o a la insuficiencia de permisos de IAM para la función de servicio.	En primer lugar, limpie todos los recursos. A continuación, vuelva a implementar los recursos del Supply Chainconjunto de datos y, a continuación, vuelva a implementar los recursos del Supply Chain flujo de integración.
El flujo Supply Chain de integración no busca los nuevos archivos de datos cargados para los conjuntos de datos. Supply Chain	1. Compruebe que el prefijo de la configuración del flujo de Supply Chain integración coincida con el prefijo utilizado al cargar los archivos de datos de muestra. 2. Si se han vuelto a crear los recursos de Supply Chain los conjuntos de datos, sus nombres de recursos de Amazon (ARNs) asociados cambian internamente. Por lo tanto, vuelva a implementar los recursos

Problema	Solución
	para los recursos de los flujos de integración de Supply Chain servicios.

Recursos relacionados

AWS documentación

- Supply Chain

Otros recursos

- Descripción de los flujos de trabajo de GitHub Actions (GitHub documentación)

Información adicional

Esta solución se puede replicar para más conjuntos de datos y se puede consultar para su posterior análisis, a través de paneles prediseñados que se proporcionan con Amazon Quick Sight o mediante una integración Supply Chain personalizada con Amazon Quick Sight. Además, puedes usar Amazon Q para hacer preguntas relacionadas con tu Supply Chain instancia.

Analice los datos con Supply Chain Analytics

Para obtener instrucciones sobre cómo configurar Supply Chain Analytics, consulte Configuración de Supply Chain Analytics en la Supply Chain documentación.

Este patrón demostró la creación de conjuntos de datos Calendar y Outbound_Order_Line. Para crear un análisis que utilice estos conjuntos de datos, siga los siguientes pasos:

1. Para analizar los conjuntos de datos, utilice el panel de análisis de estacionalidad. Para agregar el panel, siga los pasos que se indican en los paneles prediseñados de la documentación. Supply Chain
2. Elija el panel para ver su análisis, que se basa en archivos CSV de muestra para los datos del calendario y los datos de las líneas de pedidos salientes.

El panel proporciona información sobre demanda a lo largo de los años en función de los datos ingeridos para los conjuntos de datos. Puede especificar además el ProductID, el CustomeriD, los años y otros parámetros para el análisis.

Usa Amazon Q para hacer preguntas relacionadas con tu Supply Chain instancia

Amazon Q in Supply Chain es un asistente de IA generativa interactivo que le ayuda a gestionar su cadena de suministro de forma más eficiente. Amazon Q puede hacer lo siguiente:

- Analice los datos de su lago Supply Chain de datos.
- Proporcione información operativa y financiera.
- Responda a sus preguntas inmediatas sobre la cadena de suministro.

Para obtener más información sobre el uso de Amazon Q, consulte Activación de Amazon Q Supply Chain y Uso de Amazon Q Supply Chain in en la Supply Chain documentación.

Automatice la evaluación de recursos de AWS

Naveen Suthar, Arun Bagal, Manish Garg y Sandeep Gawande, Amazon Web Services

Resumen

Este patrón describe un enfoque automatizado para configurar las capacidades de evaluación de recursos mediante AWS Cloud Development Kit (AWS CDK). Usando este patrón, los equipos de operaciones recopilan los detalles de auditoría de los recursos de forma automatizada y ven los detalles de todos los recursos implementados en una cuenta de AWS en un único panel. Esto resulta útil en los siguientes casos de uso:

- Identificar las herramientas de infraestructura como código (IaC) y aislar los recursos creados por diferentes soluciones de IaC, como HashiCorp Terraform, AWS CloudFormation, AWS CDK y AWS Command Line Interface (AWS CLI)
- Obtener información de auditoría de recursos

Esta solución también ayuda al equipo directivo a obtener información sobre los recursos y las actividades de una cuenta de AWS desde un único panel.

Nota: Amazon Quick Sight es un servicio de pago. Antes de ejecutarlo para analizar los datos y crear un panel de control, consulta los precios de Amazon Quick Sight.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Roles y permisos de AWS Identity and Access Management (IAM) con acceso a recursos de aprovisionamiento
- Una cuenta Amazon Quick creada con acceso a Amazon Simple Storage Service (Amazon S3) y Amazon Athena
- Se ha instalado la versión 2.55.1 o posterior de AWS CDK
- Se ha instalado la versión 3.9 o posterior de Python

Limitaciones

- Esta solución se implementa en una única cuenta de AWS.
- La solución no rastreará los eventos que ocurrieron antes de su implementación, a menos que AWS ya CloudTrail estuviera configurado y almacenando datos en un bucket de S3.

Versiones de producto

- CDK de AWS, versión 2.55.1 o posterior
- Python, versión 3.9 o posterior

Arquitectura

Pila de tecnología de destino

- Amazon Athena
- AWS CloudTrail
- AWS Glue
- AWS Lambda
- Amazon Quick Suite
- Amazon S3

Arquitectura de destino

El código de AWS CDK implementará todos los recursos necesarios para configurar las capacidades de evaluación de recursos en una cuenta de AWS. El siguiente diagrama muestra el proceso de envío de CloudTrail registros a AWS Glue, Amazon Athena y Quick Sight.

1. CloudTrail envía los registros a un depósito de S3 para su almacenamiento.
2. Una notificación de evento invoca una función de Lambda que procesa los registros y genera datos filtrados.
3. Los datos filtrados se almacenan en otro bucket de S3.
4. Se configura un rastreador de AWS Glue en los datos filtrados del bucket de S3 para crear un esquema en la tabla del catálogo de datos de AWS Glue.
5. Los datos filtrados están listos para que Amazon Athena los consulte.
6. Quick Sight accede a los datos consultados para su visualización.

Automatización y escala

- Esta solución se puede escalar de una cuenta de AWS a varias cuentas de AWS si existe un registro que abarque a toda la organización en AWS CloudTrail Organizations. CloudTrail Al implementarla a nivel organizacional, también puede usar esta solución para obtener detalles de auditoría de recursos para todos los recursos necesarios.
- Este patrón emplea recursos sin servidor de AWS para implementar la solución.

Tools (Herramientas)

Servicios de AWS

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.
- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura en la nube de AWS en código.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS le CloudTrail ayuda a auditar la gobernanza, el cumplimiento y el riesgo operativo de su cuenta de AWS.
- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos. Este patrón emplea un rastreador de AWS Glue y una tabla del catálogo de datos de AWS Glue.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Quick es un servicio de inteligencia empresarial (BI) a escala de nube que le ayuda a visualizar, analizar y elaborar informes sobre sus datos en un único panel de control.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Repositorio de código

El código de este patrón está disponible en el GitHub infrastructure-assessment-iac-automationrepositorio.

El repositorio de código contiene los siguientes archivos y carpetas:

- Carpeta `lib` – los archivos Python de constructo de AWS CDK usados para crear los recursos de AWS
- `src/lambda_code` – El código Python que se ejecuta en la función de Lambda
- `requirements.txt` – La lista de todas las dependencias de Python que se deben instalar
- `cdk.json` – El archivo de entrada que proporciona los valores necesarios para activar los recursos

Prácticas recomendadas

Configure la supervisión y las alertas para las funciones de Lambda de AWS. Para obtener más información, consulte Supervisión y solución de problemas de funciones de Lambda. Para obtener más información sobre las prácticas recomendadas generales en el uso de funciones de Lambda, consulte la documentación de AWS.

Epics

Configure su entorno

Tarea	Descripción	Habilidades requeridas
Clone el repositorio en su máquina local.	Para clonar el repositorio, ejecute el comando `git clone https://github.com/aws-samples/infrastructure-assessment-iac-automation.git` .	AWS DevOps, DevOps ingeniero
Configure el entorno virtual de Python e instale las dependencias necesarias.	Para configurar y activar el entorno virtual de Python, ejecute el siguiente comando.	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	`cd infrastructure-assessment-iac-automation`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	
	Ejecute el comando `pip install -r requirements.txt` para configurar las dependencias necesarias.	

Configure el entorno de AWS CDK y sintetice el código de AWS CDK.	1. Para configurar el entorno de AWS CDK en su cuenta de AWS, ejecute el comando `cdk bootstrap aws://ACCOUNT-NUMBER/REGION` . 2. Para convertir el código en una configuración de CloudFormation pila de AWS, ejecute el comando`cdk synth`.	AWS DevOps, DevOps ingeniero

Configuración de las credenciales de AWS en su máquina local

Tarea	Descripción	Habilidades requeridas
Exporte las variables de cuenta y región en las que se implementará la pila.	Para proporcionar las credenciales de AWS para AWS CDK mediante variables de entorno, ejecute los siguientes comandos.	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`export CDK_DEFAU LT_ACCOUNT=<12 Digit AWS Account Number>` `export CDK_DEFAU LT_REGION=<region>`	
Configure el perfil de AWS CLI.	Para configurar el perfil de AWS CLI para la cuenta, siga las instrucciones de la documentación de AWS.	AWS DevOps, DevOps ingeniero

Configure e implemente la herramienta de evaluación de recursos

Tarea	Descripción	Habilidades requeridas
Implementar recursos en la cuenta.	Para implementar recursos en la cuenta de AWS mediante AWS CDK, haga lo siguiente: 1. En la raíz del repositor io clonado, en el archivo `cdk.json`, introduzca entradas para los siguientes parámetros: • `s3_context` • `ct_context` • `kms_context` • `lambda_context` • `glue_context` • `qs_context` Estos valores definen la nomenclatura y la configura ción de los recursos. Los	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	valores predeterminados están establecidos, y se pueden cambiar si es necesario. **Note** Para evitar que aparezca un error que indique que el bucket de S3 ya existe, asegúrese de proporcionar nombres exclusivos para `s3_context` en las secciones `ct` y `output`. 2. Ejecute el `cdk deploy` comando para implementar los recursos. El `cdk deploy` comando crea un CloudTrail recurso para registrar eventos y guardar el archivo de registro en el depósito S3 de entrada. La función de Lambda procesa los archivos de registros de la ruta. Los resultados filtrados se almacenan en el depósito S3 de salida y están listos para que	

Tarea	Descripción	Habilidades requeridas
	Amazon Athena y Amazon Quick Sight los consuman.	

Tarea	Descripción	Habilidades requeridas
Ejecute el rastreador de AWS Glue y cree la tabla del catálogo de datos.	El rastreador de AWS Glue se usa para mantener el esquema de datos dinámico. La solución crea y actualiza las particiones en la tabla del catálogo de datos de AWS Glue, ejecutando el rastreador periódicamente según lo definido en el programador de rastreo de AWS Glue. Una vez que los datos estén disponibles en el bucket de S3 de salida, siga estos pasos para ejecutar el rastreador de AWS Glue y crear el esquema de la tabla del catálogo de datos para realizar las pruebas: 1. Inicie sesión en la consola de administración de AWS y vaya a la consola de AWS Glue. 2. En el panel de navegación, en Catálogo de datos, seleccione rastreador. 3. Seleccione el rastreador `iac-tool-qa-resource-iac-json-crawler` . 4. Ejecute el rastreador. 5. Una vez que el rastreador se ejecuta correctamente, crea una tabla de Catálogo de datos de AWS Glue.	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Quick Sight utilizará la tabla para visualizar los datos. **Note** El código de AWS CDK configura el rastreador de AWS Glue para que se ejecute en un momento determina do, pero también puede ejecutarlo bajo demanda.	
Implemente la construcción Quick Sight.	1. Para implementar la construcción Quick Sight, descomente el código que hay entre `#QuickSig ht setup - start` y dentro`#QuickSig ht setup – ends . resource_iac_tool_ stack.py` 2. Tras eliminar los comentari os, ejecute el `cdk deploy` comando para crear `QuickSigh t DataSource` y `QuickSight DataSet` en la cuenta de Quick Sight.	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Cree el panel de control de Quick Sight.	Para crear el panel y el análisis de Quick Sight de ejemplo, haga lo siguiente: 1. Diríjase a la consola Quick Sight y seleccione la región de AWS en la que se implementan los recursos. 2. En el panel de navegación, elija Conjuntos de datos y valide que se `ct-operations-iac-ds` haya creado un conjunto de datos denominado en el conjunto de datos de Quick Sight. Si no ve el conjunto de datos, vuelva a implementar la construcción de Quick Sight. 3. Seleccione el conjunto de datos `ct-operations-iac-ds` y elija USAR EN ANÁLISIS. 4. Seleccione la hoja predeterminada. 5. Seleccione las columnas correspondientes de la lista de campos de la izquierda. 6. Tras seleccionar las columnas necesarias, seleccione el tipo de	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	visualización adecuado para los datos. Para obtener más información, consulte Inicio de un análisis en Amazon Quick Sight y Tipos visuales en Amazon Quick Sight.	

Limpie todos los recursos de AWS de la solución

Tarea	Descripción	Habilidades requeridas
Elimine los recursos de AWS.	1. Para eliminar los recursos de AWS implementados por la solución, ejecute el comando `cdk destroy`. 2. Elimine todos los objetos de los dos buckets de S3 y, a continuación, elimine los buckets. Para obtener más informaci ón, consulte Eliminación de un bucket.	AWS DevOps, DevOps ingeniero

Configure funciones adicionales además de la automatización de la herramienta de evaluación de recursos de AWS

Tarea	Descripción	Habilidades requeridas
Supervise y limpie los recursos creados manualmen te.	(Opcional) Si su organización tiene requisitos de conformid ad para crear recursos con las	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	herramientas de IaC, puede satisfacerlos automatizando las herramientas de evaluación de recursos de AWS para obtener los recursos aprovisionados manualmente. También puede usar la herramienta para importar los recursos a una herramienta de IaC o volver a crearlos. Realice las siguientes tareas de alto nivel para supervisar los recursos aprovisionados de manera manual: 1. Implemente la automatización de la herramienta de evaluación de recursos de AWS. 2. Configure una función de Lambda para consultar las tablas de Athena a diario, buscar los datos relevantes sobre los recursos aprovisionados manualmente y exportarlos a un archivo de valores separados por comas (CSV). 3. Una vez ejecutada la función de Lambda, puede enviar una notificación con los datos necesarios a las respectivas partes interesadas.	

Tarea	Descripción	Habilidades requeridas
	4. El archivo .csv se puede almacenar en el bucket de S3 para prolongar su retención. 5. En función de la informaci ón del archivo .csv, elimine los recursos creados manualmente o impórtelo s a una solución IaC existente.	

Resolución de problemas

Problema	Solución
AWS CDK devuelve errores.	Para obtener ayuda con los errores de AWS CDK, consulte Solución de problemas comunes de AWS CDK.

Recursos relacionados

- Creación de funciones de Lambda con Python
- Introducción a AWS CDK
- Utilización de AWS CDK en Python
- Creando un CloudTrail registro
- Comience con Amazon Quick Sight

Información adicional

Cuentas múltiples

Para configurar la credencial de AWS CLI para múltiples cuentas, use los perfiles de AWS. Para obtener más información, consulte la sección Configurar varios perfiles en Configurar AWS CLI.

Comandos de AWS CDK

Cuando trabaje con AWS CDK, recuerde los siguientes comandos útiles:

- Muestra todas las pilas de la aplicación

```
cdk ls
```

- Emite la plantilla de AWS CloudFormation sintetizada

```
cdk synth
```

- Implementa la pila en la cuenta y región de AWS predeterminadas

```
cdk deploy
```

- Compara la pila implementada con el estado actual

```
cdk diff
```

- Abre la documentación de AWS CDK

```
cdk docs
```

Instalar sistemas SAP automáticamente mediante herramientas de código abierto

Guilherme Sesterheim, Amazon Web Services

Resumen

Este patrón muestra cómo automatizar la instalación de sistemas SAP mediante el uso de herramientas de código abierto para crear los recursos siguientes:

- Una base de datos SAP S/4HANA 1909
- Una instancia de SAP ABAP Central Services (ASCS)
- Una instancia de servidor principal de aplicaciones (PAS) de SAP

HashiCorp Terraform crea la infraestructura del sistema SAP y Ansible configura el sistema operativo (SO) e instala las aplicaciones SAP. Jenkins ejecuta la instalación.

Con esta configuración, la instalación de sistemas SAP se convierte en un proceso repetible, lo que puede ayudar a aumentar la eficiencia y la calidad de la implementación.

> **Note**
>
> El código de ejemplo que se proporciona en este patrón funciona tanto para sistemas de alta disponibilidad (HA) como para sistemas que no lo son.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un bucket de Amazon Simple Storage Service (Amazon S3) que contenga todos sus archivos multimedia de SAP
- Una entidad principal de Identity and Access Management (IAM) de AWS con una clave de acceso y una clave secreta y con los siguientes permisos:
  - Permisos de solo lectura: Amazon Route 53, AWS Key Management Service (AWS KMS)

  - Permisos de lectura y escritura: Amazon S3, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic File System (Amazon EFS), IAM, Amazon CloudWatch, Amazon DynamoDB
- Una zona alojada privada de Route 53
- Una suscripción a Red Hat Enterprise Linux para SAP con Imagen de máquina de Amazon (AMI) de alta disponibilidad y Update Services 8.2 en Amazon Marketplace
- Una clave gestionada de cliente de AWS KMS
- Un par de claves Secure Shell (SSH)
- Un grupo de EC2 seguridad de Amazon que permite la conexión SSH en el puerto 22 desde el nombre de host donde instalas Jenkins (lo más probable es que el nombre de host sea localhost)
- Vagrant by instalado y configurado HashiCorp
- VirtualBoxinstalado y configurado por Oracle
- Familiaridad con Git, Terraform, Ansible y Jenkins

Limitaciones

- Solamente SAP S/4HANA 1909 se ha probado completamente para este escenario específico. El código de Ansible de ejemplo de este patrón requiere modificaciones si utiliza otra versión de SAP HANA.
- El procedimiento de ejemplo de este patrón funciona para los sistemas operativos Mac y Linux. Algunos de los comandos solo se pueden ejecutar en terminales basados en Unix. Sin embargo, puede lograr un resultado similar utilizando diferentes comandos y un sistema operativo Windows.

Versiones de producto

- SAP S/4HANA 1909
- Red Hat Enterprise Linux (RHEL) versión 8.2 o posterior

Arquitectura

El diagrama siguiente muestra un ejemplo de flujo de trabajo que utiliza herramientas de código abierto para automatizar la instalación de sistemas SAP en una cuenta de AWS:

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Jenkins orquesta la instalación del sistema SAP mediante la ejecución del código de Terraform y Ansible.
2. El código de Terraform crea la infraestructura del sistema SAP.
3. El código de Ansible configura el sistema operativo e instala las aplicaciones SAP.
4. En una instancia de Amazon se instalan una base de datos SAP S/4HANA 1909, una instancia de ASCS y una instancia de PAS que incluyen todos los requisitos previos definidos. EC2

> **Note**
>
> El ejemplo de configuración de este patrón crea automáticamente un bucket de Amazon S3 en su cuenta de AWS para almacenar el archivo de estado de Terraform.

Pila de tecnología

- Terraform
- Ansible
- Jenkins
- Una base de datos SAP S/4HANA 1909
- Una instancia de SAP ASCS
- Una instancia de SAP PAS
- Amazon EC2

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.

- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Otras herramientas

- HashiCorp Terraform es una aplicación de interfaz de línea de comandos que le ayuda a usar código para aprovisionar y administrar la infraestructura y los recursos de la nube.
- Ansible es una herramienta de código abierto de configuración como código (CaC) que ayuda a automatizar las aplicaciones, las configuraciones y la infraestructura de TI.
- Jenkins es un servidor de código abierto de automatización que permite a los desarrolladores crear, probar e implementar su software.

Código

El código de este patrón está disponible en el repositorio -jenkins-ansible. GitHub aws-install-sap-with

Epics

Configurar los requisitos previos

Tarea	Descripción	Habilidades requeridas
Añada sus archivos multimedia SAP a un bucket de Amazon S3.	Cree un bucket de Amazon S3 que contenga todos sus archivos multimedia SAP. **Important** Asegúrese de seguir la jerarquía de carpetas de AWS Launch Wizard para S/4HANA en la documentación de Launch Wizard.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Instala. VirtualBox	Instalación y configuración VirtualBoxpor parte de Oracle.	DevOps ingeniero
Instalar Vagrant.	Instale y configure Vagrant mediante. HashiCorp	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Configurar su cuenta de AWS.	1. Compruebe que tiene una entidad principal de IAM con una clave de acceso y una clave secreta, y que tiene los permisos siguientes: • Permisos de solo lectura: Amazon Route 53, AWS Key Management Service (AWS KMS) • Permisos de lectura y escritura: Amazon S3, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic File System (Amazon EFS), IAM, Amazon CloudWatch, Amazon DynamoDB 2. Guarde la clave de acceso y la clave secreta de la entidad principal de IAM para consultarlas más adelante. 3. Cree una zona alojada privada de Route 53, si aún no la tiene. Guarde el nombre de la zona (por ejemplo, sapteam.net) para consultarlo más adelante. 4. Suscríbase a Red Hat Enterprise Linux para SAP con AMI de alta disponibilidad y Update Services 8.2	AWS general

Tarea	Descripción	Habilidades requeridas
	en Amazon Marketplace. Guarde el ID de AMI (por ejemplo, ami-0000000) para consultarlo más adelante. 5. Cree una clave gestionada de cliente de AWS KMS. Guarde el nombre de recurso de Amazon (ARN) de la clave de cifrado para consultarlo más adelante. **Note** A continuación, se muestra un ejemplo de ARN de una clave administrada por el cliente de AWS KMS: arn:aws:kms:us-east-1:123412341234:key/uuid 6. Cree un par de claves SSH. Guarde el nombre del par de claves y el archivo .pem para consultarlos más adelante. 7. Crea un grupo de EC2 seguridad de Amazon que permita la conexión SSH en el puerto 22 desde el nombre de host en el que instalas Jenkins. Guarde el ID del grupo de seguridad	

Tarea	Descripción	Habilidades requeridas
	para consultarlo más adelante. **Note** Lo más probable es que el nombre de host sea localhost.	

Crear y ejecutar su instalación de SAP

Tarea	Descripción	Habilidades requeridas
Clona el repositorio de código desde. GitHub	Clona el repositorio aws-install-sap-with-jenkins-ansible en. GitHub	DevOps ingeniero
Inicie el servicio de Jenkins.	Abra la terminal de Linux. A continuación, navegue hasta la carpeta local que contiene la carpeta del repositorio de código clonado y ejecute el comando siguiente: `sudo vagrant up` **Note** Jenkins tarda unos 20 minutos en iniciarse. El comando devuelve el mensaje Service is up and running (El servicio	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	está funcionando) cuando el funcionamiento es correcto.	
Abra Jenkins en un navegador web e inicie sesión.	1. En un navegador web, escriba http://localhost:5555. Se abrirá Jenkins. 2. Inicie sesión en Jenkins usando admin como nombre de usuario y my_secret_pass_from_vault como contraseña.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Configure los parámetros de instalación de su sistema SAP.	1. En Jenkins, seleccione Manage Jenkins (Administrar Jenkins). A continuación, seleccione Manage Credentials (Administrar credenciales). Se muestra una lista de variables de credenciales que puede configurar. 2. Configure todas las variables de credenciales siguientes: • En AWS_ACCOUNT_CREDENTIALS, introduzca el ID de la clave de acceso y el ID de la clave de acceso secreta del director de IAM. • Para AMI_ID, escriba el ID de AMI de Red Hat Enterprise Linux para SAP con el ID de AMI del AMI alta disponibilidad y Update Services 8.2. • Para KMS_KEY_ARN, escriba el ARN de la clave gestionada de cliente de AWS KMS. • Para SSH_KEYPAIR_NAME, escriba el nombre del par de claves	Administrador de sistemas de AWS, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	SSH, sin el tipo de archivo .pem. • Para SSH_KEYPAIR_FILE, escriba el nombre completo del archivo .pem del par de claves (por ejemplo, mykeypair.pem). Asegúrese de cargar también el archivo .pem de los pares de claves en Jenkins. • Para S3_ROOT_FOLDER_INSTALL_FILES, introduzca el nombre del depósito de Amazon S3 y de la carpeta, si procede, (por ejemplo, s3:///S4H1909) que contiene los archivos multimedia de SAP. my-media-bucket • Para PRIVATE_DNS_ZONE_NAME, escriba el nombre de su zona alojada privada de Route 53 (por ejemplo, myprivatecompanyurl.net). • Para VPC_ID, escriba el ID de VPC (por ejemplo, vpc-12345) de la VPC de Amazon en la que va a crear los recursos de SAP. • Para SUBNET_IDS, introduzca dos subredes públicas IDs si trabaja en un entorno de prueba (para	

Tarea	Descripción	Habilidades requeridas
	futuras capacidades de alta disponibilidad). Si trabaja en un entorno de producción, se recomienda utilizar dos subredes privadas con un host bastión. • En SECURITY_GROUP_ID, introduce el ID del grupo de EC2 seguridad de Amazon que permite la conexión SSH en el puerto 22 desde el nombre de host en el que instalaste Jenkins. **Note** Puede configurar los demás parámetros no obligatorios según sea necesario, en función de su caso de uso. Así, por ejemplo, puede cambiar el ID del sistema SAP (SID) de las instancias, la contraseña predeterminada, los nombres y las etiquetas del sistema SAP. Todas las variables obligatorias muestran Required (Obligato	

Tarea	Descripción	Habilidades requeridas
	ria) al principio de sus nombres.	

Tarea	Descripción	Habilidades requeridas
Ejecute la instalación de su sistema SAP.	1. En Jenkins, seleccione Jenkins Home. A continuación, seleccione 3 instancias de SAP Hana+ASCS+PAS. 2. Seleccione Spin up and install (Poner en marcha e instalar). A continuación, seleccione Main (Principal). 3. Seleccione Build now (Crear ahora). Para obtener información sobre los pasos del proceso, consulte la sección Understanding the pipeline steps (Comprender los pasos del proceso) de Automating SAP installation with open-source tools (Automatizar la instalación de SAP con herramientas de código abierto) en el blog de AWS. **Note** Si se produce un error, mueva el cursor sobre el cuadro de error rojo que aparece y seleccione Registros. Aparecen los registros del paso del proceso en el que se produjo el error. La mayoría	DevOps ingeniero, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	de los errores se producen debido a una configuración de parámetros incorrecta.	

Recursos relacionados

- DevOps para SAP: instalación de SAP: de 2 meses a 2 horas (videoteca de DevOps Enterprise Summit)

Automatice la implementación de productos y la cartera de AWS Service Catalog mediante AWS CDK

Sandeep Gawande, Viyoma Sachdeva y RAJNEESH TYAGI, Amazon Web Services

Resumen

AWS Service Catalog le ayuda a administrar de forma centralizada los catálogos de servicios de TI o productos aprobados para su uso en el entorno de AWS de su organización. La cartera es una colección de productos que, además, contiene información de configuración. Con AWS Service Catalog, puede crear una cartera de productos personalizada para cada tipo de usuario de su organización y conceder acceso a la cartera de productos apropiada. Después, esos usuarios pueden implementar rápidamente cualquier producto que necesiten de la cartera.

Si tiene una infraestructura de red compleja, como arquitecturas en múltiples regiones y cuentas, se recomienda crear y administrar las carteras de Service Catalog en una única cuenta centralizada. Este patrón describe cómo usar AWS Cloud Development Kit (AWS CDK) para automatizar la creación de carteras de Service Catalog en una cuenta central, conceder a los usuarios finales acceso a ellas y, opcionalmente, aprovisionar productos en una o más cuentas de AWS de destino. Esta ready-to-use solución crea las carteras de Service Catalog en la cuenta de origen. También, de forma opcional, aprovisiona los productos en las cuentas de destino mediante AWS CloudFormation stacks y le ayuda a TagOptions configurarlos:

- AWS CloudFormation StackSets: puede utilizarlos StackSets para lanzar productos de Service Catalog en varias regiones y cuentas de AWS. La implementación de esta solución le permite aprovisionar productos automáticamente. Para obtener más información, consulte Uso de AWS CloudFormation StackSets (documentación de Service Catalog) y StackSets conceptos (CloudFormation documentación).
- TagOption biblioteca: puede administrar las etiquetas de los productos aprovisionados mediante la TagOption biblioteca. A TagOptiones un par clave-valor administrado en AWS Service Catalog. No es una etiqueta de AWS, pero sirve como plantilla para crear una etiqueta de AWS basada en TagOption. Para obtener más información, consulte la TagOption biblioteca (documentación de Service Catalog).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa que quiera usar como cuenta de supervisión para administrar carteras de Service Catalog.
- Si usa esta solución para aprovisionar productos en una o más cuentas de destino, la cuenta de destino debe existir ya y estar activa.
- Permisos de AWS Identity and Access Management (IAM) para acceder a AWS Service Catalog CloudFormation, AWS y AWS IAM.

Versiones de producto

- AWS CDK versión 2.27.0

Arquitectura

Pila de tecnología de destino

- Carteras de Service Catalog en una cuenta de AWS centralizada
- Productos de Service Catalog implementados en la cuenta de destino

Arquitectura de destino

1. En la cuenta de cartera (u origen), debe actualizar el archivo config.json con la información de la cuenta de AWS, la región de AWS, el rol de IAM, la cartera y el producto para su caso de uso.
2. Implemente la aplicación AWS CDK.
3. La aplicación AWS CDK asume el rol de IAM de implementación y crea las carteras y los productos de Service Catalog definidos en el archivo config.json.

   Si ha configurado StackSets la implementación de productos en una cuenta de destino, el proceso continúa. Si no lo configuraste StackSets para aprovisionar ningún producto, el proceso está completo.
4. La aplicación AWS CDK asume la función de StackSet administrador e implementa el conjunto de CloudFormation pilas de AWS que definió en el archivo config.json.
5. En la cuenta de destino, StackSets asume la función de StackSet ejecución y aprovisiona los productos.

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- El Kit de herramientas de AWS CDK es un kit de desarrollo en la nube de línea de comandos que le ayuda a interactuar con su aplicación AWS CDK.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Service Catalog le ayuda a administrar de forma centralizada los catálogos de servicios de TI aprobados para AWS. Los usuarios finales pueden implementar rápidamente solo los servicios de TI aprobados que necesitan, de acuerdo con las limitaciones establecidas por su organización.

Repositorio de código

El código de este patrón está disponible en GitHub, en el aws-cdk-servicecatalog-automationrepositorio. El repositorio de código contiene los siguientes archivos y carpetas:

- cdk-sevicecatalog-app— Esta carpeta contiene la aplicación AWS CDK para esta solución.
- config: esta carpeta contiene el archivo config.json y la CloudFormation plantilla para implementar los productos de la cartera de Service Catalog.
- config/config.json: este archivo contiene toda la información de configuración. Actualice este archivo para personalizar esta solución según su caso de uso.
- config/templates: esta carpeta contiene las CloudFormation plantillas de los productos de Service Center.
- setup.sh: este script implementa la solución.
- uninstall.sh: este script elimina la pila y todos los recursos de AWS creados al implementar esta solución.

Para usar el código de muestra, siga las instrucciones en sección Epics.

Prácticas recomendadas

- Los roles de IAM usados para implementar esta solución deben cumplir con el principio de privilegio mínimo (documentación de IAM).
- Respete las Prácticas recomendadas para desarrollar aplicaciones en la nube con AWS CDK (publicación del blog de AWS).
- Siga las prácticas CloudFormation recomendadas de AWS (CloudFormation documentación).

Epics

Configure su entorno

Tarea	Descripción	Habilidades requeridas

Instale el kit de herramientas de AWS CDK.	Asegúrese de tener instalado el kit de herramientas de AWS CDK. Ejecute el siguiente comando para confirmar si está instalado y verifique la versión.
	`cdk --version`
	Si el kit de herramientas de AWS CDK no está instalado, ejecute el siguiente comando para instalarlo.
	`npm install -g aws-cdk@2.27.0`
	Si la versión del kit de herramientas de AWS CDK es anterior a la 2.27.0, ejecute el siguiente comando para actualizarla a la versión 2.27.0.
		AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`npm install -g aws-cdk@2.27.0 --force`	

Clonar el repositorio.	Escriba el siguiente comando. En Clonar el repositorio, en la sección Información adicional, puede copiar el comando completo que contiene la URL del repositorio. Esto clona el aws-cdk-servicecatalog-automationrepositorio desde GitHub.
	`git clone <repository-URL>.git`
	Se creará la carpeta `cd aws-cdk-servicecatalog-automation` en el directorio de destino. Ejecute el siguiente comando para navegar a esta carpeta.
	`cd aws-cdk-servicecatalog-automation`
		AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Configure las credenciales de AWS.	Introduzca los comandos siguientes. Se exportan las siguientes variables, que definen la cuenta y la región de AWS en las que se va a implementar la pila.
	`export CDK_DEFAU LT_ACCOUNT=<12-digit AWS account number>`
	`export CDK_DEFAU LT_REGION=<AWS Region>`
	Las credenciales de AWS para AWS CDK se proporcio nan a través de variables de entorno.
		AWS DevOps, DevOps ingeniero

Configurar permisos de roles de IAM para usuarios finales.	Si va a usar roles de IAM para conceder acceso a la cartera y a los productos que contiene, estos roles deben tener permisos para que los asuma la entidad principal servicecatalog.amazonaws.co m. Para obtener instrucciones sobre cómo conceder estos permisos, consulte Habilitar acceso de confianza con Service Catalog (document ación de AWS Organizations).	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Configure las funciones de IAM requeridas por StackSets.	Si va StackSets a aprovisionar automáticamente los productos en las cuentas de destino, debe configurar las funciones de IAM que administran y ejecutan el conjunto apilado. 1. En la cuenta de origen, confirme que ya existe `AWSCloudFormationStackSetAdministrationRole` . En la cuenta de destino, confirme que ya existe `AWSCloudFormationStackSetExecutionRole` . Si estos roles ya existen, puede pasar a la siguiente épica. 2. Siga las instrucciones de Conceder permisos autogestionados (documentación de IAM) para crear el rol de administración de conjunto de pilas en la cuenta de cartera y crear el rol de ejecución en cada cuenta de destino.	AWS DevOps, DevOps ingeniero

Personalice e implemente la solución

Tarea	Descripción	Habilidades requeridas
Crea las CloudFormation plantillas.	En la `config/templates` carpeta, crea CloudForm ation plantillas para cualquier producto que desees incluir en tus carteras. Para obtener más información, consulte Trabajar con CloudFormation plantillas de AWS (CloudFor mation documentación).	Desarrollador de aplicacio nes, AWS DevOps, DevOps ingeniero
Personalice el archivo de configuración.	En la carpeta `config`, abra el archivo config.json y defina los parámetros según correspon da a su caso de uso. Los siguientes parámetros son obligatorios a menos que se indique lo contrario: En la sección `portfolio s` , defina los siguientes parámetros para crear una o más carteras de Service Catalog: • `portfolioName` : El nombre de la cartera. • `providerName` : El nombre de la persona, equipo u organización que administra la cartera. • `description` : Descripci ón breve de la cartera.	Desarrollador de aplicacio nes, DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• `roles`: (Opcional) Nombres de rol de IAM que deban tener acceso a esta cartera. Los usuarios con este rol pueden acceder a los productos de esta cartera. • `users`: (Opcional) Nombres de todos los usuarios de IAM que deban tener acceso a esta cartera y sus productos. • `groups`: (Opcional) Nombres de cualquier grupo de usuarios de IAM que deban tener acceso a esta cartera y sus productos. ⚠ Warning Los usuarios de IAM tienen credenciales de larga duración, lo que supone un riesgo de seguridad . Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios únicament e los permisos que necesitan para realizar la tarea y que los	

Tarea	Descripción	Habilidades requeridas
	elimine cuando ya no los necesiten. **Important** `roles`, `users` y `groups` son todos parámetros opcionales, pero si no define uno de ellos, nadie podrá ver la cartera de productos en la consola de Service Catalog. Defina al menos uno de estos parámetros. Para obtener más información, consulte Conceder permisos a los usuarios finales de Service Catalog (documentación de Service Catalog). • (Opcional) En la `tagOption` sección, defina TagOptions para los productos: • `key`— Nombre de la TagOption clave	

Tarea	Descripción	Habilidades requeridas
	• `value`— Valores de cadena permitidos para la TagOption Para obtener más información, consulte la TagOption biblioteca (documentación de Service Catalog). • En la sección `products`, defina los siguientes parámetros para los productos: • `portfolioName` – Nombre de la cartera a la que se agregará el producto. Puede especificar solo una cartera. • `productName` : El nombre del producto. • `owner`: El propietario del producto. • `productVersionName` : Nombre de la versión del producto en un valor de cadena, por ejemplo `v1`. • `templatePath` — La ruta del archivo de la CloudFormation plantilla del producto. • `deployWithStackSets` — (Opcional) Especifique una o más cuentas	

Tarea	Descripción	Habilidades requeridas
	y regiones en las que desee StackSets aprovisionar automáticamente los productos de las carteras. Si usa esta opción de implementación, es obligatorio introducir todos los parámetros de esta sección: • `accounts`: Las cuentas de destino. • `regions`: Las regiones de destino. • `stackSetAdministrationRoleName` — El nombre del rol de IAM utilizado para administrar la StackSets configuración. No cambie este valor. El rol debe tener este nombre exacto. • `stackSetExecutionRoleName` : El nombre del rol de IAM en la cuenta de destino que implementa las instancias de la pila. No cambie este valor. El rol debe tener este nombre exacto.	

Tarea	Descripción	Habilidades requeridas
	Para ver un ejemplo de un archivo de configuración completo, consulte el Ejemplo de archivo de configuración en la sección Información adicional.	
Implemente la solución.	Escriba el siguiente comando. Esto implementa la aplicación AWS CDK y aprovisiona las carteras y productos de Service Catalog, tal y como se especifica en el archivo config.json. `sh +x setup.sh`	Desarrollador de aplicaciones, DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Comprobar la implementación.	Compruebe que la implementación se ha realizado correctamente de la siguiente manera: 1. Inicie sesión en la consola de administración de AWS con credenciales que puedan acceder a una o más de las carteras que definió en el archivo de configuración. 2. Abra la consola de Service Catalog en https://console.aws.amazon.com/servicecatalog/. 3. En el panel de navegación, en Aprovisionamiento, elija Productos. Compruebe que ve una lista de los productos que especificó para la cartera. 4. Siga las instrucciones de Lanzamiento de un producto (documentación de Service Catalog) para lanzar uno de los productos disponibles. Confirme que las versiones y etiquetas de los productos disponibles coincidan con los valores que proporcionó en el archivo de configuración.	AWS general

Tarea	Descripción	Habilidades requeridas
	5. Si opta por aprovisionar automáticamente los productos en una o más cuentas de destino mediante StackSets, haga lo siguiente: a. Inicie sesión con credenciales que le otorguen permisos para ver los productos aprovisionados en una de las cuentas de destino. b. En la consola de Service Catalog, en el panel de navegación, en Aprovisionamiento, seleccione Productos aprovisionados. c. Confirme que los productos esperados aparecen en la lista.	

Tarea	Descripción	Habilidades requeridas
(Opcional) Actualice las carteras y los productos.	Si desea usar esta solución para actualizar las carteras o los productos, o para aprovisionar nuevos productos: 1. Realice los cambios necesarios en el archivo config.json. 2. Añada o modifique CloudFormation las plantillas que necesite en la `config/template` carpeta. 3. Implementar la solución. Por ejemplo, puede añadir carteras adicionales o aprovisionar más recursos. La aplicación AWS CDK implementará solo los cambios. Si no hay cambios en las carteras o los productos implementados anteriormente, la reimplementación no les afectará.	Desarrollador de aplicaciones, DevOps ingeniero, AWS general

Elimine la solución

Tarea	Descripción	Habilidades requeridas
(Opcional) Elimine los recursos de AWS implementados por esta solución.	Si desea eliminar un producto aprovisionado, siga las instrucciones de Eliminar	AWS DevOps, DevOps ingeniero, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	productos aprovisionados (documentación de Service Catalog). Si desea eliminar todos los recursos creados por esta solución, ejecute el siguiente comando. `sh uninstall.sh`	

Recursos relacionados

- Biblioteca de constructos de AWS Service Catalog (referencia de API de AWS)
- StackSets conceptos (CloudFormation documentación)
- AWS Service Catalog (marketing de AWS)
- Uso de Service Catalog con AWS CDK (taller de AWS)

Información adicional

Clone el repositorio

Introduzca el siguiente comando desde el que desea clonar el repositorio GitHub.

```
git clone https://github.com/aws-samples/aws-cdk-servicecatalog-automation.git
```

Ejemplo de archivo de configuración

El siguiente es un archivo de muestra config.json con valores de ejemplo.

```
{
    "portfolios": [
        {
            "displayName": "EC2 Product Portfolio",
            "providerName": "User1",
            "description": "Test1",
```

```
            "roles": [
                "<Names of IAM roles that can access the products>"
            ],
            "users": [
                "<Names of IAM users who can access the products>"
            ],
            "groups": [
                "<Names of IAM user groups that can access the products>"
            ]
        },
        {
            "displayName": "Autoscaling Product Portfolio",
            "providerName": "User2",
            "description": "Test2",
            "roles": [
                "<Name of IAM role>"
            ]
        }
    ],
    "tagOption": [
        {
            "key": "Group",
            "value": [
                "finance",
                "engineering",
                "marketing",
                "research"
            ]
        },
        {
            "key": "CostCenter",
            "value": [
                "01",
                "02",
                "03",
                "04"
            ]
        },
        {
            "key": "Environment",
            "value": [
                "dev",
                "prod",
                "stage"
```

```
            ]
        }
    ],
    "products": [
        {
            "portfolioName": "EC2 Product Profile",
            "productName": "Ec2",
            "owner": "owner1",
            "productVersionName": "v1",
            "templatePath": "../../config/templates/template1.json"
        },
        {
            "portfolioName": "Autoscaling Product Profile",
            "productName": "autoscaling",
            "owner": "owner1",
            "productVersionName": "v1",
            "templatePath": "../../config/templates/template2.json",
            "deployWithStackSets": {
                "accounts": [
                    "012345678901",
                ],
                "regions": [
                    "us-west-2"
                ],
                "stackSetAdministrationRoleName":
 "AWSCloudFormationStackSetAdministrationRole",
                "stackSetExecutionRoleName": "AWSCloudFormationStackSetExecutionRole"
            }
        }
    ]
}
```

Automatice la gestión dinámica de canalizaciones para implementar soluciones de hotfix en entornos de Gitflow mediante el uso y AWS Service Catalog AWS CodePipeline

Balaji Vedagiri, Faisal Shahdad, Shanmugam Shanker y Vivek Thangamuthu, Amazon Web Services

Resumen

> **Note**
>
> AWS CodeCommit ya no está disponible para nuevos clientes. Los clientes actuales de AWS CodeCommit pueden seguir utilizando el servicio con normalidad. Más información

Este patrón aborda un escenario en el que se administra una canalización de revisiones dinámica que se dedica exclusivamente a implementar de forma segura soluciones de revisión en un entorno de producción. La solución se implementa y administra mediante una AWS Service Catalog cartera y un producto. Se utiliza una EventBridge regla de Amazon para la automatización de eventos. Las restricciones se imponen mediante el uso de las restricciones de la cartera de Service Catalog y los roles de AWS Identity and Access Management (IAM) para los desarrolladores. Solo una AWS Lambda función puede lanzar el producto Service Catalog, activada por la EventBridge regla. Este patrón está diseñado para entornos con una configuración específica de Gitflow, que se describe en Información adicional.

Por lo general, se implementa una revisión para abordar problemas críticos o de seguridad notificados en un entorno activo, como el de producción. Las revisiones se deben implementar directa y únicamente en los entornos de prueba y producción. Las canalizaciones de prueba y producción se utilizan ampliamente en las solicitudes de desarrollo habituales. Estas canalizaciones no se pueden usar para implementar revisiones, porque ya hay características de control de calidad activas que no se pueden pasar a la fase de producción. Para publicar revisiones, este patrón describe un proceso dinámico y de corta duración con las siguientes características de seguridad:

- Creación automática: cada vez que se crea una rama de revisiones en un repositorio, se crea automáticamente una AWS CodeCommit canalización de revisiones.
- Restricciones de acceso: los desarrolladores no tienen acceso para crear esta canalización fuera del proceso de revisión.

- Etapa controlada: la canalización tiene una etapa controlada con un token de acceso especial, lo que garantiza que una solicitud de extracción (PR) solo se pueda crear una vez.
- Etapas de aprobación: las etapas de aprobación se incluyen en la canalización para obtener las aprobaciones necesarias de las partes interesadas pertinentes.
- Eliminación automática: la canalización de revisiones se elimina automáticamente cada vez que se elimina una `hotfix` rama del CodeCommit repositorio después de fusionarla con un PR.

Requisitos previos y limitaciones

Requisitos previos

- Se Cuentas de AWS requieren tres activos, de la siguiente manera:
  - Cuenta de herramientas: para la configuración de integración y entrega continuas (CI/CD).
  - Cuenta de etapa: para realizar pruebas de aceptación por parte de los usuarios.
  - Cuenta de producción: para un usuario final de empresa.
  - (Opcional) Agregue una Cuenta de AWS para que actúe como una cuenta de control de calidad. Esta cuenta es necesaria si desea disponer tanto de una configuración de canalización principal, incluido el control de calidad, como de una solución de canalización con revisiones para realizar pruebas.
- Una AWS CloudFormation pila con la condición opcional de implementarla en la cuenta de control de calidad mediante la canalización principal, si es necesario. El patrón aún se puede probar sin la configuración de la canalización principal; para ello, solo debe crear y eliminar una rama de `hotfix`.
- Un depósito de Amazon Simple Storage Service (Amazon S3) para almacenar CloudFormation las plantillas que se utilizan para crear los productos del Service Catalog.
- Cree reglas de aprobación de relaciones públicas para el CodeCommit repositorio de acuerdo con los requisitos de conformidad (después de crear el repositorio).
- Restrinja los permisos de IAM de los desarrolladores y líderes de equipo para denegar la ejecución de la función de Lambda prcreation-lambda, ya que solo debe invocarse desde la canalización.

Limitaciones

- El CloudFormation proveedor se utiliza en la fase de despliegue y la aplicación se despliega mediante un conjunto de CloudFormation cambios. Si desea utilizar una opción de implementación diferente, modifique la CodePipeline pila según sea necesario.

- Este patrón utiliza AWS CodeBuild y otros archivos de configuración para implementar un microservicio de muestra. Si tiene un tipo de carga de trabajo diferente (por ejemplo, cargas de trabajo sin servidor), debe actualizar todas las configuraciones pertinentes.
- Este patrón despliega la aplicación en un solo extremo Región de AWS (por ejemplo, US-east-1 de EE. UU. Este (Virginia del Norte)). Cuentas de AWS Para realizar la implementación en varias regiones, cambie la referencia a la región en los comandos y las pilas.
- Algunas Servicios de AWS no están disponibles en todos. Regiones de AWS Para obtener información sobre la disponibilidad en regiones, consulte AWS services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

Los diagramas de esta sección proporcionan los flujos de trabajo para los eventos de creación y eliminación del ciclo de vida.

El diagrama anterior para crear un evento de ciclo de vida muestra lo siguiente:

1. El desarrollador crea una `hotfix-*` rama en el CodeCommit repositorio para desarrollar una solución relacionada con las revisiones.
2. El evento `hotfix-*` de creación de sucursales se captura mediante la EventBridge regla. Los detalles del evento incluyen los nombres del repositorio y de la sucursal.
3. La EventBridge regla invoca la AWS Lambda función. `hotfix-lambda-function` La EventBridge regla pasa la información del evento a la función Lambda como entrada.
4. La función de Lambda procesa la entrada para recuperar los nombres del repositorio y de la rama. Activa el producto de Service Catalog con los valores recuperados de la entrada procesada.
5. El producto de Service Catalog incluye una configuración de canalización que implementará la solución en los entornos de etapa y producción. El bloque de canalización incluye las etapas de origen, compilación e implementación. Además, hay una etapa de aprobación manual para favorecer la implementación en el entorno de producción.
6. La etapa de origen recupera el código del repositorio y la rama de `hotfix-*` que se crearon en el primer paso. El código se pasa a la fase de compilación a través de un bucket de Amazon S3 para artefactos. En la etapa de compilación, se crea una imagen de contenedor que incluye la revisión que se ha desarrollado en la rama de `hotfix-*` y se ha agregado a Amazon Elastic Container Registry (Amazon ECR).

7. La etapa de implementación en el entorno de la etapa actualiza Amazon Elastic Container Service (Amazon ECS) con la imagen del contenedor más reciente que incluye la revisión. El hotfix se implementa mediante la creación y ejecución de un conjunto de CloudFormation cambios.
8. La función de Lambda `prcreation-lambda` se invoca después de una implementación correcta en el entorno de etapa. Esta función de Lambda crea una PR desde la rama de `hotfix-*` hacia las ramas `develop` y `main` del repositorio. La función de Lambda garantiza que la solución desarrollada en la rama de `hotfix-*` se fusione e incluya en las implementaciones posteriores.
9. Una etapa de aprobación manual ayuda a garantizar que las partes interesadas necesarias revisen la solución y aprueben su implementación en la fase de producción.
10. La etapa de implementación en el entorno de producción actualiza Amazon ECS con la imagen del contenedor más reciente que incluye la revisión. El hotfix se implementa mediante la creación y ejecución de un conjunto de CloudFormation cambios.

El diagrama anterior para eliminar un evento de ciclo de vida muestra lo siguiente:

1. El desarrollador elimina la rama de `hotfix-*` después de implementar correctamente la revisión en el entorno de producción.
2. El evento de eliminación de una `hotfix-*` rama se captura mediante una EventBridge regla. Los detalles del evento incluyen los nombres del repositorio y de la sucursal.
3. La EventBridge regla invoca la función Lambda. La EventBridge regla pasa la información del evento a la función Lambda como entrada.
4. La función de Lambda procesa la entrada para recuperar los nombres del repositorio y de la rama. La función de Lambda determina el producto de Service Catalog correspondiente a partir de la entrada pasada y, a continuación, finaliza el producto.
5. La finalización del producto aprovisionado de Service Catalog elimina la canalización y los recursos relevantes que se crearon anteriormente en ese producto.

Automatización y escala

- El patrón incluye una EventBridge regla y una función Lambda, que puede gestionar varias solicitudes de creación de sucursales de hotfix en paralelo. La función de Lambda aprovisiona el producto de Service Catalog para la regla de eventos coincidentes.

- La configuración de la canalización se gestiona mediante el producto de Service Catalog, que proporciona funciones de control de versiones. La solución también se escala automáticamente para gestionar en paralelo múltiples desarrollos de revisiones de la misma aplicación.
- La función prcreation-lambda garantiza que estos cambios de revisión también se vuelvan a combinar en `main` y las ramas de `develop` mediante la creación automática de solicitudes de extracción. Este enfoque es esencial para mantener `main` y las ramas de `develop` actualizadas con todas las correcciones y evitar posibles regresiones de código. Este proceso permite mantener la coherencia entre las ramas y evita las regresiones de código, ya que garantiza que las ramas más antiguas tengan las correcciones más recientes.

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todo el territorio y. Cuentas de AWS Regiones de AWS
- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- AWS CodeCommit es un servicio de control de versiones que permite almacenar y administrar repositorios de Git de forma privada, sin necesidad de administrar su propio sistema de control de origen. AWS CodeCommit ya no está disponible para clientes nuevos. Los clientes actuales de AWS CodeCommit pueden seguir utilizando el servicio con normalidad. Para obtener más información, consulta Cómo migrar tu AWS CodeCommit repositorio a otro proveedor de Git.
- AWS CodePipeline permite diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software y automatizar los pasos necesarios para lanzar los cambios en el software de manera continua.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores escalable y rápido que ayuda a ejecutar, detener y administrar contenedores en un clúster.
- AWS Key Management Service (AWS KMS) te ayuda a crear y controlar claves criptográficas para proteger tus datos.

- AWS Service Catalogle ayuda a gestionar de forma centralizada los catálogos de servicios de TI aprobados. AWS Los usuarios finales pueden implementar rápidamente solo los servicios de TI aprobados que necesitan, de acuerdo con las limitaciones establecidas por su organización.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

- CloudFormation Linter (cfn-lint) es un linter que compara las plantillas CloudFormation YAML o JSON con la especificación del recurso. CloudFormation También realiza otras comprobaciones, como verificar los valores válidos de las propiedades de los recursos y el cumplimiento de las prácticas recomendadas.
- cfn-nag es una herramienta de código abierto que identifica posibles problemas de seguridad en las plantillas mediante la búsqueda de patrones. CloudFormation
- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización del sistema operativo para entregar software en contenedores. Este patrón utiliza Docker para crear y probar imágenes de contenedores de forma local.
- Git es un sistema de control de versiones distribuido y de código abierto.

Repositorio de código

El código de este patrón está disponible en el repositorio dynamic_hotfix_codepipeline GitHub .

Prácticas recomendadas

Revise y ajuste los roles de IAM y las políticas de control de servicios (SCP) de su entorno para asegurarse de que restringen el acceso de forma adecuada. Esto es crucial para evitar cualquier acción que pueda anular las medidas de seguridad incluidas en este patrón. Siga el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Configuración del entorno de trabajo

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Para clonar el repositorio de muestras en un nuevo directorio de su ubicación de trabajo, ejecute el siguiente comando: `git clone git@github.com:aws-samples/dynamic_hotfix_codepipeline.git`	AWS DevOps
Exporte variables de entorno para el despliegue de CloudFormation pilas.	Defina las siguientes variables de entorno que se utilizarán como entrada en las CloudFormation pilas más adelante en este patrón. • `ApplicationName` : esta variable se usa para nombrar los recursos creados para una aplicación, lo que facilita su seguimiento. Utilice el siguiente comando y sustituya `Applicationname` por el nombre real de la aplicación: `export ApplicationName=<Applicationname>`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	• `BucketStartName` : esta variable sirve para asignar un nombre a un bucket de Amazon S3. Los nombres de los buckets de S3 deben ser únicos a nivel mundial en todos Cuentas de AWS ellos. Utilice el siguiente comando y sustituya `BucketName` por un nombre único para su bucket de S3:
	
	`export BucketStartName=<BucketName>`
	
	• Números de cuenta y regiones: estas variables almacenan Cuenta de AWS los números de los diferentes entornos y de la región de implementación. Utilice los siguientes comandos y sustituya los marcadores de posición (como `prodaccountnumber yregion`) por sus Cuenta de AWS números reales y los Región de AWS que esté utilizando.
	
	Note
	`QAAccount` es opcional. Si quiere usar `QAAccount`	

Tarea	Descripción	Habilidades requeridas
	, configúrala con los parámetros de la pila principal de canalizaciones. `export ProdAccou nt=<prodaccountnum ber> export StageAcco unt=<stage/preprod accountnumber> export QAAccount =<qaccountnumber> export ToolsAcco unt=<toolsaccountn umber> export DepRegion =<region>`	

Configure los requisitos previos necesarios en Cuentas de AWS

Tarea	Descripción	Habilidades requeridas
Cree los recursos necesario s para CI/CD la cuenta de herramientas.	Para implementar la CloudFormation pila en la cuenta de herramientas, usa los siguientes comandos. (Elimine el parámetro `QAAccount` si no utiliza la cuenta de control de calidad en la configuración). `#InToolsAccount aws cloudformation deploy \`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`--template-file pre-requisites/pre-reqs.yaml \ --stack-name prereqs \ --parameter-overrides BucketStartName=${BucketStartName} \ ApplicationName=${ApplicationName} ProdAccount=${ProdAccount} \ StageAccount=${StageAccount} ToolsAccount=${ToolsAccount} \ QAAccount=${QAAccount} \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM --region ${DepRegion}`  Anote los recursos que el CodeCommit repositorio y Amazon ECR crearon a partir de la pila anterior. Estos parámetros son necesarios para configurar la rama de `main` de la canalización en los próximos pasos.	

Tarea	Descripción	Habilidades requeridas

Cree los recursos necesarios para CI/CD las cuentas de carga de trabajo.	1. Para empaquetar la CloudFormation plantilla en cada cuenta de carga de trabajo (fase, producción y control de calidad opcional), utilice los siguientes comandos. En el siguiente comando, sustituya `S3bucketpackage` por el nombre del bucket de Amazon S3 que desee usar en la compresión.
	
	`#InStageAccount`
	`aws cloudformation package \`
	`--template-file pre-requisites/infrastack.yaml \`
	`--s3-bucket <S3bucketpackage> \`
	`--s3-prefix infraStack \`
	`--region ${DepRegion} \`
	`--output-template-file pre-requisites/infrastructure_stage.template`
	
	`#InProdAccount`
	`aws cloudformation package \`
	`--template-file pre-requisites/infrastack.yaml \`
	`--s3-bucket <S3bucketpackage> \`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	<pre>--s3-prefix infraStack \
	--region ${DepRegion} \
	--output-template-file pre-requisites/infrastructure_prod.template</pre>
	2. Para implementar la CloudFormation plantilla en cada cuenta de carga de trabajo, utilice los siguientes comandos:
	<pre>#InStageAccount
	aws cloudformation deploy --stack-name inframainstack \
	--parameter-overrides Applicationname=${Applicationname} ToolsAccount=${ToolsAccount} DepRegion=${DepRegion} \
	--template-file pre-requisites/infrastructure_stage.template --region ${DepRegion} --capabilities CAPABILITY_NAMED_IAM
	
	#InProdAccount
	aws cloudformation deploy --stack-name inframainstack \</pre>	

Tarea	Descripción	Habilidades requeridas
	`--parameter-overrides ApplicationName=${ApplicationName} ToolsAccount=${ToolsAccount} DepRegion=${DepRegion} \` `--template-file pre-requisites/infrastructure_prod.template --region ${DepRegion} --capabilities CAPABILITY_NAMED_IAM`	

Tarea	Descripción	Habilidades requeridas

Actualice la política de bucket de artefactos de S3 para permitir el acceso a las cuentas de carga de trabajo.	Para actualizar los requisitos previos de la CloudFormation pila en la cuenta de herramientas, utilice los siguientes comandos para añadir todos los permisos necesarios para las cuentas de carga de trabajo de Stage y Production. (Elimine el parámetro `QAAccount` si no lo utiliza en la configuración).
	
	`#InToolsAccount`
	`aws cloudformation deploy \`
	`--template-file pre-requisites/pre-reqs.yaml \`
	`--stack-name prereqs \`
	`--parameter-overrides BucketStartName=${BucketStartName} \`
	`ApplicationName=${ApplicationName} ProdAccount=${ProdAccount} \`
	`StageAccount=${StageAccount} ToolsAccount=${ToolsAccount} \`
	`QAAccount=${QAAccount} PutPolicy=true \`
	`--capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM --region ${DepRegion}`
		AWS DevOps

Configuración de la función de Lambda y los recursos de Service Catalog en la cuenta de herramientas

Tarea	Descripción	Habilidades requeridas

Configure la cartera y los productos de Service Catalog.	Para configurar la cartera y los productos de Service Catalog, haga lo siguiente:
	
	1. Cargue las plantillas pipeline-main.yaml y pipeline-hotfix.yaml desde el repositorio del directorio a CodePipeline un bucket de Amazon S3 existente () en la región en la que desee implementar (`Bucketname`). `DepRegion`
	
	`#InToolsAccount`
	`aws s3 cp ./codepipeline/pipeline-main.yaml s3://<Bucketname>/pipeline-main.yaml`
	`aws s3 cp ./codepipeline/pipeline-hotfix.yaml s3://<Bucketname>/pipeline-hotfix.yaml`
	
	2. Configure la cartera y el producto de Service Catalog que administrarán la canalización de las ramas `main` y `hotfix`. Anote los detalles de la sección
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`Outputs` correspondiente a `MainProductId` y `MainProductArtifactId` de la siguiente pila. Tendrá que usar esa información en los pasos posteriores de la configuración de la canalización de la rama de `main`.
	
	`#InToolsAccount`
	`aws cloudformation deploy \`
	`--template-file pre-requisites/servicecatalogsetup.yaml \`
	`--stack-name servicecatalogsetup \`
	`--parameter-overrides TemplateBucket=<Bucketname> \`
	`--capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM --region ${DepRegion}`
	
	3. Proporcione acceso a un rol de IAM que implementará los recursos de la cuenta de herramientas en la cartera de canalización principal de la cartera de Service Catalog. Utilice esta cartera para implementar la aplicación mediante	

Tarea	Descripción	Habilidades requeridas
	la rama de `main`. Para más información sobre cómo proporcionar acceso, consulte la Concesión de acceso a los usuarios en la documentación de Service Catalog.	

Tarea	Descripción	Habilidades requeridas
Configure as funciones de Lambda.	Esta solución utiliza las siguientes funciones de Lambda para administrar los flujos de trabajo de revisiones: • `hotfix-lambda-function` gestiona el aprovisionamiento de productos de Service Catalog cuando se crea una rama de `hotfix`. • `hotfix-cleanup-lambda-function` administra la finalización del producto cuando se elimina una rama de `hotfix`. • `prcreation-lambda` crea solicitudes de extracción desde la rama de `hotfix` a las ramas `develop` y `main`. Para permitir que las funciones de Lambda aprovisionen y cancelen los productos de Service Catalog cuando se creen o eliminen `hotfix` sucursales mediante la EventBridge regla asociada, siga estos pasos: 1. Para crear las funciones y los permisos de IAM para las funciones de Lambda, utilice el siguiente	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	comando para implementar CloudFormation una pila: `#InToolsAccount aws cloudformation deploy \ --template-file pre-requisites/lambdasetup.yaml \ --stack-name prsclambdasetup \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM --region ${DepRegion}` 2. Tras la implementación de la pila, conceda el acceso `hotfix-lambda-execution-role` a la cartera de canalizaciones de revisión de la cartera de Service Catalog mediante la Consola de administración de AWS. Este acceso permite a la función de Lambda iniciar o finalizar el producto de Service Catalog en las ramas de revisión.	

Creación de una canalización para la rama principal e implementación de la aplicación en las cuentas de carga de trabajo

Tarea	Descripción	Habilidades requeridas

Configure la canalización para la rama de `main`.	Para configurar la canalización de la rama principal, ejecute el siguiente comando en la cuenta de herramientas. Sustituya los parámetros de `MainProductId` y `MainProductArtifactId` con los valores de los resultados de pila `servicecatalogsetup`.
	
	`#InToolsAccount`
	`aws servicecatalog provision-product \`
	`--product-id <MainProductId> \`
	`--provisioning-artifact-id <MainProductArtifactId> \`
	`--provisioned-product-name "${ApplicationName}-main-pipeline" \`
	`--provisioning-parameters Key=CodeCommitRepoName,Value="${ApplicationName}-repository" Key=ECRRepository,Value="${ApplicationName}-app" \`
	`--region=${DepRegion}`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
Implemente la aplicación mediante la rama de `main`.	1. Para clonar el CodeCommit repositorio que se creó en los requisitos previos, utilice el `git clone` comando. Para obtener más información, consulte Conectarse al CodeCommit repositorio mediante la clonación del repositorio tal y como se describe en la CodeCommit documentación. 2. Copie todos los archivos de la aplicación del directorio `repotemplates` disponible en el repositorio a su repositorio local clonado (`${ApplicationName}-repository`). Modifique los siguientes archivos para actualizar el ID `ToolsAccount` . En cada archivo, busque el parámetro `RegistryAccountid` y establezca su valor en su ID `ToolsAccount` . Confirma los cambios en el CodeCommit repositorio y envía los archivos a la rama `main` y a la `develop` rama. • ecs-configuration-prod.yaml • ecs-configuration-qa.yaml	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• ecs-configuration-stage.yaml 3. Para verificar el despliegue de la aplicación, supervise la CodePipeline ejecución mediante. Consola de administración de AWS Una vez completada la implementación, acceda a la aplicación mediante el FQDN del equilibrador de carga de aplicación en el entorno del escenario. Confirme que la aplicación funciona según lo previsto. 4. Para aprobar el despliegue en producción, utilice la CodePipeline consola para localizar la canalización de la aplicación. Busque la etapa `ApprovalToStart` . Revise los cambios y, si son satisfactorios, apruebe manualmente la implementación en el paso de producción.	

Creación de la canalización para una rama de hotfix-* e implementación de la revisión

Tarea	Descripción	Habilidades requeridas
Cree una rama de `hotfix-*` y confirme los cambios.	Para crear una canalización para la rama de `hotfix-*` e implementar la revisión en las	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	cuentas de carga de trabajo, haga lo siguiente: 1. Cree una rama con un nombre que comience por la palabra clave `hotfix`. Por ejemplo, este patrón usa la `hotfix-check1` rama del repositorio de CodeCommit aplicaciones (`${ApplicationName}-repository`). Para ver pasos más detallados, consulta Conectarse a un AWS CodeCommit repositorio y Comandos básicos de Git en la CodeCommit documentación. 2. Compruebe que el producto `Hotfix CICD Pipeline` de Service Catalog se aprovisione correctamente de forma dinámica en la rama de `hotfix-check1`. El nombre del producto aprovisionado recibe el nombre de esta rama de hotfix y del nombre del CodeCommit repositorio de la aplicación. 3. Realice algunos cambios menores en el archivo index.html y envíelos al CodeCommit repositorio.	

Tarea	Descripción	Habilidades requeridas
	4. Compruebe que la CodePipeline ejecución se ha realizado correctamente en el entorno del escenario . Para implementarlo en el entorno de producción, proporcione la aprobación manual en CodePipeline. 5. Compruebe que los cambios estén visibles en la página de inicio de la aplicación mediante el nombre de dominio (FQDN) del equilibrador de carga de aplicación. El FQDN está disponible en la sección `Outputs` de `inframain stack-ALBStack-*` .	
Elimine la rama de `hotfix-check1` .	Para eliminar la rama de `hotfix-check1` que creó anteriormente, haga lo siguiente: 1. Elimine la `hotfix-check1` rama que está en el repositorio de CodeCommit aplicaciones. 2. Compruebe que el producto de Service Catalog que se aprovisionó para la rama de `hotfix-check1` finalizó correctamente.	AWS DevOps

Eliminar recursos

Tarea	Descripción	Habilidades requeridas

Limpie todos los recursos implementados.	Para limpiar los recursos que se implementaron anteriorm ente, haga lo siguiente:
	1. Para reducir verticalmente el servicio Amazon ECS a cero réplicas en las cuentas de carga de trabajo, utilice el siguiente comando:
	`aws ecs update-service --cluster ${ApplicationName}-Cluster --service ${ApplicationName}-Service-stage --desired-count 0 --region ${DepRegion}`
	`aws ecs update-service --cluster ${ApplicationName}-Cluster --service ${ApplicationName}-Service-prod --desired-count 0 --region ${DepRegion}`
	2. Finalice el producto de Service Catalog que se aprovisionó para la rama de `main`.
	3. Limpie los objetos creados en los buckets de Amazon S3 de la cuenta de herramientas. Elimine todas las imágenes de Docker
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	en Amazon ECR antes de eliminar el propio registro.
	4. Elimine los roles de IAM en la sección de acceso concedido de las carteras de Service Catalog antes de eliminar la cartera de Service Catalog.
	5. Elimine las CloudFormation pilas desplegadas en la cuenta de herramientas y en las cuentas de carga de trabajo.
	
	`##In Tools Account##`
	`aws cloudformation delete-stack --stack-name servicecatalogsetup --region ${DepRegion}`
	`aws cloudformation delete-stack --stack-name prlambdasetup --region ${DepRegion}`
	`aws cloudformation delete-stack --stack-name prereqs --region ${DepRegion}`
	
	`##In Workload Accounts##`
	`aws cloudformation delete-stack --stack-name inframainstack --region ${DepRegion}`	

Tarea	Descripción	Habilidades requeridas
	Para más información, consulte Eliminación de productos aprovisionados en la documentación de Service Catalog.	

Resolución de problemas

Problema	Solución
Los cambios que ha realizado en el CodeCommit repositorio no se están implement ando.	Comprueba los CodeBuild registros para ver si hay errores en la acción de compilación de Docker. Para obtener más información, consulte la Documentación de CodeBuild .
El producto de Service Catalog no se está aprovisionando.	Revisa las CloudFormation pilas relacionadas para ver si hay eventos fallidos. Para obtener más información, consulte la Documentación de CloudFormation .

Recursos relacionados

- Comandos básicos de Git
- Configure una política de IAM para limitar las transferencias y fusiones a una sucursal
- Conectarse a un AWS CodeCommit repositorio
- Concesión de acceso a los usuarios
- Enviar una imagen de Docker a un repositorio privado de Amazon ECR
- Solución de problemas AWS CodeBuild
- ¿Qué es? AWS CodePipeline

Información adicional

Este patrón está diseñado para entornos con una configuración de Gitflow que se adopta en el CI/CD proceso para el flujo de trabajo de desarrollo. Las canalizaciones siguen el ciclo de implementación, que comienza con el desarrollo y pasa por los entornos de control de calidad (QA), etapas y producción. La CI/CD configuración incluye dos ramas de git con despliegues promocionales en los siguientes entornos:

- La rama de `develop` se implementa en el entorno de desarrollo.
- La rama de `main` realiza implementaciones en los entornos de control de calidad, de etapas y de producción.

En esta configuración, es todo un desafío aplicar una revisión o un parche de seguridad más rápido que el ciclo de implementación habitual mientras se continúa con el desarrollo activo de nuevas características. Es necesario establecer un proceso dedicado para abordar las solicitudes de revisión o seguridad, a fin de garantizar que los entornos activos sigan funcionando correctamente y sean seguros.

Sin embargo, puede utilizar otras opciones disponibles sin necesidad de un usar proceso de implementación específico si:

- El CI/CD proceso está bien equipado con pruebas automatizadas, como las funcionales y end-to-end las pruebas, que eliminan la necesidad de realizar pruebas manuales y evitan demoras en las implementaciones en la producción. Sin embargo, si las pruebas automatizadas no están bien integradas en el CI/CD proceso, introducir una pequeña modificación en el entorno de producción puede resultar complejo y engorroso para los desarrolladores. Esto se debe a que es posible que haya nuevas características pendientes de aprobación y cierre en el entorno de control de calidad. No se puede poner en fase de producción una revisión o una corrección de seguridad de forma sencilla y simultánea.
- Los equipos de desarrollo implementan continuamente nuevas características en el entorno de producción e integran revisiones o parches de seguridad en la implementación programada de cada nueva característica. En otras palabras, la próxima actualización de características del entorno de producción consta de dos componentes: la incorporación de una nueva característica y la inclusión de la revisión o el parche de seguridad. Sin embargo, si el ciclo de implementación no es continuo, es posible que ya haya varias características nuevas pendientes de aprobación en el entorno de control de calidad. Administrar diferentes versiones y garantizar que se vuelvan a aplicar los cambios correctos puede convertirse en algo complejo y propenso a errores.

> **Note**
>
> Si utilizas la versión 2 de AWS CodePipeline con los activadores adecuados configurados en la `hotfix` sucursal, necesitarás un proceso específico para atender las solicitudes no programadas. En la versión 2, puede configurar desencadenadores para las solicitudes entrada o salida. La ejecución se pondrá en cola o se ejecutará inmediatamente, en función del estado anterior de la canalización. Sin embargo, con una canalización específica, las correcciones se aplican inmediatamente al entorno de producción, lo que garantiza que los problemas urgentes se resuelvan sin demora.

Automatice la eliminación de AWS CloudFormation pilas y recursos asociados

SANDEEP SINGH y James Jacob, Amazon Web Services

Resumen

AWS CloudFormation es un servicio muy utilizado para gestionar la infraestructura como código (IaC) en la nube. Cuando los usa CloudFormation, administra los recursos relacionados como una sola unidad denominada pila. Puede crear, actualizar y eliminar una colección de recursos mediante la creación, actualización y eliminación de pilas.

A veces, ya no necesitas los recursos de una CloudFormation pila. Según los recursos y sus configuraciones, puede resultar complicado eliminar una pila y sus recursos asociados. En los sistemas de producción reales, las eliminaciones a veces fallan o tardan mucho tiempo debido a condiciones conflictivas o restricciones que CloudFormation no se pueden anular. Es posible que necesite realizar una planificación y ejecución cuidadosas para garantizar que todos los recursos se eliminen correctamente de manera eficiente y coherente. Este patrón describe cómo configurar un marco que le ayude a gestionar la eliminación de CloudFormation pilas que presentan las siguientes complejidades:

- Recursos con protección contra eliminaciones: es posible que algunos recursos tengan habilitada la protección contra eliminaciones. Algunos ejemplos comunes son las tablas de Amazon DynamoDB y los buckets de Amazon Simple Storage Service (Amazon S3). La protección contra la eliminación impide la eliminación automática, como la eliminación automática. CloudFormation Si desea eliminar estos recursos, debe anular o deshabilitar temporalmente la protección contra eliminaciones de forma manual o programática. Debe evaluar detenidamente las implicaciones de eliminar estos recursos antes de continuar.
- Recursos con políticas de retención: algunos recursos, como las claves AWS Key Management Service (AWS KMS) y los buckets de Amazon S3, pueden tener políticas de retención que especifiquen cuánto tiempo deben conservarse después de solicitar su eliminación. Debes tener en cuenta estas políticas en la estrategia de limpieza para garantizar el cumplimiento de las políticas de la organización y los requisitos normativos.
- Eliminación retrasada de las funciones de Lambda asociadas a una VPC: la eliminación de una función de AWS Lambda adjunta a una nube privada virtual (VPC) puede tardar entre 5 y 40 minutos, en función de las múltiples dependencias interconectadas que intervienen en el

proceso. Si desconecta la función de la VPC antes de eliminar la pila, puede reducir este retraso a menos de 1 minuto.

- Recursos no creados directamente por CloudFormation: en algunos diseños de aplicaciones, los recursos pueden crearse fuera de la CloudFormation pila original, ya sea por la propia aplicación o por recursos aprovisionados a través de la pila. A continuación se muestran dos ejemplos:
  - CloudFormation podría aprovisionar una instancia de Amazon Elastic Compute Cloud (Amazon EC2) que ejecute un script de datos de usuario. A continuación, este script podría crear un parámetro de AWS Systems Manager para almacenar los datos relacionados con la aplicación. Este parámetro no se administra de forma completa CloudFormation.
  - CloudFormation podría aprovisionar una función Lambda que genere automáticamente un grupo de Amazon CloudWatch Logs para almacenar registros. Este grupo de registros no se administra mediante CloudFormation.

  Aunque estos recursos no los administra directamente CloudFormation, a menudo es necesario limpiarlos cuando se elimina la pila. Si no se administran, pueden quedar huérfanos y provocar un consumo innecesario de recursos.

Si bien estas barreras de protección pueden ser complejas, recuerde que son intencionales e imprescindibles. CloudFormation Permitir anular todas las restricciones y eliminar los recursos de forma indiscriminada podría tener consecuencias perjudiciales e imprevistas en muchos escenarios. Sin embargo, como ingeniero de nube responsable de administrar el entorno, hay ocasiones en las que puede ser necesario anular estas restricciones, especialmente en los entornos de desarrollo, pruebas DevOps o puesta en escena.

Resultados empresariales específicos

La implementación de este marco de trabajo proporciona los siguientes beneficios:

- Gestión de costes: la limpieza regular y eficiente de los entornos temporales, como end-to-end los entornos de pruebas de aceptación por parte de los usuarios, ayuda a evitar que los recursos se agoten durante más tiempo del necesario. Esto puede reducir considerablemente los costos.
- Seguridad: la limpieza automática de los recursos obsoletos o no utilizados reduce la superficie de ataque y ayuda a mantener un entorno seguro. AWS
- Eficiencia operativa: la limpieza periódica y automatizada puede proporcionar los siguientes beneficios operativos:
  - Los scripts automatizados que eliminan grupos de registros antiguos o depósitos vacíos de Amazon S3 pueden mejorar la eficiencia operativa al mantener el entorno limpio y manejable.

- Eliminar y volver a crear pilas con rapidez permite una iteración rápida para el diseño y la implementación, lo que puede conducir a una arquitectura más sólida y resiliente.
- Eliminar y reconstruir entornos con regularidad puede ayudarle a identificar y solucionar posibles problemas. Gracias a esto, puede garantizar que la infraestructura pueda soportar situaciones del mundo real.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- La versión 3.6 o posterior de Python instalada
- AWS Command Line Interface (AWS CLI), instalado y configurado

Limitaciones

- Se utiliza una convención de nomenclatura para identificar los recursos que se deben eliminar. El código de ejemplo de este patrón usa un prefijo para el nombre del recurso, pero puede definir su propia convención de nomenclatura. Los recursos que no utilicen esta convención de nomenclatura no se identificarán ni se eliminarán posteriormente.

Arquitectura

El siguiente diagrama muestra cómo este marco identifica la CloudFormation pila de destino y los recursos adicionales asociados a ella.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Reúna recursos: el marco de automatización utiliza una convención de nomenclatura para devolver todas las CloudFormation pilas relevantes, los repositorios de Amazon Elastic Container Registry (Amazon ECR), las tablas de DynamoDB y los buckets de Amazon S3.

> **Note**
>
> Las funciones de esta etapa utilizan paginadores, una característica de Boto3 que resume el proceso de iteración sobre un conjunto de resultados de API truncado. Esto garantiza

que se procesen todos los recursos. Para optimizar aún más el rendimiento, considere la posibilidad de aplicar un filtrado del lado del servidor o de utilizarlo para realizar un filtrado del lado del cliente. JMESPath

2. Procesamiento previo: el marco de automatización identifica y aborda las restricciones del servicio que deben anularse para poder eliminar los recursos. CloudFormation Por ejemplo, cambia la configuración `DeletionProtectionEnabled` de las tablas de DynamoDB a `False`. En la interfaz de línea de comandos de cada recurso, recibirá una petición en la que se le preguntará si desea anular la restricción.
3. Eliminar pila: el marco de automatización elimina la pila. CloudFormation En la interfaz de línea de comandos, recibirá una petición en la que se le preguntará si desea anular la pila.
4. Posprocesamiento: el marco de automatización elimina todos los recursos relacionados que no se hayan aprovisionado directamente CloudFormation como parte de la pila. Algunos ejemplos de estos tipos de recursos son los parámetros y los grupos de CloudWatch registros de Systems Manager. Las funciones independientes recopilan estos recursos, los procesan previamente y, a continuación, los eliminan. En la interfaz de línea de comandos de cada recurso, recibirá una petición en la que se le preguntará si desea eliminar el recurso.

> **Note**
>
> Las funciones de esta etapa utilizan paginadores, una característica de Boto3 que resume el proceso de iteración sobre un conjunto de resultados de API truncado. Esto garantiza que se procesen todos los recursos. Para optimizar aún más el rendimiento, considere la posibilidad de aplicar un filtrado del lado del servidor o de utilizarlo JMESPath para realizar un filtrado del lado del cliente.

Automatización y escala

Si tu CloudFormation pila incluye otros recursos que no están incluidos en el código de ejemplo o si la pila tiene una restricción que no se ha abordado en este patrón, puedes adaptar el marco de automatización a tu caso de uso. Siga la misma metodología de recopilación de recursos, procesamiento previo, eliminación de la pila y procesamiento posterior.

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida a lo largo de todo Cuentas de AWS el ciclo de vida. Regiones de AWS
- CloudFormation La interfaz de línea de comandos (CFN-CLI) es una herramienta de código abierto que le ayuda a desarrollar AWS y probar extensiones de terceros y luego registrarlas para su uso. CloudFormation
- AWS SDK para Python (Boto3)es un kit de desarrollo de software que le ayuda a integrar su aplicación, biblioteca o script de Python con Servicios de AWS.

Otras herramientas

- Click es una herramienta de Python que lo ayuda a crear interfaces de línea de comandos.
- Poetry es una herramienta de empaquetado y administración de dependencias de Python.
- Pyenv es una herramienta que lo ayuda a administrar y cambiar entre versiones de Python.
- Python es un lenguaje de programación informático de uso general.

Repositorio de código

El código de este patrón está disponible en el GitHub cloudformation-stack-cleanuprepositorio.

Prácticas recomendadas

- Etiquetado de recursos para una fácil identificación: implemente una estrategia de etiquetado para identificar los recursos que se crean para diferentes entornos y propósitos. Las etiquetas pueden simplificar el proceso de limpieza al ayudarte a filtrar los recursos en función de sus etiquetas.
- Configuración de los ciclos de vida de los recursos: defina los ciclos de vida de los recursos para eliminarlos automáticamente después de un período determinado. Esta práctica lo ayuda a garantizar que los entornos temporales no se conviertan en pasivos de costos permanentes.

Epics

Instalar herramientas

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	1. Cree una carpeta en su entorno virtual. Póngale el nombre del proyecto. 2. Abra un terminal en la máquina local y vaya a la carpeta. 3. Introduzca el siguiente comando para clonar el cloudformation-stack-cleanup repositorio en el directorio de su proyecto: `git clone https://github.com/aws-samples/cloudformation-stack-cleanup.git`	DevOps ingeniero
Instale Poetry.	Siga las instrucciones (documentación de Poetry) para instalar Poetry en el entorno virtual de destino.	DevOps ingeniero
Instale las dependencias.	1. Introduzca el siguiente comando para navegar al directorio del proyecto: `cd cloudformation-stack-cleanup` 2. Introduzca el siguiente comando:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`poetry install` Esto instala todas las dependencias necesarias, como Boto3, click y el código fuente de la CLI. CloudFormation	
(Opcional) Instale Pyenv.	Siga las instrucciones (GitHub) para instalar Pyenv.	DevOps ingeniero

(Opcional) Personalice el marco.

Tarea	Descripción	Habilidades requeridas
Cree funciones que recopilen, procesen previamente y eliminen los recursos de destino.	1. En el repositorio clonado, introduzca el siguiente comando para acceder al directorio de la `cli`. `cd cfncli/cli` 2. Abra el archivo cleanup_environment.py. 3. Cree una nueva función de Python que recopile el tipo de recurso que desee modificar. Para ver un ejemplo, consulte la función de `gather_ddb_tables` en este archivo. 4. Cree una nueva función de Python que anule las restricciones de servicio del	DevOps ingeniero, Python

Tarea	Descripción	Habilidades requeridas
	recurso de destino. Para ver un ejemplo, consulte la función de `remove_ddb_deletion_protection` en este archivo. 5. Cree una nueva función de Python que recopile los recursos de destino no administrados. Para ver un ejemplo, consulte la función de `gather_log_groups` en este archivo. 6. Cree una nueva función de Python que elimine los recursos de destino no administrados. Para ver un ejemplo, consulte la función de `delete_log_group` en este archivo. 7. Guarde y cierre el archivo cleanup_enviornment.py.	

Creación de recursos de muestra

Tarea	Descripción	Habilidades requeridas
Crea una CloudFormation pila.	1. Desplácese hasta el directorio del proyecto . 2. Introduzca el siguiente comando para crear una CloudFormation pila que aprovisione una tabla de DynamoDB y un grupo de	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	seguridad. Anote el valor de <VPCID>. `aws cloudformation create-stack \ --stack-name sampleforcleanup-Stack \ --template-body file://samples/sample-cfn-stack.yaml \ --parameters ParameterKey=VpcId,ParameterValue=<VPCID> \ --region us-east-1`	
Cree un parámetro de Systems Manager.	Introduzca el siguiente comando para crear un parámetro de Systems Manager que no se aprovisione mediante CloudFormation: `aws ssm put-parameter \ --name "/samplefor cleanup/database/password" \ --value "your_db_password" \ --type "SecureString" \ --description "Database password for my app" \ --tier "Standard" \ --region "us-east-1"`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Crear un bucket de Amazon S3.	Introduce el siguiente comando para crear un bucket de Amazon S3 que no esté aprovisionado: CloudFormation `aws s3api create-bucket \ --bucket samplesorcleanup-unmanagedbucket-<UniqueIdentifier> \ --region us-east-1 \ --create-bucket-configuration LocationConstraint=us-east-1`	AWS DevOps

Eliminacion de los recursos de muestra

Tarea	Descripción	Habilidades requeridas
Elimine la CloudFormation pila.	1. Introduzca el siguiente comando para eliminar la CloudFormation pila de muestras, el parámetro de Systems Manager y el bucket de Amazon S3 que creó: `cfncli --region us-east-1 \ dev cleanup-env \ --prefix-list sampleforcleanup`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	2. Escriba Y para continuar cuando se le solicite.	
Valide la eliminación de recursos.	En el resultado, confirme que se hayan eliminado todos los recursos de muestra. Para ver un resultado de ejemplo, consulte la sección Información adicional de este patrón.	AWS DevOps

Recursos relacionados

- Eliminar una pila (CloudFormation documentación)
- Solución de problemas CloudFormation (CloudFormation documentación)
- Concesión a las funciones de Lambda de acceso a los recursos de una VPC de Amazon (documentación de Lambda)
- ¿Cómo elimino una AWS CloudFormation pila que está atascada en el estado DELETE_FAILED? (Centro de conocimiento)AWS

Información adicional

A continuación, se muestra un resultado de ejemplo del comando `cfncli`:

```
cfncli --region aus-east-1  dev cleanup-env --prefix-list sampleforcleanup


https://sts.us-east-1.amazonaws.com
Cleaning up: ['sampleforcleanup'] in xxxxxxxxxx:us-east-1
Do you want to proceed? [Y/n]: Y
No S3 buckets
No ECR repositories
No Lambda functions in VPC
The following DynamoDB tables will have their deletion protection removed:
sampleforcleanup-MyDynamoDBTable
Do you want to proceed with removing deletion protection from these tables? [Y/n]: Y
Deletion protection disabled for DynamoDB table 'sampleforcleanup-MyDynamoDBTable'.
```

```
The following CloudFormation stacks will be deleted:
sampleforcleanup-Stack
Do you want to proceed with deleting these CloudFormation stacks? [Y/n]: Y
Initiated deletion of CloudFormation stack: `sampleforcleanup-Stack`
Waiting for stack `sampleforcleanup-Stack` to be deleted...
CloudFormation stack `sampleforcleanup-Stack` deleted successfully.
The following ssm_params will be deleted:
/sampleforcleanup/database/password
Do you want to proceed with deleting these ssm_params? [Y/n]: Y
Deleted SSM Parameter: /sampleforcleanup/database/password
Cleaned up: ['sampleforcleanup']
```

Automatización de la ingesta y visualización de métricas personalizadas de Amazon MWAA en Amazon Managed Grafana mediante Terraform

Faisal Abdullah y Satya Vajrapu, Amazon Web Services

Resumen

En este patrón se explica cómo usar Amazon Managed Grafana para crear y supervisar métricas personalizadas que Amazon Managed Workflows para Apache Airflow (Amazon MWAA) incorpora. Amazon MWAA actúa como orquestador de los flujos de trabajo y emplea gráficos acíclicos dirigidos (DAGs) que se escriben en Python. Este patrón se centra en la supervisión de métricas personalizadas, como el número total de ejecuciones en la última hora, el recuento de aprobaciones y errores en DAGs cada hora y la DAGs duración media de estos procesos. Este análisis muestra cómo Amazon Managed Grafana se integra con Amazon MWAA para permitir una supervisión exhaustiva y obtener información sobre la orquestación de los flujos de trabajo en este entorno.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS con los permisos de usuario necesarios para crear y gestionar lo siguiente Servicios de AWS:
  - AWS Identity and Access Management Funciones y políticas (IAM)
  - AWS Lambda
  - Amazon Managed Grafana
  - Flujos de trabajo administrados de Amazon para Apache Airflow (Amazon MWAA)
  - Amazon Simple Storage Service (Amazon S3)
  - Amazon Timestream
- Acceso a un entorno del intérprete de comandos que puede ser un terminal en su máquina local o AWS CloudShell.
- Un entorno de shell con Git instalado y la última versión de AWS Command Line Interface (AWS CLI) instalada y configurada. Para obtener más información, consulta Instalar o actualizar a la última versión de AWS CLI en la AWS CLI documentación.
- La siguiente versión de Terraform instalada: `required_version = ">= 1.6.1, < 2.0.0"`. Puede usar tfswitch para cambiar entre diferentes versiones de Terraform.

- La fuente de identidad configurada es AWS IAM Identity Center para su Cuenta de AWS. Para más información, consulte Confirmación de los orígenes de identidad en IAM Identity Center en la documentación de IAM Identity Center. Puede elegir entre el Active Directory predeterminado Directorio de IAM Identity Center o un proveedor de identidad (IdP) externo, como Okta. Para más información, consulte Recursos relacionados.

Limitaciones

- Algunos Servicios de AWS no están disponibles en todos. Regiones de AWS Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- Terraform `required_version = ">= 1.6.1, < 2.0.0"`
- Amazon Managed Grafana, versión 9.4 o posterior. Este patrón se probó en la versión 9.4.

Arquitectura

El siguiente diagrama de arquitectura destaca lo que se Servicios de AWS utiliza en la solución.

En el anterior diagrama se muestra el flujo de trabajo siguiente:

1. Las métricas personalizadas de Amazon MWAA se originan en las DAGs que se ejecutan en el entorno. Las métricas se cargan en el bucket de Amazon S3 en un formato de archivo CSV. A continuación, se DAGs utilizan las funciones de consulta de bases de datos de Amazon MWAA:
   - `run-example-dag`: este DAG contiene un ejemplo de código de Python que define una o más tareas. Se ejecuta cada 7 minutos e imprime la fecha. Tras imprimir la fecha, el DAG incluye una tarea para suspender o pausar la ejecución durante un período específico.
   - `other-sample-dag`: este DAG se ejecuta cada 10 minutos e imprime la fecha. Tras imprimir la fecha, el DAG incluye una tarea para suspender o pausar la ejecución durante un período específico.

- `data-extract`: este DAG se ejecuta cada hora y consulta la base de datos de Amazon MWAA y recopila métricas. Una vez recopiladas las métricas, este DAG las escribe en un bucket de Amazon S3 para poder realizar un procesamiento y análisis posterior.

2. Para agilizar el procesamiento de datos, las funciones de Lambda se ejecutan cuando las activan eventos de Amazon S3, lo que facilita la carga de métricas en Timestream.
3. Timestream se integra como origen de datos en Amazon Managed Grafana, donde se almacenan todas las métricas personalizadas de Amazon MWAA.
4. Los usuarios pueden consultar los datos y crear paneles personalizados para visualizar los indicadores clave de rendimiento y obtener información sobre la orquestación de los flujos de trabajo de Amazon MWAA.

Tools (Herramientas)

Servicios de AWS

- AWS IAM Identity Centerle ayuda a gestionar de forma centralizada el acceso mediante el inicio de sesión único (SSO) a todas sus aplicaciones y a las de la nube. Cuentas de AWS
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice. En este patrón, AWS Lambda ejecuta el código de Python en respuesta a los eventos de Amazon S3 y administra los recursos informáticos automáticamente.
- Amazon Managed Grafana es un servicio de visualización de datos seguro y completamente administrado que puede utilizar para consultar, correlacionar, visualizar y recibir al instante alertas sobre métricas operativas, registros y seguimientos de varios orígenes. Este patrón utiliza Amazon Managed Grafana para crear un panel que le permita ver las métricas y alertas.
- Amazon Managed Workflows para Apache Airflow (Amazon MWAA) es un servicio de orquestación administrada de Apache Airflow que puede usar para configurar y usar canalizaciones de datos en la nube a escala. Apache Airflow es una herramienta de código abierto que se utiliza para crear, programar y supervisar secuencias de procesos y tareas denominadas flujos de trabajo mediante programación. En este patrón, se implementan una muestra DAGs y un extractor de métricas DAG en Amazon MWAA.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

En este patrón, Amazon S3 se utiliza para almacenar DAGs scripts y métricas personalizadas en formato CSV.

- Amazon Timestream LiveAnalytics for is es una base de datos de series temporales rápida, escalable, totalmente administrada y diseñada específicamente que facilita el almacenamiento y el análisis de billones de puntos de datos de series temporales por día. Timestream for LiveAnalytics también se integra con los servicios más utilizados para la recopilación de datos, la visualización y el aprendizaje automático. En este patrón, se utiliza para ingerir las métricas personalizadas de Amazon MWAA que se hayan generado.

Otras herramientas

- HashiCorp Terraform es una herramienta de infraestructura como código (IaC) que facilita usar el código para aprovisionar y administrar los recursos y la infraestructura en la nube. Este patrón utiliza un módulo de Terraform para automatizar el aprovisionamiento de la infraestructura en AWS.

Repositorio de código

El código de este patrón está disponible GitHub en el repositorio visualize-amazon-mwaa-custom-metrics-grafana. La carpeta `stacks/Infra` contiene los siguientes elementos:

- Archivos de configuración de Terraform para todos los recursos AWS
- Archivo .json del panel de control de Grafana en la carpeta `grafana`
- Amazon Managed Workflows para Apache Airflow DAGs en la carpeta `mwaa/dags`
- Código de Lambda para analizar el archivo.csv y almacenar las métricas en la base de datos de Timestream de la carpeta `src`
- Los archivos .json de la política de IAM están en la carpeta `templates`

Prácticas recomendadas

Terraform debe almacenar el estado de su infraestructura y configuración administradas para poder asignar recursos del mundo real a su configuración. De forma predeterminada, Terraform almacena el estado de forma local en un archivo denominado `terraform.tfstate`. Es imprescindible garantizar la seguridad e integridad de su archivo de estado de Terraform, ya que mantiene el estado actual de su infraestructura. Para más información, consulte Estado remoto en la documentación de Terraform.

Epics

Implementación de la infraestructura mediante Terraform

Tarea	Descripción	Habilidades requeridas

Implemente la infraestructura.	Para implementar la infraestructura de la solución, haga lo siguiente:
	1. Abra un terminal o una línea de comandos en su ordenador local o mediante AWS CloudShell.
	2. Desplácese hasta el directorio en el que desee clonar el repositorio.
	3. Para clonar el repositorio, ejecute el siguiente comando:
	`git clone https://github.com/aws-samples/visualize-amazon-mwaa-custom-metrics-grafana`
	4. Una vez finalizado el proceso de clonación, ejecute el siguiente comando para ir al directorio del repositorio clonado:
	`cd visualize-amazon-mwaa-custom-metrics-grafana/stacks/infra`
	5. Ejecute el siguiente comando para descargar e
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	inicializar los proveedores necesarios:
	
	`terraform init`
	
	6. Para obtener una visión completa de todos los recursos que Terraform creará, ejecute el siguiente comando:
	
	`terraform plan`
	
	Terraform aprovisiona los siguientes recursos:
	• Amazon Virtual Private Cloud (Amazon VPC) y componentes de red asociados
	• Recursos de Amazon S3
	• AWS Lambda funciones
	• Recursos de Amazon Managed Grafana (espacio de trabajo, paneles, origen de datos)
	• Recursos de IAM de soporte (roles y políticas)
	7. Para crear los AWS recursos a partir del resultado del plan, ejecute el siguiente comando:
	
	`terraform apply -auto-approve`	

Tarea	Descripción	Habilidades requeridas
	El aprovisionamiento de la infraestructura debería completarse en 20 minutos, aproximadamente. 8. Para crear los AWS recursos especificados de acuerdo con la configura ción definida en sus archivos de Terraform , ejecute el siguiente comando: `terraform apply`	

Validación de los recursos de infraestructura implementados

Tarea	Descripción	Habilidades requeridas
Valide el entorno de Amazon MWAA	Para validar el entorno de Amazon MWAA, haga lo siguiente: 1. Inicie sesión en Consola de administración de AWS, vaya a la consola del panel de control de Amazon MWAA y seleccione Open Airflow UI. 2. Deberás ver los tres siguientes DAGs en estado activo: • data-extract • run-example-dag	AWS DevOps, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	• other-sample-dag 3. Si un DAG no está activo, puede activarlo mediante el conmutador situado junto al nombre del DAG.	
Compruebe los programas de DAG.	Para ver cada programa del DAG, vaya a la pestaña Programación de la interfaz de usuario de Airflow. Cada una de las siguiente s DAGs opciones tiene una programación preconfigurada, que se ejecuta en el entorno Amazon MWAA y genera métricas personalizadas: • run-example-dag- Se ejecuta cada 7 minutos • other-sample-dag- Se ejecuta cada 10 minutos • data-extract: se ejecuta cada hora También puede ver las ejecuciones correctas de cada DAG en la columna Ejecucion es.	Ingeniero de datos, AWS DevOps

Configuración del entorno de Amazon Managed Grafana

Tarea	Descripción	Habilidades requeridas
Configure el acceso al espacio de trabajo de Amazon Managed Grafana.	Los scripts de Terraform crearon el espacio de trabajo, los paneles y la página de métricas de Amazon Managed Grafana necesarios. Para configurar el acceso de forma que pueda verlos, haga lo siguiente: 1. Abra la consola de Amazon Managed Grafana. 2. En Espacios de trabajo, seleccione el espacio de trabajo `grafana-ws-dev` y vaya a la pestaña Autenticación en el panel inferior. 3. Seleccione el botón Asignar nuevo usuario o grupo. 4. Añada su grupo en la pestaña Grupos o un usuario en la pestaña Usuarios y, a continuación, pulse el botón Asignar usuarios y grupos. 5. Una vez agregado el usuario (o grupo), conviértalo en administrador. Seleccione el usuario en Usuarios o grupos asignados en la pestaña Grupo de usuarios	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	asignados y elija Convertir en administrador en el menú desplegable. Para obtener más información, consulta Uso AWS IAM Identity Center con tu espacio de trabajo de Grafana gestionado por Amazon en la documentación de Amazon Managed Grafana. 6. Vaya a Espacios de trabajo y, a continuación, elija la URL del espacio de trabajo de Grafana. Para iniciar sesión en Amazon Managed Grafana como administrador, seleccione Iniciar sesión con. AWS IAM Identity Center	

Tarea	Descripción	Habilidades requeridas
Instalación del complemento de Amazon Timestream.	Las métricas personalizadas de Amazon MWAA se cargan en la base de datos de Timestream. Use el complemento de Timestream para visualizar las métricas con los paneles de Amazon Managed Grafana. Para instalar el complemento de Timestream, siga este procedimiento: 1. En la consola de Amazon Managed Grafana, amplíe el menú del panel de navegación izquierdo y vaya a Administración, Complementos. 2. Busque e instale la última versión del complemento de Amazon Timestream. 3. Una vez instalado el complemento, vaya a Administración y Orígenes de datos para ver el origen de datos de Timestream. Si el origen de datos no aparece en la lista, actualice la página. Para más información, consulte Ampliación del espacio de trabajo con	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	complementos en la documentación de Amazon Managed Grafana.	

Visualización de las métricas personalizadas en el panel de Amazon Managed Grafana

Tarea	Descripción	Habilidades requeridas
Consulte el panel de Amazon Managed Grafana.	Para ver las métricas que se incorporaron al espacio de trabajo de Amazon Managed Grafana, haga lo siguiente: 1. En la consola de Amazon Managed Grafana, seleccione Paneles en el panel de navegación izquierdo. 2. Para ver las métricas, elija los paneles de eventos de MWAA y, a continuación, seleccione mwaa_metrics. Las métricas del panel muestran la siguiente información: • El total de ejecuciones de DAG en la última hora • Número total de ejecucion es de DAG correctas, con errores y en ejecución en la última hora	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• Duración media de todas las ejecuciones de DAG correctas y con errores	
Personalice el panel de Amazon Managed Grafana.	Para personalizar los paneles para futuras mejoras, siga este procedimiento: 1. En la página `mwaa_metrics` del panel de Amazon Managed Grafana, seleccione el icono Configuración del panel. 2. Para ver la estructura de datos que define el panel, elija el modelo JSON. Puede personalizar el panel mediante modificaciones que podrá hacer en este modelo de JSON directamente en la consola. Como alternativa, el código fuente de este panel está disponible en el `dashboard.json` archivo de la `stacks/infra/grafana` carpeta del GitHub repositorio.	AWS DevOps

Limpie AWS los recursos

Tarea	Descripción	Habilidades requeridas
Pause las ejecuciones de DAG en Amazon MWAA.	Para pausar las ejecuciones de DAG, siga este procedimiento: 1. En la consola de Amazon MWAA, vaya a los entornos de Airflow y elija Abrir interfaz de usuario de Airflow. 2. Para pausar los DAG, utilice el conmutador situado junto a cada DAG. 3. Actualice la página de la interfaz de usuario de Airflow, que debería incluir tres DAGs en la sección En pausa.	AWS DevOps, ingeniero de datos
Elimine todos los objetos de los buckets de Amazon S3.	Para eliminar los buckets de Amazon S3 mwaa-events-bucket-* y mwaa-metrics-bucket-*, siga las instrucciones de uso de la consola de Amazon S3 que se encuentran en Eliminar un bucket en la documentación de Amazon S3.	AWS DevOps
Elimine los recursos creados por Terraform.	Para eliminar los recursos creados por Terraform y el archivo de estado local de Terraform asociado, haga lo siguiente:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	1. (Opcional) Antes de eliminar los recursos, puede previsualizar los cambios que realizará Terraform. Para generar un plan, ejecute el siguiente comando: `terraform plan -destroy` El resultado del comando muestra que el `destroy` comando eliminará todos los AWS recursos que se crearon anteriormente. 2. `terraform destroy -auto-approve` Este comando tarda aproximadamente 20 minutos en eliminar la infraestructura. **Note** Use el siguiente comando para eliminar todos los recursos administr ados por Terraform . : la etiqueta `-auto-approve` no espera la confirmación	

Tarea	Descripción	Habilidades requeridas

	del usuario para empezar a eliminar los recursos.
	3. Use los siguientes comandos para eliminar el archivo de estado de Terraform local:
	`rm .terraform.lock.hcl`
	`rm -rf .terraform`
	`rm terraform.tfstate*`	

Resolución de problemas

Problema	Solución
`null_resource.plugin_mgmt (local-exec): aws: error: argument operation: Invalid choice, valid choices are:`	Actualice la AWS CLI suya a la versión más reciente.
Error al cargar los orígenes de datos - `Fetch error: 404 Not Found Instantiating…`	El error es intermitente. Espere unos minutos y, a continuación, actualice los orígenes de datos para ver el origen de datos de Timestream de la lista.

Recursos relacionados

AWS documentación

- Amazon Managed Grafana para la creación de paneles y la visualización
- Configurar Grafana gestionada por Amazon para usar Okta

- Úsalo AWS IAM Identity Center con tu espacio de trabajo de Grafana gestionado por Amazon
- Trabajando con DAGs Amazon MWAA

AWS vídeos

- Configure el Centro de identidades de IAM con Amazon Managed Grafana para realizar la autenticación, tal como se muestra en el siguiente video.

https://www.youtube-nocookie.com/embed/XX2¿Xcz-Ps9U? controles = 0

- Si el Centro de identidades de IAM no está disponible, también puede integrar la autenticación de Amazon Managed Grafana mediante un proveedor de identidades (IdP) externo, como Okta, tal como se muestra en el siguiente video.

https://www.youtube-nocookie.com/embed/A4 Og? JHxl2xp controles = 0

Información adicional

Puede crear una solución integral de supervisión y alertas para su entorno de Amazon MWAA, que permita realizar una administración proactiva y obtener una respuesta rápida a posibles problemas o anomalías. Amazon Managed Grafana incluye las siguientes funciones:

Alertas: puede configurar alertas en Amazon Managed Grafana en función de los umbrales o condiciones predefinidos. Configure notificaciones por correo electrónico para alertar a las partes interesadas pertinentes cuando determinadas métricas superen o estén por debajo de los umbrales especificados. Para más información, consulte Alertas de Grafana en la documentación de Amazon Managed Grafana.

Integración: puedes integrar Grafana gestionada por Amazon con varias herramientas de terceros OpsGenie, como o Slack PagerDuty, para mejorar las capacidades de notificación. Por ejemplo, puedes configurar webhooks o integrarlos APIs para activar incidentes y notificaciones en estas plataformas en función de las alertas generadas en Grafana gestionado por Amazon. Además, este patrón proporciona un GitHub repositorio para crear AWS recursos. Puede integrar aún más este código con los flujos de trabajo de implementación de su infraestructura.

Adjunte automáticamente una política gestionada por AWS para Systems Manager a los perfiles de EC2 instancia mediante Cloud Custodian y AWS CDK

Ali Asfour y Aaron Lennon, Amazon Web Services

Resumen

Puede integrar las instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager para automatizar las tareas operativas y ofrecer más visibilidad y control. Para integrarse con Systems Manager, EC2 las instancias deben tener un agente de AWS Systems Manager (SSM Agent) instalado y una política de `AmazonSSMManagedInstanceCore` AWS Identity and Access Management (IAM) adjunta a sus perfiles de instancia.

Sin embargo, si quiere asegurarse de que todos los perfiles de EC2 instancia tengan la `AmazonSSMManagedInstanceCore` política adjunta, puede tener dificultades para actualizar nuevas EC2 instancias que no tienen perfiles de instancia o EC2 instancias que tienen un perfil de instancia pero no tienen la `AmazonSSMManagedInstanceCore` política. También puede resultar difícil añadir esta política en varias cuentas de Amazon Web Services (AWS) y regiones de AWS.

Este patrón ayuda a resolver estos desafíos mediante la implementación de tres políticas de Cloud Custodian en sus cuentas de AWS:

- La primera política de Cloud Custodian comprueba si hay EC2 instancias existentes que tienen un perfil de instancia pero que no cuentan con la `AmazonSSMManagedInstanceCore` política. A continuación, se adjunta la política `AmazonSSMManagedInstanceCore`.
- La segunda política de Cloud Custodian comprueba las EC2 instancias existentes sin un perfil de instancia y agrega un perfil de instancia predeterminado que incluye la `AmazonSSMManagedInstanceCore` política adjunta.
- La tercera política de Cloud Custodian crea funciones de AWS Lambda en sus cuentas para supervisar la creación EC2 de instancias y perfiles de instancias. Esto garantiza que la `AmazonSSMManagedInstanceCore` política se adjunte automáticamente al crear una EC2 instancia.

Este patrón utiliza DevOps las herramientas de AWS para lograr una implementación continua y a escala de las políticas de Cloud Custodian en un entorno de varias cuentas, sin aprovisionar un entorno informático independiente.

Requisitos previos y limitaciones

Requisitos previos

- Dos o más cuentas de AWS activas. Una cuenta es la cuenta de seguridad y las demás son cuentas de miembros.
- Permisos para aprovisionar recursos de AWS en la cuenta de seguridad. Este patrón utiliza permisos de administrador, pero usted debe conceder los permisos de acuerdo con los requisitos y las políticas de su organización.
- Capacidad para asumir un rol de IAM desde la cuenta de seguridad hasta las cuentas de los miembros y crear los roles de IAM necesarios. Para obtener más información al respecto, consulte Delegar el acceso entre cuentas de AWS utilizando roles de IAM en la documentación de IAM.
- **Important**

  Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada. Para realizar pruebas, puede configurar la AWS CLI mediante el comando `aws configure` o configurando variables de entorno. : esto no se recomienda para entornos de producción y recomendamos que a esta cuenta solo se le conceda el acceso con privilegios mínimos. Para obtener más información al respecto, consulte Conceder privilegios mínimos en la documentación de IAM.
- El archivo `devops-cdk-cloudcustodian.zip` (adjunto), descargado en su equipo local.
- Familiaridad con Python.
- Las herramientas necesarias (Node.js, AWS Cloud Development Kit (AWS CDK) y Git), instaladas y configuradas. Puede usar el archivo `install-prerequisites.sh` incluido en el archivo `devops-cdk-cloudcustodian.zip` para instalar estas herramientas. Asegúrese de ejecutar este archivo con privilegios de administrador.

Limitaciones

- Si bien este patrón se puede utilizar en un entorno de producción, asegúrese de que todos los roles y las políticas de IAM cumplan con los requisitos y las políticas de su organización.

Versiones de paquetes

- Cloud Custodian, versión 0.9 o posterior

- TypeScript versión 3.9.7 o posterior
- Node.js versión 14.15.4 o posterior
- `npm` versión 7.6.1 o posterior
- CDK de AWS, versión 1.96.0 o posterior

Arquitectura

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Las políticas de Cloud Custodian se envían a un CodeCommit repositorio de AWS en la cuenta de seguridad. Una regla de Amazon CloudWatch Events inicia automáticamente la CodePipeline canalización de AWS.
2. La canalización obtiene el código más reciente CodeCommit y lo envía a la parte de integración continua de la canalización de integración continua y entrega continua (CI/CD) gestionada por AWS. CodeBuild
3. CodeBuild realiza todas las DevSecOps acciones, incluida la validación de la sintaxis de las políticas de Cloud Custodian, y ejecuta estas políticas en `--dryrun` modo automático para comprobar qué recursos están identificados.
4. Si no hay errores, la siguiente tarea avisa al administrador para que revise los cambios y apruebe la implementación en las cuentas de los miembros.

Pila de tecnología

- AWS CDK
- CodeBuild
- CodeCommit
- CodePipeline
- IAM
- Cloud Custodian

Automatizar y escalar

El módulo AWS CDK Pipelines proporciona una CI/CD canalización que se utiliza CodePipeline para organizar la creación y las pruebas del código fuente CodeBuild, además de la implementación de los recursos de AWS con las pilas de AWS. CloudFormation Puede usar este patrón para todas las cuentas de miembros y regiones de su organización. También puede ampliar la pila `Roles creation` para implementar otros roles de IAM en sus cuentas de miembros.

Tools (Herramientas)

- El AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software para definir la infraestructura de nube en el código y aprovisionarla a través de AWS. CloudFormation
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos.
- AWS CodeBuild es un servicio de compilación en la nube totalmente gestionado.
- AWS CodeCommit es un servicio de control de versiones que puede utilizar para almacenar y gestionar activos de forma privada.
- AWS CodePipeline es un servicio de entrega continua que puede utilizar para modelar, visualizar y automatizar los pasos necesarios para lanzar el software.
- AWS Identity and Access Management (IAM) es un servicio web que le ayuda a controlar de forma segura el acceso a los recursos de AWS.
- Cloud Custodian es una herramienta que unifica las decenas de herramientas y scripts que la mayoría de las organizaciones utilizan para administrar sus cuentas de nube pública en una sola herramienta de código abierto.
- Node.js es un JavaScript motor de ejecución basado en el JavaScript motor V8 de Google Chrome.

Código

Para obtener una lista detallada de los módulos, las funciones de la cuenta, los archivos y los comandos de implementación que se utilizan en este patrón, consulte el archivo `README` en el archivo `devops-cdk-cloudcustodian.zip` (adjunto).

Epics

Configure la canalización con AWS CDK

Tarea	Descripción	Habilidades requeridas
Configura el CodeCommit repositorio.	1. Arranque el archivo `devops-cdk-cloudcustodian.zip` (adjunto) en el directorio de trabajo en su equipo local. 2. Inicie sesión en la consola de administración de AWS de su cuenta de seguridad, abra la CodeCommit consola y, a continuación, cree un `devops-cdk-cloudcustodian` repositorio nuevo. 3. Diríjase al directorio del proyecto y configure el CodeCommit repositorio como origen, confirme los cambios y, a continuación, envíelos a la rama de origen ejecutando los siguientes comandos: • `cd devops-cdk-cloudcustodian` • `git init --initial-branch=main` • `git add . git commit -m 'initial commit'`	Desarrollador

Tarea	Descripción	Habilidades requeridas
	• `git remote add origin https://git-codecommit.us-east-1.amazonaws.com/v1/devops-cdk-cloudcustodian` • `git push origin main` Para obtener más información al respecto, consulte Creación de un CodeCommit repositorio en la CodeCommit documentación de AWS.	
Instalar las herramientas necesarias.	Utilice el archivo `install-prerequisites.sh` para instalar todas las herramientas necesarias en Amazon Linux. Esto no incluye la AWS CLI porque viene preinstalada. Para obtener más información al respecto, consulte la sección Requisitos previos de Introducción a AWS CDK en la documentación de AWS CDK.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Instalar los paquetes de AWS CDK obligatorios.	1. Configure su entorno virtual ejecutando el siguiente comando en la CLI de AWS: `$ python3 -m venv .env` 2. Active su entorno virtual ejecutando el siguiente comando: `$ source .env/bin/activate` 3. Después de activar el entorno virtual, instale las dependencias necesarias mediante la ejecución del siguiente comando: `$ pip install -r requirements.txt` 4. Para añadir dependencias adicionales (por ejemplo, otras bibliotecas de AWS CDK), agréguelas al archivo `requirements.txt` y ejecute el siguiente comando: `pip install -r requirements.txt` AWD CDK requiere los siguientes paquetes y se incluyen en el archivo `requirements.txt` : • `aws-cdk.aws-cloudwatch`	Desarrollador

Tarea	Descripción	Habilidades requeridas
	• `aws-cdk.aws-codebuild` • `aws-cdk.aws-codecommit` • `aws-cdk.aws-codedeploy` • `aws-cdk.aws-codepipeline` • `aws-cdk.aws-codepipeline-actions` • `aws-cdk.aws-events` • `aws-cdk.aws-events-targets` • `aws-cdk.aws-iam` • `aws-cdk.aws-logs` • `aws-cdk.aws-s3` • `aws-cdk.aws-sns` • `aws-cdk.aws-sns-subscriptions` • `aws-cdk.aws-sqs` • `aws-cdk.core`	

Configuración de su entorno.

Tarea	Descripción	Habilidades requeridas
Actualice las variables requeridas.	Abra el `vars.py` archivo en la carpeta raíz del CodeCommit repositorio y actualice las siguientes variables:	Desarrollador

Tarea	Descripción	Habilidades requeridas
	• Actualice `var_deploy_region = 'us-east-1'` con la región de AWS en la que desea implementar la canalización. • Actualízalo `var_codecommit_repo_name = "cdk-cloudcustodian"` con el nombre de tu CodeCommit repositorio. • Actualiza `var_codecommit_branch_name = "main"` con el nombre de la CodeCommit sucursal. • Actualice `var_adminEmail=notifyadmin@email.com'` con la dirección de correo electrónico del administrador que aprueba los cambios. • Actualice `var_slackWebHookUrl = https://hooks.slack.com/services/T000000000/B00000000/XXXXXXXXXXXXXXXXXXXXXXXX` con el webhook de Slack que se utiliza para enviar notificaciones a Cloud Custodian cuando se realizan cambios. • Actualice `var_orgId = 'o-yyyyyyyyyy'` con el ID de su organización.	

Tarea	Descripción	Habilidades requeridas
	• Actualice `security_account = '123456789011'` con el ID de cuenta de AWS para la cuenta en la que se implementa la canalización. • Actualice `member_accounts = ['111111111111','111111111112','111111111113']` con las cuentas de los miembros en las que desee iniciar la pila de AWS CDK e implementar los roles de IAM necesarios. • Configure `cdk_bootstrap_member_accounts = True` como `True` si desea que la canalización inicie automáticamente AWS CDK en sus cuentas de miembros. Si se configura como `True`, esto también requiere el nombre de un rol de IAM existente en las cuentas de los miembros que se pueda asumir desde la cuenta de seguridad. Este rol de IAM también debe tener los permisos necesarios para arrancar AWS CDK.	

Tarea	Descripción	Habilidades requeridas
	• **Note** Actualice `cdk_bootstrap_role = 'AWSControlTowerExecution'` con el rol de IAM existente en las cuentas de los miembros que se pueden asumir desde la cuenta de seguridad. Este rol también debe tener permiso para arrancar AWS CDK. : Esto sólo se aplica si `cdk_bootstrap_member_accounts` está configurado en `True`.	

Tarea	Descripción	Habilidades requeridas

Actualice el archivo account.yml con la información de la cuenta del miembro.	Para ejecutar la herramienta Cloud Custodian de c7n-org en varias cuentas, debe colocar el archivo de configuración `accounts.yml` en la raíz del repositorio. A continuación, se muestra un ejemplo de archivo de configuración de Cloud Custodian para AWS.
	`accounts:`
	`- account_id: '123123123123'`
	`  name: account-1`
	`  regions:`
	`  - us-east-1`
	`  - us-west-2`
	`  role: arn:aws:iam::123123123123:role/CloudCustodian`
	`  vars:`
	`  charge_code: xyz`
	`  tags:`
	`  - type:prod`
	`  - division:some division`
	`  - partition:us`
	`  - scope:pci`
		Desarrollador

Arrancar las cuentas de AWS

Tarea	Descripción	Habilidades requeridas
Arranque la cuenta de seguridad.	Arranque `deploy_account` con la aplicación `cloudcust`	Desarrollador

Tarea	Descripción	Habilidades requeridas
	`odian_stack` ejecutando el siguiente comando: `cdk bootstrap -a 'python3 cloudcustodian/cloudcustodian_stack.py`	
Opción 1: arrancar automáticamente las cuentas de los miembros.	Si la variable `cdk_bootstrap_member_accounts` está establecida en `True` en el archivo `vars.py`, la canalización arranca automáticamente las cuentas especificadas en la variable `member_accounts` . Si es necesario, puede actualizar `*cdk_bootstrap_role*` con un rol de IAM que pueda asumir desde la cuenta de seguridad y que tenga los permisos necesarios para arrancar la AWS CDK. La canalización arranca automáticamente las cuentas nuevas que se agreguen a la variable `member_accounts` para poder implementar los roles necesarios.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Opción 2: Inicie manualmente el proceso de arranque de las cuentas de los miembros.	Aunque no se recomiend a utilizar este enfoque, puede establecer el valor de `cdk_bootstrap_memb er_accounts` y `False`, y realizar este paso manualmen te ejecutando el siguiente comando: `$ cdk bootstrap -a 'python3 cloudcust odian/member_accou nt_roles_stack.py' \ --trust {security _account_id} \ --context assume-ro le-credentials:wri teIamRoleName={rol e_name} \ --context assume-ro le-credentials:rea dIamRoleName={role _name} \ --mode=ForWriting \ --context bootstrap =true \ --cloudformation- execution-policies arn:aws:iam::aws:p olicy/Administrato rAccess`	Desarrollador

Tarea	Descripción	Habilidades requeridas
	Important Asegúrese de actualizar los valores `{security_account_id}` y `{role_name}` con el nombre de un rol de IAM que pueda asumir desde la cuenta de seguridad y que tenga los permisos necesarios para iniciar el proceso de arranque de AWS CDK. También puede utilizar otros enfoques para impulsar las cuentas de los miembros, por ejemplo, con AWS CloudFormation. Para obtener más información al respecto, consulte Proceso de arranque en la documentación de AWS CDK.	

Implemente la pila de AWD CDK.

Tarea	Descripción	Habilidades requeridas
Cree los roles de IAM en las cuentas de los miembros.	Ejecute el siguiente comando para implementar la pila	Desarrollador

Tarea	Descripción	Habilidades requeridas
	`member_account_roles_stack` y crear los roles de IAM en las cuentas de miembros: `cdk deploy --all -a 'python3 cloudcustodian/member_account_roles_stack.py' --require-approval never`	
Implemente la pila de canalizaciones de Cloud Custodian.	Ejecute el siguiente comando para crear la canalización `cloudcustodian_stack.py` de Cloud Custodian que se implementa en la cuenta de seguridad: `cdk deploy -a 'python3 cloudcustodian/cloudcustodian_stack.py'`	Desarrollador

Recursos relacionados

- Introducción a los AWS CDK

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Cree CI/CD canalizaciones y clústeres de Amazon ECS de forma automática para microservicios mediante AWS CDK

Varsha Raju, Amazon Web Services

Resumen

Este patrón describe cómo crear automáticamente la integración continua y la entrega continua (CI/CD) pipelines and underlying infrastructure for building and deploying microservices on Amazon Elastic Container Service (Amazon ECS). You can use this approach if you want to set up proof-of-concept CI/CD pipelines to show your organization the benefits of CI/CD, microservices, and DevOps. You can also use this approach to create initial CI/CDpipelines), que luego puede personalizar o cambiar de acuerdo con los requisitos de su organización.

El enfoque del patrón crea un entorno de producción y un entorno de no producción, cada uno con una nube privada virtual (VPC) y un clúster de Amazon ECS configurado para ejecutarse en dos zonas de disponibilidad. Todos los microservicios comparten estos entornos y, a continuación, se crea una CI/CD canalización para cada microservicio. Estas CI/CD canalizaciones extraen los cambios de un repositorio de origen en AWS CodeCommit, los crean automáticamente y, a continuación, los implementan en sus entornos de producción y no producción. Cuando una canalización completa correctamente todas sus etapas, puede utilizarla URLs para acceder al microservicio en los entornos de producción y no producción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa.
- Un bucket de Amazon Simple Storage Service (Amazon S3) existente que contiene el archivo `starter-code.zip` (adjunto).
- AWS Cloud Development Kit (AWS CDK), instalado y configurado en su cuenta. Para obtener más información al respecto, consulte Introducción a AWS CDK en la documentación de AWS CDK.
- Python 3 y `pip`, instalado y configurado. Para obtener más información, consulte la documentación de Python.
- Familiaridad con AWS CDK CodeBuild, CodePipeline AWS, CodeCommit Amazon Elastic Container Registry (Amazon ECR), Amazon ECS y AWS Fargate.
- Conocimientos de Docker.

- Una comprensión de y. CI/CD DevOps

Limitaciones

- Se aplican límites generales a las cuentas de AWS. Para obtener más información al respecto, consulte AWS Service Quotas en la documentación de referencia general de AWS.

Versiones de producto

- El código se probó usando Node.js versión 16.13.0 y AWS CDK versión 1.132.0.

Arquitectura

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un desarrollador de aplicaciones envía el código a un CodeCommit repositorio.
2. Se inicia una canalización.
3. CodeBuild compila y envía la imagen de Docker a un repositorio de Amazon ECR
4. CodePipeline implementa una nueva imagen en un servicio Fargate existente en un clúster de Amazon ECS que no es de producción.
5. Amazon ECS extrae la imagen del repositorio de Amazon ECR y la coloca en un servicio Fargate de no producción.
6. Las pruebas se realizan mediante una URL de no producción.
7. El administrador de versiones aprueba la implementación de producción.
8. CodePipeline implementa la nueva imagen en un servicio Fargate existente en un clúster de Amazon ECS de producción
9. Amazon ECS extrae la imagen del repositorio de Amazon ECR y la coloca en el servicio Fargate de producción.
10. Los usuarios de producción acceden a su característica mediante una URL de producción.

Pila de tecnología

- AWS CDK
- CodeBuild

- CodeCommit
- CodePipeline
- Amazon ECR
- Amazon ECS
- Amazon VPC

Automatización y escala

Puede utilizar el enfoque de este patrón para crear canalizaciones para los microservicios implementados en una pila de AWS CloudFormation compartida. La automatización puede crear más de un clúster de Amazon ECS en cada VPC y también crear canalizaciones para los microservicios implementados en un clúster de Amazon ECS compartido. Sin embargo, esto requiere que proporcione nueva información sobre los recursos como entradas a la pila de canalizaciones.

Tools (Herramientas)

- AWS CDK: el AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software para definir la infraestructura de nube en el código y aprovisionarla a través de AWS. CloudFormation
- AWS CodeBuild: AWS CodeBuild es un servicio de compilación en la nube totalmente gestionado. CodeBuild compila su código fuente, ejecuta pruebas unitarias y produce artefactos que están listos para su implementación.
- AWS CodeCommit: AWS CodeCommit es un servicio de control de versiones que le permite almacenar y gestionar de forma privada los repositorios de Git en la nube de AWS. CodeCommit elimina la necesidad de administrar su propio sistema de control de código fuente o de preocuparse por escalar su infraestructura.
- AWS CodePipeline: AWS CodePipeline es un servicio de entrega continua que puede utilizar para modelar, visualizar y automatizar los pasos necesarios para lanzar su software. Puede modelar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software. CodePipeline automatiza los pasos necesarios para publicar los cambios de software de forma continua.
- Amazon ECS: Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores altamente escalable y rápido que se utiliza para ejecutar, detener y administrar contenedores en un clúster. Las tareas y los servicios se pueden ejecutar en una infraestructura sin servidor administrada por AWS Fargate. Alternativamente, para obtener más control sobre

su infraestructura, puede ejecutar sus tareas y servicios en un clúster de instancias de Amazon Elastic Compute Cloud (Amazon EC2) que administre.

- Docker: Docker ayuda a los desarrolladores a empaquetar, enviar y ejecutar cualquier aplicación como un contenedor ligero, portátil y autosuficiente.

Código

El código de este patrón está disponible en los archivos `cicdstarter.zip` y `starter-code.zip` (adjuntos).

Epics

Configure su entorno

Tarea	Descripción	Habilidades requeridas
Configure el directorio de trabajo de AWS CDK.	1. Cree un directorio denominado `cicdproject` en su máquina local. 2. Descargue el archivo `cicdstarter.zip` (adjunto) al directorio `cicdproject` y descomprímalo. Esto crea una carpeta denominada `cicdstarter`. 3. Ejecute el comando `cd <user-home>/cicdproject/cicdstarter`. 4. Configure el entorno virtual de Python ejecutando el comando `python3 -m venv .venv`. 5. Ejecute el comando `source ./.venv/bin/activate`.	AWS DevOps, infraestructura en la nube

Tarea	Descripción	Habilidades requeridas
	6. Configure su entorno de AWS ejecutando el comando `aws configure` o utilizando las siguientes variables de entorno: • `AWS_ACCESS_KEY_ID` • `AWS_SECRET_ACCESS_KEY` • `AWS_DEFAULT_REGION`	

Crear la infraestructura compartida

Tarea	Descripción	Habilidades requeridas
Cree la infraestructura compartida.	1. En su directorio de trabajo, ejecute el comando `cd cicdvpcecs .` 2. Ejecute el comando `pip3 install -r requirements.txt` para instalar todas las dependencias de Python necesarias. 3. Ejecute el `cdk bootstrap` command para configurar el entorno de AWS para AWS CDK. 4. Ejecute el comando `cdk synth --context aws_account=<aws_account_ID> --context aws_region=<aws-region> .`	AWS DevOps, infraestructura en la nube

Tarea	Descripción	Habilidades requeridas
	5. Ejecute el comando `cdk deploy --context aws_account=<aws_account_ID> --context aws_region=<aws-region>` .	
	6. La CloudFormation pila de AWS crea la siguiente infraestructura: • Una VPC de no producción denominada `cicd-vpc-ecs/cicd-vpc-nonprod` • Una VPC de producción denominada `cicd-vpc-ecs/cicd-vpc-prod` • Un clúster de Amazon ECS de no producción denominado `cicd-ecs-nonprod` • Un clúster de Amazon ECS de producción denominado `cicd-ecs-prod`	

Tarea	Descripción	Habilidades requeridas
Supervise la CloudFormation pila de AWS.	1. Inicie sesión en la consola de administración de AWS, abra la CloudFormation consola de AWS y, a continuación, elija la `cicd-vpc-ecs` pila de la lista. 2. En el panel de detalles de la pila, seleccione la pestaña Eventos y supervise el progreso de la creación de la pila.	AWS DevOps, infraestructura en la nube

Tarea	Descripción	Habilidades requeridas
Pruebe la CloudFormation pila de AWS.	1. Una vez creada la CloudFormation pila de `cicd-vpc-ecs` AWS, asegúrese de que `cicd-vpc-ecs/cicd-vpc-prod` VPCs se `cicd-vpc-ecs/cicd-vpc-nonprod` hayan creado las y. 2. Asegúrese de que se creen los clústeres de Amazon ECS `cicd-ecs-nonprod` y `cicd-ecs-prod` . **Important** Asegúrese de registrar el grupo de seguridad IDs para los dos VPCs y el grupo de seguridad IDs para los grupos de seguridad predeterminados en ambos VPCs.	AWS DevOps, infraestructura en la nube

Cree una CI/CD canalización para un microservicio

Tarea	Descripción	Habilidades requeridas
Cree la infraestructura para el microservicio.	1. Asigne un nombre a su microservicio. Por ejemplo, este patrón utiliza	AWS DevOps, infraestructura en la nube

Tarea	Descripción	Habilidades requeridas
	`myservice1` como nombre del microservicio. 2. En su directorio de trabajo, ejecute el comando `cd <working-directory>/cdkpipeline` . 3. Ejecute el comando `pip3 install -r requirements.txt` . 4. Ejecute el comando `cdk synth` completo que está disponible en la sección de Información adicional de este patrón. 5. Ejecute el comando `cdk deploy` completo que está disponible en la sección de Información adicional de este patrón. **Note** También puede proporcionar los valores de ambos comandos mediante el archivo `cdk.json` del directorio.	

Tarea	Descripción	Habilidades requeridas
Supervise la CloudFormation pila de AWS.	Abra la CloudFormation consola de AWS y supervise el progreso de la `myservice 1-cicd-stack` pila. Finalmente, el estado cambia a `CREATE_COMPLETE` .	AWS DevOps, infraestructura en la nube

Tarea	Descripción	Habilidades requeridas
Pruebe la CloudFormation pila de AWS.	1. En la CodeCommit consola de AWS, compruebe que `myservice1` existe un repositorio con el nombre y que contiene el código de inicio. 2. En la CodeBuild consola de AWS, compruebe que `myservice1` existe un proyecto de compilación denominado. 3. En la consola de Amazon ECR, verifique que existe un repositorio de Amazon ECR denominado `myservice1` . 4. En la consola de Amazon ECS, verifique que exista un servicio de Fargate denominado `myservice1` en un clúster de Amazon ECS tanto de no producción como de producción. 5. En la consola de Amazon Elastic Compute Cloud (Amazon EC2), verifique que se hayan creado los equilibradores de carga de aplicaciones de no producción y de producción. Registre los nombres DNS del ALBs.	

Tarea	Descripción	Habilidades requeridas
	6. En la CodePipeline consola de AWS, compruebe que `myservice1` existe una canalización con el nombre. Debe tener las etapas `Source`, `Build`, `Deploy-NonProd` y `Deploy-Prod`. La canalización también debe tener un estado `in progress`. 7. Supervise la canalización hasta que se completen todas las etapas. 8. Apruébela manualmente para la producción. 9. En una ventana del navegador, introduzca los nombres DNS del ALBs. 10. La aplicación debería mostrarse tanto `Hello World` en la fase de producción como en la de producción URLs.	

Tarea	Descripción	Habilidades requeridas
Use la canalización.	1. Abra el CodeCommit repositorio que creó anteriormente y abra el `index.js` archivo. 2. Sustituya `Hello World` por `Hello CI/CD`. 3. Guarde y confirme los cambios en la rama principal. 4. Verifique que la canalización se inicie y que el cambio pase por las etapas `Build`, `Deploy-NonProd` y `Deploy-Prod` . 5. Apruebe la producción manualmente. 6. Ahora URLs deberían *`Hello CICD`* mostrarse tanto la producción como la no producción.	AWS DevOps, infraestructura en la nube
Repita esta épica para cada microservicio.	Repita las tareas de esta epopeya para crear una CI/CD canalización para cada uno de sus microservicios.	AWS DevOps, infraestructura en la nube

Recursos relacionados

- Uso de Python con AWS CDK
- Referencia sobre Python de AWS CDK
- Creación de un servicio de AWS Fargate con AWS CDK

Información adicional

Comando de la **`cdk synth`**

```
cdk synth --context aws_account=<aws_account_number> --context
 aws_region=<aws_region> --context vpc_nonprod_id=<id_of_non_production
 VPC> --context vpc_prod_id=<id_of_production_VPC> --context
 ecssg_nonprod_id=< default_security_group_id_of_non-production_VPC>
 --context ecssg_prod_id=<default_security_group_id_of_production_VPC>
 --context code_commit_s3_bucket_for_code=<S3 bucket name> --context
 code_commit_s3_object_key_for_code=<Object_key_of_starter_code> --context
 microservice_name=<name_of_microservice>
```

`cdk deploy` command

```
cdk deploy --context aws_account=<aws_account_number> --context
 aws_region=<aws_region> --context vpc_nonprod_id=<id_of_non_production_VPC>
 --context vpc_prod_id=<id_of_production_VPC> --context ecssg_nonprod_id=<
 default_security_group_id_of_non-production_VPC> --context
 ecssg_prod_id=<default_security_group_id_of_production_VPC> --
context code_commit_s3_bucket_for_code=<S3 bucket name> --context
 code_commit_s3_object_key_for_code=<Object_key_of_starter_code> --context
 microservice_name=<name_of_microservice>
```

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Cree e inserte imágenes de Docker en Amazon ECR mediante GitHub Actions y Terraform

Ruchika Modi, Amazon Web Services

Resumen

Este patrón explica cómo puede crear GitHub flujos de trabajo reutilizables para crear su Dockerfile y enviar la imagen resultante a Amazon Elastic Container Registry (Amazon ECR). El patrón automatiza el proceso de creación de sus Dockerfiles mediante Terraform y Actions. GitHub Esto minimiza la posibilidad de que se cometan errores humanos y reduce sustancialmente el tiempo de implementación.

Una GitHub acción de envío a la rama principal de tu GitHub repositorio inicia el despliegue de los recursos. El flujo de trabajo crea un repositorio Amazon ECR único en función de la combinación de la GitHub organización y el nombre del repositorio. A continuación, inserta la imagen de Dockerfile en un repositorio de Amazon ECR.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una GitHub cuenta activa.
- Un GitHub repositorio.
- La versión 1 o posterior de Terraform instalada y configurada.
- Un bucket de Amazon Simple Storage Service (Amazon S3) para el backend de Terraform.
- Una tabla de Amazon DynamoDB para el bloqueo y la coherencia del estado de Terraform. La tabla debe tener una clave de partición denominada `LockID` con un tipo de `String`. Si no está configurado, se deshabilitará el bloqueo por estado.
- Un rol de AWS Identity and Access Management (IAM) con permisos para configurar el backend de Amazon S3 para Terraform. Para obtener instrucciones sobre la configuración, consulte la documentación de Terraform.

Limitaciones

Este código reutilizable solo se ha probado con GitHub Actions.

Arquitectura

Pila de tecnología de destino

- Repositorio de Amazon ECR
- GitHub Acciones
- Terraform

Arquitectura de destino

En el siguiente diagrama se ilustra lo siguiente:

1. Un usuario añade plantillas de Dockerfile y Terraform al repositorio. GitHub

2. Estas adiciones inician un GitHub flujo de trabajo de acciones.

3. El flujo de trabajo comprueba si existe un repositorio de Amazon ECR. De lo contrario, crea el repositorio en función de la GitHub organización y el nombre del repositorio.

4. El flujo de trabajo crea el Dockerfile e inserta la imagen en el repositorio de Amazon ECR.

Tools (Herramientas)

Servicios de Amazon

- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de contenedor administrado que es seguro, escalable y fiable.

Otras herramientas

- GitHub Actions está integrado en la GitHub plataforma para ayudarte a crear, compartir y ejecutar flujos de trabajo en tus GitHub repositorios. Puedes usar GitHub Actions para automatizar tareas como crear, probar e implementar tu código.
- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar infraestructuras locales y en la nube.

Repositorio de código

El código de este patrón está disponible en el repositorio de flujos de trabajo de GitHub Docker ECR Actions.

- Al crear GitHub acciones, los archivos de flujo de trabajo de Docker se guardan en la `/.github/workflows/` carpeta de este repositorio. El flujo de trabajo de esta solución se encuentra en el archivo workflow.yaml.
- La carpeta `e2e-test` proporciona un ejemplo de Dockerfile para consultarlo y probarlo.

Prácticas recomendadas

- Para conocer las prácticas recomendadas para escribir Dockerfiles, consulte la documentación de Docker.
- Use un punto de conexión de VPC para Amazon ECR. Los puntos de enlace de VPC funcionan con AWS PrivateLink, una tecnología que le permite acceder de forma privada a Amazon ECR a APIs través de direcciones IP privadas. Para las tareas de Amazon ECS que utilizan el tipo de lanzamiento Fargate, el punto de conexión de VPC permite a la tarea extraer imágenes privadas de Amazon ECR sin necesidad de asignar una dirección IP pública a la tarea.

Epics

Configure el proveedor y el repositorio del OIDC GitHub

Tarea	Descripción	Habilidades requeridas
Configure OpenID Connect.	Cómo crear un proveedor de OpenID Connect (OIDC) Usará el proveedor de la política de confianza para el rol de IAM que se use en esta acción. Para obtener instrucciones, consulte Configuración de OpenID Connect en Amazon Web Services en la GitHub documentación.	Administrador de AWS DevOps, AWS general

Tarea	Descripción	Habilidades requeridas
Clona el GitHub repositorio.	Clona el repositorio de GitHub Docker ECR Actions Workflow en tu carpeta local: `$git clone https://github.com/aws-samples/docker-ecr-actions-workflow`	DevOps ingeniero

Personalice el flujo de trabajo GitHub reutilizable e implemente la imagen de Docker

Tarea	Descripción	Habilidades requeridas
Personalice del evento que inicia el flujo de trabajo de Docker.	El flujo de trabajo de esta solución se encuentra en workflow.yaml. Actualmente, este script está configurado para implementar recursos cuando recibe el evento `workflow_dispatch` . Para personalizar esta configuración, cambe el evento a `workflow_call` y llame al flujo de trabajo desde otro flujo de trabajo principal.	DevOps ingeniero
Personalice el flujo de trabajo.	El archivo workflow.yaml está configurado para crear un flujo de trabajo dinámico y reutilizable. GitHub Puedes editar este archivo para personalizar la configuración predeterminada o puedes pasar los valores de entrada desde la	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	consola de GitHub Actions si utilizas el `workflow_dispatch` evento para iniciar la implementación manualmente.
	• Asegúrese de especificar el ID de cuenta de AWS y la región de destino correctos.
	• Cree una política de ciclo de vida de Amazon ECR (consulte la política de ejemplo) y actualice la ruta predeterminada (`e2e-test/policy.json`) en consecuencia.
	• El archivo del flujo de trabajo requiere dos roles de IAM como entrada:
	  • Un rol de IAM que tiene permisos para configura r el backend de Amazon S3 para Terraform (consulte la sección Requisitos previos). Puede actualizar el nombre del rol predeterm inado `workload-assumable-role` en el archivo `.yaml` en consecuencia.
	  • Un rol de IAM que tiene permisos de acceso GitHub. Este rol también	

Tarea	Descripción	Habilidades requeridas
	se utiliza en la política de Amazon ECR para restringir las operaciones de Amazon ECR. Para obtener más información, consulte el archivo data.tf file.	
Implemente las plantillas de Terraform.	El flujo de trabajo implementa automáticamente las plantillas de Terraform que crean el repositorio de Amazon ECR, en función del GitHub evento que haya configurado. Estas plantillas están disponibles como archivos `.tf` en la raíz del repositorio de Github.	AWS DevOps, DevOps ingeniero

Resolución de problemas

Problema	Solución
Problemas o errores al configurar Amazon S3 y DynamoDB como el backend remoto de Terraform.	Siga las instrucciones de la documentación de Terraform para configurar los permisos necesarios en los recursos de Amazon S3 y DynamoDB para la configuración del backend remoto.
No se pudo ejecutar ni iniciar el flujo de trabajo con el evento `workflow_dispatch` .	El flujo de trabajo que está configurado para implementarse desde el evento `workflow_dispatch` solo funcionará si también está configurado en la rama principal.

Recursos relacionados

- Reutilización de flujos de trabajo (GitHub documentación)
- Activación de un flujo de trabajo (documentación) GitHub

Cree y pruebe aplicaciones iOS con AWS CodeCommit CodePipeline, AWS y AWS Device Farm

Abdullahi Olaoye, Amazon Web Services

Resumen

Este patrón describe los pasos para crear una canalización de integración y entrega continuas (CI/CD) que utilice AWS CodePipeline para crear y probar aplicaciones iOS en dispositivos reales de AWS. El patrón utiliza AWS CodeCommit para almacenar el código de la aplicación, la herramienta de código abierto de Jenkins para crear la aplicación iOS y AWS Device Farm para probar la aplicación creada en dispositivos reales. Estas tres fases se organizan juntas en una canalización mediante AWS CodePipeline.

Este patrón se basa en la publicación Creación y prueba de aplicaciones iOS y iPadOS con AWS DevOps y servicios móviles en el DevOps blog de AWS. Para obtener instrucciones más detalladas, consulte la entrada del blog.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una cuenta de desarrollador de Apple
- Servidor de compilación (macOS)
- Xcode versión 11.3 (instalada y configurada en el servidor de compilación)
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada en la estación de trabajo
- Conocimientos básicos de Git

Limitaciones

- El servidor de compilación de aplicaciones debe ejecutar macOS.
- El servidor de compilación debe tener una dirección IP pública, por lo que CodePipeline puede conectarse a ella de forma remota para iniciar las compilaciones.

Arquitectura

Pila de tecnología de origen

- Un proceso de creación de aplicaciones iOS en las instalaciones que implica el uso de un simulador o una prueba manual en dispositivos físicos

Pila de tecnología de destino

- Un CodeCommit repositorio de AWS para almacenar el código fuente de las aplicaciones
- Un servidor Jenkins para compilar aplicaciones con Xcode
- Un conjunto de dispositivos de AWS Device Farm para probar aplicaciones en dispositivos reales

Arquitectura de destino

Cuando un usuario confirma cambios en el repositorio fuente, la canalización (AWS CodePipeline) recupera el código del repositorio fuente, inicia una compilación de Jenkins y pasa el código de la aplicación a Jenkins. Tras la compilación, la canalización recupera el artefacto de compilación e inicia un trabajo de AWS Device Farm para probar la aplicación en un grupo de dispositivos.

Tools (Herramientas)

- AWS CodePipeline es un servicio de entrega continua totalmente gestionado que le ayuda a automatizar sus procesos de lanzamiento para obtener actualizaciones rápidas y fiables de las aplicaciones y la infraestructura. CodePipeline automatiza las fases de creación, prueba e implementación del proceso de lanzamiento cada vez que se produce un cambio de código, en función del modelo de lanzamiento que defina.
- AWS CodeCommit es un servicio de control de código fuente totalmente gestionado que aloja repositorios seguros basados en Git. Facilita a los equipos la colaboración en el código en un ecosistema seguro y altamente escalable. CodeCommit elimina la necesidad de operar su propio sistema de control de código fuente o preocuparse por escalar su infraestructura.
- AWS Device Farm es un servicio de pruebas de aplicaciones que le permite mejorar la calidad de sus aplicaciones web y móviles probándolas en una amplia gama de navegadores de escritorio y dispositivos móviles reales, sin tener que aprovisionar ni administrar ninguna infraestructura de pruebas.

- Jenkins es un servidor de código abierto de automatización que permite a los desarrolladores crear, probar e implementar su software.

Epics

Configure el entorno de compilación

Tarea	Descripción	Habilidades requeridas
Instalar Jenkins en el servidor de compilación que ejecuta macOS.	Jenkins se utilizará para crear la aplicación, por lo que debe instalarla antes de nada en el servidor de compilación. Para obtener instrucciones detalladas para esta y otras tareas posteriores, consulte la entrada del blog de AWS sobre cómo crear y probar aplicaciones iOS y iPadOS con AWS DevOps y servicios móviles y otros recursos en la sección Recursos relacionados al final de este patrón.	DevOps
Configure Jenkins.	Siga las instrucciones en pantalla para configurar Jenkins.	DevOps
Instale el CodePipeline complemento de AWS para Jenkins.	Este complemento debe estar instalado en el servidor de Jenkins para que Jenkins interactúe con el servicio de AWS CodePipeline .	DevOps
Cree un proyecto de estilo libre de Jenkins.	En Jenkins, cree un proyecto de estilo libre. Configure el proyecto para especificar los activadores y otras opciones	DevOps

Tarea	Descripción	Habilidades requeridas
	de configuración de compilación.	

Configure AWS Device Farm

Tarea	Descripción	Habilidades requeridas
Cree un proyecto de Device Farm.	Abra la consola de AWS Device Farm. Cree un proyecto y un grupo de dispositivos para realizar pruebas. Consulte esta entrada de blog para obtener instrucciones.	Desarrollador

Configure el repositorio de origen

Tarea	Descripción	Habilidades requeridas
Cree un CodeCommit repositorio.	Cree un repositorio donde se almacenará el código fuente.	DevOps
Confirme el código de la aplicación en el repositorio.	Conéctese al CodeCommit repositorio que creó. Inserte el código desde el equipo local en el repositorio.	DevOps

Configure la canalización

Tarea	Descripción	Habilidades requeridas
Cree una canalización en AWS CodePipeline.	Abra la CodePipeline consola de AWS y cree una canalizac	DevOps

Tarea	Descripción	Habilidades requeridas
	ión. La canalización organiza todas las fases del CI/CD proceso. Para obtener instrucciones, consulte la entrada del blog de AWS sobre cómo crear y probar aplicaciones iOS y iPadOS con AWS DevOps y servicios móviles.	
Añada una etapa de prueba a la canalización.	Edite la canalización para añadir una etapa de prueba e integrarla con AWS Device Farm.	DevOps
Inicie la canalización.	Para iniciar la canalización y el CI/CD proceso, selecciona Release change.	DevOps

Vea los resultados de las pruebas de la aplicación

Tarea	Descripción	Habilidades requeridas
Revisar los resultados de la prueba.	En la consola de AWS Device Farm, seleccione el proyecto que creó y revise los resultados de las pruebas. La consola mostrará los detalles de cada prueba.	Desarrollador

Recursos relacionados

Step-by-step instrucciones para este patrón

- Creación y prueba de aplicaciones para iOS y iPadOS con AWS DevOps y servicios móviles (entrada del DevOps blog de AWS)

Configure AWS Device Farm

- Consola AWS Device Farm

Configure el repositorio de origen

- Crear un CodeCommit repositorio de AWS
- Conéctese a un CodeCommit repositorio de AWS

Configure la canalización

- CodePipeline Consola AWS

Recursos adicionales

- CodePipeline Documentación de AWS
- CodeCommit Documentación de AWS
- Documentación de AWS Device Farm
- Documentación de Jenkins
- Instalación de Jenkins en macOS
- CodePipeline Complemento de AWS para Jenkins
- Instalación de Xcode
- Instalación y configuración de AWS CLI
- Documentación de Git

Configure autenticación TLS mutua para aplicaciones ejecutadas en Amazon EKS

Mahendra Revanasiddappa, Amazon Web Services

Resumen

La seguridad mutua de la capa de transporte (TLS) basada en certificado es un componente de TLS opcional que proporciona autenticación entre pares bidireccional para servidores y clientes. Con la TLS mutua, los clientes deben proporcionar un certificado X.509 durante el proceso de negociación de la sesión. El servidor utiliza este certificado para identificar y autenticar al cliente.

El TLS mutuo es un requisito común para las aplicaciones de Internet de las cosas (IoT) y se puede usar para business-to-business aplicaciones o estándares como la banca abierta.

Este patrón describe cómo configurar TLS mutua para aplicaciones ejecutadas en un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) mediante un controlador de entrada de NGINX. Puede habilitar las funciones de TLS mutua integradas para el controlador de entrada de NGINX anotando el recurso de entrada. Para obtener más información sobre las anotaciones de TLS mutua en los controladores NGINX, consulte Autenticación con certificados de cliente en la documentación de Kubernetes.

> **Important**
>
> Este patrón emplea certificados autofirmados. Se recomienda utilizar este patrón solo con clústeres de prueba y no en entornos de producción. Si desea usar este patrón en un entorno de producción, puede usar AWS Private Certificate Authority (AWS Private CA) o su estándar de infraestructura de clave pública (PKI) existente para emitir certificados privados.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa.
- Un clúster existente de Amazon EKS.
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 1.7, instalada y configurada en macOS, Linux o Windows.

- Utilidad de línea de comandos kubectl, instalada y configurada para acceder al clúster de Amazon EKS. Para obtener más información sobre esto, consulte Instalar kubectl en la documentación de Amazon EKS.
- Un nombre existente de sistema de nombres de dominio (DNS) para probar la aplicación.

Limitaciones

- Este patrón emplea certificados autofirmados. Se recomienda utilizar este patrón solo con clústeres de prueba y no en entornos de producción.

Arquitectura

Pila de tecnología

- Amazon EKS
- Amazon Route 53
- Kubectl

Tools (Herramientas)

- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar Kubernetes en AWS sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.
- Kubectl es una utilidad de línea de comandos que se usa para interactuar con un clúster de Amazon EKS.

Epics

Genere los certificados autofirmados

Tarea	Descripción	Habilidades requeridas
Genere el certificado y la clave del servidor.	Genere la clave y el certificado de la entidad de certificación	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	(CA) mediante el siguiente comando. `openssl req -x509 -sha256 -newkey rsa:4096 -keyout ca.key -out ca.crt -days 356 -nodes -subj '/CN=Test Cert Authority'`	
Genere la clave y el certificado del servidor y firme con el certificado de CA.	Genere la clave y el certificado del servidor y firme con el certificado de CA, utilizando el siguiente comando. `openssl req -new -newkey rsa:4096 -keyout server.key -out server.csr -nodes -subj '/CN= <your_domain_name> ' && openssl x509 -req -sha256 -days 365 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt` **Important** Asegúrese de sustituir `<your_domain_name>` por su nombre de dominio actual.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Genere la clave y el certifica do del cliente y firme con el certificado de CA.	Genere la clave y el certificado del cliente, y firme la entidad de certificación (CA) mediante el siguiente comando. `openssl req -new -newkey rsa:4096 -keyout client.key -out client.csr -nodes -subj '/CN=Test' && openssl x509 -req -sha256 -days 365 -in client.csr -CA ca.crt -CAkey ca.key -set_serial 02 -out client.crt`	DevOps ingeniero

Implemente el controlador de entrada NGINX

Tarea	Descripción	Habilidades requeridas
Implemente el controlador de entrada de NGINX en el clúster de Amazon EKS.	Implemente el controlador de entrada de NGINX con el comando siguiente. `kubectl apply -f https://raw.githubusercontent.com/kubernetes/ingress-nginx/controller-v1.7.0/deploy/static/provider/aws/deploy.yaml`	DevOps ingeniero
Compruebe que el servicio de controlador de entrada de NGINX está en ejecución.	Compruebe que el servicio de controlador de entrada de NGINX está en ejecución	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	utilizando el siguiente comando. `kubectl get svc -n ingress-nginx` **Important** Asegúrese de que el campo de dirección del servicio contenga el nombre de dominio del equilibrador de carga de red.	

Cree un espacio de nombres en el clúster de Amazon EKS para probar la TLS mutua

Tarea	Descripción	Habilidades requeridas
Cree un espacio de nombres en el clúster de Amazon EKS.	Ejecute el siguiente comando para crear un espacio de nombres llamado `mtls` en el clúster de Amazon EKS. `kubectl create ns mtls` Se implementará la aplicación de ejemplo para probar la TLS mutua.	DevOps ingeniero

Cree la implementación y el servicio de la aplicación de ejemplo

Tarea	Descripción	Habilidades requeridas

Cree la implementación y el servicio de Kubernetes en el espacio de nombres mtls.	Cree un archivo denominado `mtls.yaml` . Pegue el código siguiente en el archivo.
	
	`kind: Deployment`
	`apiVersion: apps/v1`
	`metadata:`
	`  name: mtls-app`
	`  labels:`
	`  app: mtls`
	`spec:`
	`  replicas: 1`
	`  selector:`
	`  matchLabels:`
	`  app: mtls`
	`  template:`
	`  metadata:`
	`  labels:`
	`  app: mtls`
	`  spec:`
	`  containers:`
	`  - name: mtls-app`
	`  image: hashicorp`
	`/http-echo`
	`  args:`
	`  - "-text=mTLS`
	` is working"`
	
	`---`
	
	`kind: Service`
	`apiVersion: v1`
	`metadata:`
	`  name: mtls-service`
	`spec:`
	`  selector:`
	`  app: mtls`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	<pre>ports:
	  - port: 5678 #
	Default port for image</pre>
	Crea la implementación y el servicio de Kubernetes en el espacio de nombres `mtls` ejecutando el siguiente comando.
	<pre>kubectl create -f
	mtls.yaml -n mtls</pre>	

Compruebe que se ha creado la implementación de Kubernetes.	Ejecute el siguiente comando para comprobar que la implementación se ha creado y que hay un pod en estado disponible.
	<pre>kubectl get deploy -n
	mtls</pre>
		DevOps ingeniero

Compruebe que el servicio Kubernetes se ha creado.	Compruebe que el servicio de Kubernetes se haya creado ejecutando el siguiente comando.
	<pre>kubectl get service -n
	mtls</pre>
		DevOps ingeniero

Cree un secreto en el espacio de nombres mtls

Tarea	Descripción	Habilidades requeridas
Cree un recurso para el recurso de entrada.	Ejecute el siguiente comando para crear un secreto en el controlador de entrada NGINX con los certificados que creó anteriormente. `kubectl create secret generic mtls-certs --from-file=tls.crt=server.crt --from-file=tls.key=server.key --from-file=ca.crt=ca.crt -n mtls` Su secreto tiene un certificado de servidor para que el cliente identifique el servidor, y un certificado de CA para que el servidor verifique los certificados del cliente.	DevOps ingeniero

Cree el recurso de entrada en el espacio de nombres mtls

Tarea	Descripción	Habilidades requeridas
Cree el recurso de entrada en el espacio de nombres mtls.	Cree un archivo denominado `ingress.yaml` . Pegue el siguiente código en el archivo (sustituya `<your_domain_name>` por su nombre de dominio actual).	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	<pre>apiVersion: networkin
	g.k8s.io/v1
	kind: Ingress
	metadata:
	  annotations:
	    nginx.ingress.kube
	rnetes.io/auth-tls-
	verify-client: "on"
	    nginx.ingress.kube
	rnetes.io/auth-tls-
	secret: mtls/mtls-certs
	  name: mtls-ingress
	spec:
	  ingressClassName:
	 nginx
	  rules:
	  - host: "*.<your_
	domain_name>"
	    http:
	      paths:
	      - path: /
	        pathType: Prefix
	        backend:
	          service:
	            name: mtls-
	service
	            port:
	              number:
	 5678
	  tls:
	  - hosts:
	    - "*.<your_
	domain_name>"
	    secretName: mtls-
	certs</pre>
	Cree el recurso de entrada en el espacio de nombres `mtls` ejecutando el siguiente comando.	

Tarea	Descripción	Habilidades requeridas
	`kubectl create -f ingress.yaml -n mtls` Así, el controlador de entrada de NGINX podrá enrutar el tráfico a su aplicación de muestra.	
Compruebe que se ha creado el recurso de entrada.	Compruebe que el servicio de entrada se haya creado ejecutando el siguiente comando. `kubectl get ing -n mtls` **Important** Asegúrese de que la dirección del recurso de entrada muestre el equilibrador de carga creado para el controlador de entrada de NGINX.	DevOps ingeniero

Configure el DNS para que dirija el nombre de host al equilibrador de carga

Tarea	Descripción	Habilidades requeridas
Cree un registro CNAME que apunte al equilibrador de carga del controlador de entrada de NGINX.	Inicie sesión en la consola de administración de AWS, abra la consola de Amazon Route 53 y cree un registro de nombre canónico (CNAME)	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	que apunte `mtls.<your_domain_name>` al equilibrador de carga del controlador de entrada de NGINX. Para obtener más información, consulte Creación de registros con la consola de Amazon Route 53 en la documentación de Route 53.	

Pruebe la aplicación

Tarea	Descripción	Habilidades requeridas
Pruebe la configuración de TLS mutua sin certificados.	Ejecute el comando siguiente. `curl -k https://mtls.<your_domain_name>` Debería recibir la respuesta de error “400 No required SSL certificate was sent”.	DevOps ingeniero
Pruebe la configuración de TLS mutua con certificados.	Ejecute el comando siguiente. `curl -k https://mtls.<your_domain_name> --cert client.crt --key client.key` Debería recibir la respuesta “mTLS is working”.	DevOps ingeniero

Recursos relacionados

- Creación de registros con la consola de Amazon Route 53
- Uso de un equilibrador de carga de red con el controlador de entrada de NGINX en Amazon EKS
- Autenticación con certificado de cliente

Automatice la creación de recursos de Amazon WorkSpaces Applications mediante AWS CloudFormation

Ram Kandaswamy, Amazon Web Services

Resumen

Este patrón proporciona ejemplos de código y pasos para automatizar la creación de recursos de Amazon WorkSpaces Applications en el Nube de AWS mediante una AWS CloudFormationplantilla. El patrón le muestra cómo utilizar una CloudFormation pila para automatizar la creación de los recursos de WorkSpaces las aplicaciones, incluidos un generador de imágenes, una imagen, una instancia de flota y una pila. Puede transmitir su aplicación de WorkSpaces aplicaciones a los usuarios finales a través HTML5 de un navegador compatible mediante el modo de entrega de aplicaciones o de escritorio.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Una aceptación de los términos y condiciones de la WorkSpaces solicitud
- Conocimientos básicos de los recursos de WorkSpaces las aplicaciones, como las flotas y las pilas y los creadores de imágenes

Limitaciones

- No puede modificar el rol AWS Identity and Access Management(IAM) asociado a una instancia de WorkSpaces Applications una vez creada esa instancia.
- No puede modificar las propiedades (como la subred o el grupo de seguridad) de la instancia del generador de imágenes de WorkSpaces Applications una vez creado el generador de imágenes.

Arquitectura

En el siguiente diagrama, se muestra cómo automatizar la creación de recursos de WorkSpaces aplicaciones mediante una CloudFormation plantilla.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Puedes crear una CloudFormation plantilla basada en el código YAML en la sección de información adicional de este patrón.
2. La CloudFormation plantilla crea una pila CloudFormation de pruebas.
   a. (Opcional) Puede crear una instancia de creación de imágenes mediante WorkSpaces Aplicaciones.
   b. (Opcional) Puede crear una imagen de Windows con su software personalizado.
3. La CloudFormation pila crea una flota de WorkSpaces aplicaciones, una instancia y una pila.
4. Usted despliega los recursos de sus WorkSpaces aplicaciones para los usuarios finales en un navegador HTML5 compatible.

Tools (Herramientas)

- Amazon WorkSpaces Applications es un servicio de streaming de aplicaciones totalmente gestionado que le proporciona acceso instantáneo a sus aplicaciones de escritorio desde cualquier lugar. WorkSpaces Applications administra los AWS recursos necesarios para alojar y ejecutar sus aplicaciones, se amplía automáticamente y proporciona acceso a sus usuarios cuando lo soliciten.
- AWS CloudFormationle ayuda a modelar y configurar sus AWS recursos, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Puede gestionar y aprovisionar pilas en varios Cuentas de AWS y. Regiones de AWS

Prácticas recomendadas

- Configure correctamente el acceso a la red para los creadores de imágenes: inicie los creadores de imágenes en subredes de nube privada virtual (VPC) con el acceso adecuado a Internet mediante una puerta de enlace NAT para el acceso a Internet solo saliente.

  Pruebe la conectividad de la red con los recursos necesarios (como servidores de aplicaciones, bases de datos y servidores de licencias) antes de crear imágenes. Compruebe que las tablas de enrutamiento de la VPC permiten las conexiones a todos los recursos de red necesarios. Para obtener más información, consulte el acceso a Internet en la documentación de las WorkSpaces aplicaciones.
- Supervise la capacidad de la flota comparándola con las cuotas de servicio de forma proactiva: WorkSpaces las cuotas de tipo y tamaño de las instancias de las aplicaciones se calculan por

Cuenta de AWS unidad Región de AWS. Si tiene varias flotas en la misma región que utilicen el mismo tipo y tamaño de instancia, el número total de instancias de todas las flotas de esa región debe ser inferior o igual a la cuota aplicable. Para obtener más información, consulte Solución de problemas de flotas en la documentación de las WorkSpaces aplicaciones.

- Pruebe las aplicaciones en el modo de prueba de Image Builder antes del despliegue de la flota: valide siempre las aplicaciones en el modo de prueba de Image Builder antes de crear imágenes e implementarlas en las flotas. El modo de prueba simula los permisos limitados que tienen los usuarios finales en las instancias de la flota. Para obtener más información, consulte Solución de problemas con los generadores de imágenes en la documentación de WorkSpaces las aplicaciones.

Epics

(Opcional) Cree una imagen de la WorkSpaces aplicación

Tarea	Descripción	Habilidades requeridas
Instale un software personalizado y cree una imagen.	1. Inicie el generador de imágenes y elija los tipos de instancias, la subred, el grupo de seguridad correspondientes, etc. 2. Usa el modo de administración mientras te conectas a la instancia. 3. Usa el asistente de imágenes o un PowerShell script para crear una nueva imagen de Windows para tu software personalizado. **Note** Considere la posibilidad de utilizar la	AWS DevOps, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	AppLocker función de Windows para bloquear aún más la imagen.	

Implemente la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Actualice la CloudFormation plantilla.	1. Usa el código de la sección de información adicional de este patrón como un archivo YAML. 2. Actualice el archivo YAML con los valores necesarios para los parámetros de su entorno.	Administrador de sistemas de AWS, administrador de la nube, arquitecto de la nube, AWS general, administrador de AWS
Crea una CloudFormation pila con la plantilla.	1. Inicie sesión en la CloudFormation consola Consola de administración de AWS y ábrala. 2. En el panel de navegación, seleccione Pilas. 3. Seleccione Crear pila y, a continuación, seleccione Con nuevos recursos (estándar). 4. En Requisito previo: preparación de la plantilla, seleccione La plantilla está lista.	Propietario de la aplicación, administrador de sistemas de AWS, ingeniero de Windows

Tarea	Descripción	Habilidades requeridas
	5. En la sección Especificar plantilla, seleccione Cargar un archivo de plantilla. 6. Selecciona Elegir archivo y, a continuación, elige tu CloudFormation plantilla actualizada. 7. Complete el resto de los pasos del asistente para crear su pila.	

Resolución de problemas

Problema	Solución
Varios problemas	Para obtener más información, consulte Solución de problemas en la documentación de WorkSpaces las aplicaciones.

Recursos relacionados

Referencias

- Introducción a Amazon WorkSpaces Applications: configuración con aplicaciones de muestra
- Cree una flota y una pila de WorkSpaces aplicaciones de Amazon

Tutoriales y videos

- Flujo de trabajo WorkSpaces de usuario de Amazon Applications
- Cómo migrar una aplicación antigua de Windows Forms a Amazon WorkSpaces Applications
- AWS re:Invent 2018: Entregue aplicaciones de escritorio de forma segura con Amazon WorkSpaces Applications (01) BAP2

Información adicional

El siguiente código es un ejemplo de una CloudFormation plantilla que puede utilizar para crear automáticamente recursos de WorkSpaces aplicaciones.

```
AWSTemplateFormatVersion: 2010-09-09
Parameters:
  SubnetIds:
    Type: 'List<AWS::EC2::Subnet::Id>'
  testSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup::Id'
  ImageName:
    Type: String
Resources:

  AppStreamFleet:
    Type: 'AWS::AppStream::Fleet'
    Properties:
      ComputeCapacity:
        DesiredInstances: 5
      InstanceType: stream.standard.medium
      Name: appstream-test-fleet
      DisconnectTimeoutInSeconds: 1200
      FleetType: ON_DEMAND
      IdleDisconnectTimeoutInSeconds: 1200
      ImageName: !Ref ImageName
      MaxUserDurationInSeconds: 345600
      VpcConfig:
        SecurityGroupIds:
          - !Ref testSecurityGroup
        SubnetIds: !Ref SubnetIds
  AppStreamStack:
    Type: 'AWS::AppStream::Stack'
    Properties:
      Description: AppStream stack for test
      DisplayName: AppStream test Stack
      Name: appstream-test-stack
      StorageConnectors:
        - ConnectorType: HOMEFOLDERS
      UserSettings:
        - Action: CLIPBOARD_COPY_FROM_LOCAL_DEVICE
          Permission: ENABLED
        - Action: CLIPBOARD_COPY_TO_LOCAL_DEVICE
```

```
        Permission: ENABLED
      - Action: FILE_DOWNLOAD
        Permission: ENABLED
      - Action: PRINTING_TO_LOCAL_DEVICE
        Permission: ENABLED
AppStreamFleetAssociation:
  Type: 'AWS::AppStream::StackFleetAssociation'
  Properties:
    FleetName: appstream-test-fleet
    StackName: appstream-test-stack
  DependsOn:
    - AppStreamFleet
    - AppStreamStack
```

Crear un analizador de registros personalizado para Amazon ECS mediante un enrutador de registros Firelens

Varun Sharma, Amazon Web Services

Resumen

Firelens es un router de registros para Amazon Elastic Container Service (Amazon ECS) y AWS Fargate. Puede usar Firelens para enrutar los registros de contenedores desde Amazon ECS a Amazon CloudWatch y otros destinos (por ejemplo, Splunk o Sumo Logic). Firelens funciona con Fluentd o Fluent Bit como agente de registro, lo que significa que puede utilizar los parámetros de definición de tareas de Amazon ECS para enrutar los registros.

Al elegir analizar los registros en el nivel de origen, puede analizar los datos de registro y realizar consultas para responder de manera más eficiente y eficaz a los problemas operativos. Como las distintas aplicaciones tienen patrones de registro diferentes, es necesario utilizar un analizador personalizado que estructure los registros y facilite la búsqueda en el destino final.

Este patrón utiliza un router de registro Firelens con un analizador personalizado para enviar los registros CloudWatch desde una aplicación Spring Boot de muestra que se ejecuta en Amazon ECS. A continuación, puede utilizar Amazon CloudWatch Logs Insights para filtrar los registros en función de los campos personalizados generados por el analizador personalizado.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa.
- Interfaz de la línea de comandos de AWS (AWS CLI), instalada y configurada en su equipo local.
- Docker, instalado y configurado en su equipo local.
- Una aplicación en contenedores existente basada en Spring Boot en Amazon Elastic Container Registry (Amazon ECR).

Arquitectura

Pila de tecnología

- CloudWatch
- Amazon ECR
- Amazon ECS
- Fargate
- Docker
- Fluent Bit

Tools (Herramientas)

- Amazon ECR: Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado por AWS que es seguro, escalable y fiable.
- Amazon ECS: Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores altamente escalable y rápido que facilita la tarea de ejecutar, detener y administrar contenedores en un clúster.
- AWS Identity and Access Management (IAM): IAM es un servicio web que le ayuda a controlar el acceso seguro a los servicios de AWS.
- AWS CLI: la interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.
- Docker – Docker es una plataforma abierta para desarrollar, enviar y ejecutar aplicaciones.

Código

Los siguientes archivos se adjuntan a este patrón:

- `customFluentBit.zip` – Contiene los archivos para añadir el análisis y las configuraciones personalizados.
- `firelens_policy.json` – Contiene el documento de política para crear una política de IAM.
- `Task.json` – Contiene una muestra de definición de tarea para Amazon ECS.

Epics

Crear una imagen de Fluent Bit personalizada

Tarea	Descripción	Habilidades requeridas
Cree un repositorio de Amazon ECR.	Inicie sesión en la consola de administración de AWS, abra la consola de Amazon ECR y cree un repositorio llamado `fluentbit_custom` . Para obtener más informaci ón al respecto, consulte Creación de un repositorio en la documentación de Amazon ECR.	Administrador de sistemas, desarrollador
Descomprima el paquete .zip. customFluentBit	1. Descargue el paquete `customFluentBit.zip` (adjunto) en su máquina local. 2. Descomprima en el directorio `customFluentBit` ejecutando el siguiente comando: `unzip -d customFluentBit.zip` 3. El directorio contiene los siguientes archivos que son necesarios para añadir el análisis y las configuraciones personalizados: • `parsers/springboot_parser.conf –`	

Tarea	Descripción	Habilidades requeridas
	Contiene la directiva del analizador y define el patrón de expresión regular (regex) del analizador personalizado. Puede añadir el patrón de expresiones regulares para su analizador específico. • `conf/parse_springboot.conf` – Contiene el filtro y la directiva de servicio. • El Dockerfile	

Tarea	Descripción	Habilidades requeridas
Cree la imagen de Docker personalizada.	1. Cambie el directorio a `customFluentBit .` 2. Abra la consola Amazon ECR, seleccione el repositorio `fluentbit _custom` y, a continuación, seleccione Ver comandos push. 3. Cargar su proyecto 4. Una vez que finalice el proceso de carga, copie la URL de la compilación. Esta URL es obligatoria al crear un contenedor en Amazon ECS Para más informaciónf sobre esto, consulte Insertar una imagen de Docker en la documentación de Amazon ECR.	Administrador de sistemas, desarrollador

Configure el clúster de Amazon ECS

Tarea	Descripción	Habilidades requeridas
Cree un clúster de Amazon ECS.	Cree un clúster de Amazon ECS siguiendo las instrucciones de la sección sobre Plantillas exclusivas para redes de la sección Creación de un clúster de la documentación de Amazon ECS.	Administrador de sistemas, desarrollador

Tarea	Descripción	Habilidades requeridas
	Note Asegúrese de seleccionar Crear VPC para crear una nueva nube privada virtual (VPC) para su clúster de Amazon ECS.	

Configurar la tarea de Amazon ECS

Tarea	Descripción	Habilidades requeridas
Configurar el rol de IAM de ejecución de tareas de Amazon ECS	Cree un rol de IAM de ejecución de tareas de Amazon ECS con la política `AmazonECSTaskExecutionRolePolicy` administrada. Para obtener más información al respecto, consulte Rol de IAM de ejecución de tareas de Amazon ECS en la documentación de Amazon ECS. **Note** Asegúrese de registrar el Nombre de recurso de Amazon (ARN) del rol de IAM.	Administrador de sistemas, desarrollador

Tarea	Descripción	Habilidades requeridas
Adjunte la política de IAM al rol de IAM de ejecución de tareas de Amazon ECS.	1. Cree una política de IAM mediante el documento de política `firelens_policy.json` (adjunto). Para obtener más información al respecto, consulte Creación de políticas en la pestaña JSON de la documentación de IAM. 2. Adjunte esta política al rol de IAM de ejecución de tareas de Amazon ECS que creó anteriormente. Para obtener más información al respecto, consulte Cómo añadir políticas de IAM (AWS CLI) en la documentación de IAM.	Administrador de sistemas, desarrollador

Tarea	Descripción	Habilidades requeridas
Configure la definición de tarea de Amazon ECS.	1. Actualice las siguientes secciones de la definición de tarea de muestra `Task.json` (adjunta): • Actualice `executionRoleArn` y `taskRoleArn` con el ARN del rol de IAM de ejecución de tareas • Actualice la imagen en `containerDefinitions` con la imagen de Docker personalizada de Fluent Bit que creó anteriormente • Actualice la imagen en `containerDefinitions` con el nombre de la imagen de su aplicación 2. Abra la consola de Amazon ECS, seleccione Definiciones de tareas, seleccione Crear nueva definición de tarea y, a continuación, seleccione Fargate en la página de Selección de compatibilidades. 3. Seleccione Configurar mediante Json, pegue el archivo `Task.json` actualizado en el área de texto y, a continuación, seleccione Guardar.	Administrador de sistemas, desarrollador

Tarea	Descripción	Habilidades requeridas
	4. Crear una definición de tarea. Para obtener más informaci ón al respecto, consulte Crear una definición de tarea en la documentación de Amazon ECS.	

Ejecutar la tarea de Amazon ECS

Tarea	Descripción	Habilidades requeridas
Ejecute la tarea de Amazon ECS.	En la consola de Amazon ECS, seleccione Clústeres, seleccione el clúster que creó anteriormente y, a continuac ión, ejecute la tarea independi ente. Para obtener más información al respecto, consulte Ejecutar una tarea independiente en la documentación de Amazon ECS.	Administrador de sistemas, desarrollador

Verifica los registros CloudWatch

Tarea	Descripción	Habilidades requeridas
Verifique los registros.	1. Abra la CloudWatch consola, elija Grupos de registros y, a continuac ión, elija`/aws/ecs/`	Administrador de sistemas, desarrollador

Tarea	Descripción	Habilidades requeridas
	`containerinsights/{{cluster_ARN}}/firelens/application`. 2. Verifique los registros, en particular los campos personalizados agregados por el analizador personalizado. 3. Se utiliza CloudWatch para filtrar los registros en función de los campos personalizados.	

Recursos relacionados

- Conceptos básicos de Docker para Amazon ECS
- Amazon ECS en AWS Fargate
- Configuración de parámetros de servicio básicos

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Cree un marco de orquestación de recursos basado en API con GitHub Actions y Terragrunt

Tamilselvan P, Abhigyan Dandriyal, Sandeep Gawande y Akash Kumar, Amazon Web Services

Resumen

Este patrón aprovecha los flujos de trabajo de GitHub Actions para automatizar el aprovisionamiento de recursos mediante cargas JSON estandarizadas, lo que elimina la necesidad de realizar una configuración manual. Esta canalización automatizada gestiona todo el ciclo de vida de la implementación y puede integrarse sin problemas con varios sistemas frontend, desde componentes de interfaz de usuario personalizados hasta componentes de interfaz de usuario personalizados. ServiceNow La flexibilidad de la solución permite a los usuarios interactuar con el sistema a través de sus interfaces preferidas y, al mismo tiempo, mantener los procesos estandarizados.

La arquitectura de canalización configurable se puede adaptar para cumplir con diferentes requisitos organizativos. La implementación de ejemplo se centra en el aprovisionamiento de Amazon Virtual Private Cloud (Amazon VPC) y de Amazon Simple Storage Service (Amazon S3). El patrón aborda de manera efectiva los desafíos comunes de administración de los recursos de la nube al estandarizar las solicitudes en toda la organización y proporcionar puntos de integración consistentes. Este enfoque facilita a los equipos la solicitud y la administración de los recursos y, al mismo tiempo, garantiza la estandarización.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Una GitHub cuenta activa con acceso al repositorio configurado

Limitaciones

- Los nuevos recursos requieren la adición manual de archivos `terragrunt.hcl` a la configuración del repositorio.
- Algunas Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

En el siguiente diagrama se muestran los componentes y el flujo de trabajo de este patrón.

En el siguiente diagrama de arquitectura se muestran las siguientes acciones:

1. El usuario envía una carga útil de JSON a GitHub Actions, lo que desencadena el proceso de automatización.
2. La canalización de GitHub Actions recupera el código de recursos necesario de los repositorios de Terragrunt y Terraform, en función de las especificaciones de la carga útil.
3. La canalización asume la función AWS Identity and Access Management (IAM) adecuada con el ID especificado. Cuenta de AWS A continuación, la canalización despliega los recursos en el destino Cuenta de AWS y administra el estado de Terraform mediante el bucket de Amazon S3 específico de la cuenta y la tabla de Amazon DynamoDB.

Cada uno Cuenta de AWS contiene funciones de IAM para un acceso seguro, un depósito de Amazon S3 para el almacenamiento de estados de Terraform y una tabla de DynamoDB para el bloqueo de estados. Este diseño permite la implementación controlada y automatizada de los recursos en todas las Cuentas de AWS. El proceso de implementación mantiene una administración del estado y un control de acceso adecuados a través de buckets de Amazon S3 dedicados y roles de IAM en cada cuenta.

Tools (Herramientas)

Servicios de AWS

- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Otras herramientas

- GitHub Actions es una plataforma de integración y entrega continuas (CI/CD) que está estrechamente integrada con los repositorios. GitHub Puedes usar GitHub Actions para automatizar tu proceso de creación, prueba e implementación.
- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que te ayuda a crear y administrar recursos locales y en la nube.
- Terragrunt es una herramienta de orquestación que amplía las capacidades de Terraform y las de Terraform. OpenTofu Administra la forma en que se aplican los patrones de infraestructura genéricos, lo que facilita la escalación y el mantenimiento de grandes conjuntos de infraestructuras.

Repositorio de código

El código de este patrón está disponible en el repositorio -terraform. GitHub sample-aws-orchestration-pipeline

Prácticas recomendadas

- Almacene AWS las credenciales y los datos confidenciales utilizando los secretos GitHub del repositorio para un acceso seguro.
- Configure el proveedor OpenID Connect (OIDC) para que GitHub Actions asuma la función de IAM y evite las credenciales estáticas.
- Cumpla con el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Creación y configuración del repositorio

Tarea	Descripción	Habilidades requeridas
Inicialice el repositorio. GitHub	Para inicializar el GitHub repositorio, siga estos pasos:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	1. Cree un GitHub repositorio nuevo para alojar el código de canalización. 2. Importe los archivos `deployment.yml` y `workflow-trigger.yml` que se encuentran en la carpeta .github/workflows del repositorio de origen.	
Configure los permisos y roles de IAM	Para configurar los permisos y roles de IAM, siga estos pasos: 1. Cree un rol de IAM con las relaciones de confianza necesarias para que GitHub Actions se conecte a las acciones AWS mediante un proveedor de identidades (IdP) de OpenID Connect (OIDC). 2. Adjunte los permisos necesarios al rol de IAM para crear el backend y los recursos deseados. Para obtener más información, consulte un ejemplo de política para crear una VPC con Amazon VPC junto con el bucket de Amazon S3 de backend y la tabla de DynamoDB.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Configura GitHub secretos y variables.	Para obtener instrucciones sobre cómo configurar los secretos y las variables del repositorio en el GitHub repositorio, consulte Crear variables de configuración para un repositorio en la GitHub documentación. Configure las siguientes variables:
	• Secretos del repositorio
	  • `PAT_TOKEN` — Tu token de acceso personal con los permisos para realizar GitHub operaciones
	• Variables de repositorio
	  • `aws_role`— El rol de IAM, Amazon Resource Name (ARN) con los permisos adecuados para implementar los recursos necesarios y GitHub conectar acciones con acciones en AWS
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Cree la estructura del repositorio.	Para crear la estructura del repositorio, siga estos pasos: 1. Cree una nueva carpeta en la ramificación `main` para almacenar el archivo `terragrunt.hcl` , así como las salidas y los registros de cambios tras la creación del recurso. 2. Asigne un nombre en minúsculas a la carpeta según el tipo de recurso que desee aprovisio nar a través de ella. La carpeta se usa tal cual más adelante en la carga útil. Para obtener más informaci ón, consulte un ejemplo de estructura para Amazon S3 y Amazon VPC en el repositorio.	DevOps ingeniero

Desencadenamiento de la canalización y validación de los resultados

Tarea	Descripción	Habilidades requeridas
Ejecute la canalización con curl.	Para ejecutar la canalizac ión mediante curl, siga estos pasos: 1. Cree un archivo payload.j son en su directorio local. Siga la estructura definida	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	para el archivo de carga útil y estratifíquela antes de enviar la solicitud. Para obtener más información, consulte las cargas útiles de ejemplo en el repositorio. 2. Envía la solicitud en tu terminal mediante la GitHub API, como se muestra en el siguiente ejemplo: `curl -X POST \ -H "Accept: application/vnd.github.v3+json" \ -H "Authorization: token YOUR_GITHUB_TOKEN" \ -d @payload.json \ https://api.github.com/repos/OWNER/REPO/actions/workflows/workflow-trigger.yml/dispatches` En el ejemplo, proporcione sus propios valores para lo siguiente: • `YOUR_GITHUB_TOKEN` con tu token de acceso GitHub personal • `OWNER` con el nombre de usuario del propietario del repositorio	

Tarea	Descripción	Habilidades requeridas
	• REPO con el nombre del repositorio Para obtener más información sobre el proceso de ejecución de la canalización, consulte Información adicional.	

Tarea	Descripción	Habilidades requeridas
Validación de los resultados de la ejecución de la canalización	Para validar los resultados, siga estos pasos: 1. Supervisa la ejecución del flujo de trabajo de GitHub acciones en la pestaña Acciones de tu repositorio. 2. Tras la ejecución correcta de los flujos de trabajo, compruebe la creación de los recursos de la Consola de administración de AWS siguiente manera: a. Para Amazon VPC: • Navegue hasta el servicio Amazon VPC en el lugar especific ado. Región de AWS • Compruebe si hay una nueva VPC con etiquetas que coincidan con los parámetros de su solicitud. • Verifique el bloque de CIDR y otras configura ciones. b. Para Amazon S3: • Navegue hasta los buckets de Amazon S3. • En los buckets de uso general, compruebe si	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	hay un bucket nuevo que coincida con los parámetros de su solicitud. • Verifique el nombre del bucket de S3 y otras configuraciones. También puede realizar una verificación cruzada de los recursos creados mediante el archivo `output.json` creado en el repositorio que se encuentra dentro del mismo recurso que el archivo `terragrunt.hcl` .	

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Envíe una solicitud de limpieza.	Para eliminar recursos que ya no son necesarios, siga estos pasos: 1. Envíe la solicitud de eliminación mediante el mismo punto de conexión de la API, pero modifique la carga útil de la siguiente manera: • Cambie `RequestType` a `delete` en `RequestParameters` .	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• Mantenga todos los demás parámetros idénticos a los de la solicitud de `create`. 2. Supervisa el proceso de eliminación en GitHub Actions. 3. Una vez finalizado el flujo de trabajo, verifique que el archivo `changelog.json` dentro de la carpeta de recursos muestre el estado de `deleted`. 4. Compruebe la eliminación de recursos mediante la Consola de administración de AWS.	

Recursos relacionados

AWS Blogs

- Utilice las funciones de IAM para conectar GitHub las acciones con las acciones de AWS

Servicio de AWS documentación

- creación de roles de IAM
- Supervisión de archivos de CloudTrail registro con Amazon CloudWatch Logs
- Prácticas recomendadas de seguridad para Amazon S3

GitHub resources

- Creación de un evento de envío de repositorios

- Creación de webhooks
- Implemente controles de acceso sólidos en el repositorio GitHub
- Auditoría periódica del acceso al repositorio
- Controles de seguridad en CI/CD proceso
- Utilice la autenticación multifactorial para las cuentas GitHub

Información adicional

Proceso de ejecución en canalización

Los siguientes son los pasos de la ejecución de la canalización:

1. Valida el formato de carga útil JSON: garantiza que la configuración JSON entrante esté estructurada correctamente y contenga todos los parámetros necesarios
2. Asume la función de IAM especificada: autentica y asume la función de IAM requerida para las operaciones AWS
3. Descarga el código de Terraform y Terragrunt necesario: recupera la versión especificada del código de recursos y las dependencias
4. Ejecuta el despliegue de recursos: aplica la configuración para implementar o actualizar los AWS recursos en el entorno de destino

Ejemplo de carga útil utilizada para la creación de VPC

A continuación, se muestra un ejemplo de código para la creación de un bucket de estado del backend de Terraform:

```
state_bucket_name = "${local.payload.ApplicationName}-${local.payload.EnvironmentId}-
tfstate"
```

```
lock_table_name = "${local.payload.ApplicationName}-${local.payload.EnvironmentId}-
tfstate-lock"
```

A continuación se muestra un ejemplo de carga útil para crear una VPC con Amazon VPC, donde `vpc_cidr` define las especificaciones del bloque de CIDR para la VPC. El bucket de estado de Terraform se asigna a una variable definida en los archivos `terraform`. El parámetro `ref` contiene el nombre de la ramificación del código que se va a ejecutar.

```
{
    "ref": "main",
    "inputs": {
        "RequestParameters": {
            "RequestId": "1111111",
            "RequestType": "create",
            "ResourceType": "vpc",
            "AccountId": "1234567890",
            "AccountAlias": "account-alias",
            "RegionId": "us-west-2",
            "ApplicationName": "myapp",
            "DivisionName": "division-name",
            "EnvironmentId": "dev",
            "Suffix": "poc"
        },
        "ResourceParameters": [
            {
                "VPC": {
                    "vpc_cidr": "10.0.0.0/16"
                }
            }
        ]
    }
}
```

Los `RequestParameters` se utilizan para rastrear el estado de la solicitud en la sección de canalización y `tfstate` se crea en función de esta información. Los parámetros siguientes contienen información de control y metadatos:

- `RequestId`: identificador único para la solicitud
- `RequestType`: tipo de operación (crear, actualizar o eliminar)
- `ResourceType`: tipo de recurso que se va a aprovisionar
- `AccountId`— Objetivo de Cuenta de AWS despliegue
- `AccountAlias`— Nombre descriptivo para el Cuenta de AWS
- `RegionId`— Región de AWS para el despliegue de recursos
- `ApplicationName`: nombre de la aplicación.
- `DivisionName`: división de la organización
- `EnvironmentId`: entorno (por ejemplo, desarrollo y producción)

- `Suffix`: identificador adicional para los recursos

Los `ResourceParameters` contienen una configuración específica del recurso que se asigna a las variables definidas en los archivos de Terraform. Se debe incluir en `ResourceParameters` cualquier variable personalizada que deba pasarse a los módulos de Terraform. El parámetro `vpc_cidr` es obligatorio para Amazon VPC.

Cree solicitudes de cambios automatizadas para la AWS infraestructura gestionada por Terraform mediante Actions GitHub

Matt Padgett, Ashish Bhatt, Ashwin Divakaran, Sandip Gangapadhyay y Prafful Gupta, Amazon Web Services

Resumen

Este patrón presenta una utilidad de automatización diseñada para eliminar el trabajo manual y repetitivo que implica la gestión de los cambios en varios repositorios de Terraform. Muchas organizaciones utilizan los repositorios de Terraform para administrar su infraestructura como código (IaC), a menudo con cientos de repositorios independientes que representan diferentes entornos, servicios o equipos. Administrar estos repositorios a escala presenta un desafío operativo importante. Las tareas rutinarias, como la actualización de un parámetro, la actualización de las versiones de los módulos o la aplicación de cambios de configuración, suelen requerir la creación y la gestión de solicitudes de extracción (PRs) en muchos repositorios varias veces al día.

Incluso en el caso de cambios sencillos, este proceso manual y repetitivo lleva mucho tiempo y es propenso a errores. Los ingenieros deben aplicar el mismo cambio de forma coherente en todos los repositorios de destino y elaborar títulos y descripciones de PR significativos. Además, a menudo tienen que interactuar con herramientas externas, como Jira, para obtener o incluir referencias sobre el seguimiento de problemas. Estas tareas, si bien son necesarias, son tareas pesadas indiferenciadas que consumen un valioso tiempo de ingeniería y reducen la eficiencia general. La falta de automatización en este flujo de trabajo crea fricciones, ralentiza la entrega y aumenta la carga cognitiva de los equipos encargados de mantener las infraestructuras de Terraform a gran escala.

Descripción general de la solución

Para hacer frente a este desafío, este patrón ofrece una utilidad totalmente basada en la configuración, que permite a los usuarios definir los cambios que desean en un archivo de configuración estructurado. Este archivo especifica los repositorios, módulos, parámetros y valores de destino mediante un esquema claramente definido.

Una vez configurada, la utilidad realiza los siguientes pasos automatizados:

1. Lee la configuración definida por el usuario para determinar el alcance y la naturaleza de los cambios.

2. Crea una nueva ramificación en cada repositorio de destino a la que se aplican las actualizaciones necesarias.
3. Genera una PR para cada cambio, lo que garantiza la coherencia en todos los repositorios.
4. Envía notificaciones de Slack (opcional) para alertar a las partes interesadas con enlaces directos a la creada PRs

Al automatizar estas tareas repetitivas, la empresa de servicios reduce considerablemente el tiempo, el esfuerzo y el riesgo asociados a la gestión de actualizaciones de infraestructura a gran escala. Permite a los equipos centrarse en tareas de ingeniería de mayor valor y, al mismo tiempo, ayuda a garantizar que los cambios se apliquen de forma coherente y se puedan rastrear en todos los repositorios.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.
- Python versión 3.8 o posterior.
- Un token de acceso GitHub personal (PAT). Para obtener más información, consulte Creación de un token de acceso personal (clásico) en la GitHub documentación.
- El GitHub PAT puede acceder a los repositorios de destino para que la utilidad pueda realizar operaciones como la creación de sucursales y solicitudes de extracción de información. Para obtener más información, consulta el repositorio de GitHub códigos de este patrón.

Limitaciones

- La complejidad de la configuración presenta el principal desafío. La eficacia de la automatización está limitada por las capacidades de su archivo de configuración. Si bien el sistema gestiona los cambios estándar de manera eficiente, las modificaciones complejas de la infraestructura pueden requerir una intervención manual y algunos casos de la periferia quedan fuera del alcance de la gestión automatizada.
- La seguridad y el acceso presentan consideraciones importantes, especialmente a la hora de gestionar los tokens de GitHub acceso y los límites de velocidad de las API. Las organizaciones deben equilibrar cuidadosamente la necesidad de automatización con el almacenamiento y la administración seguros de credenciales, garantizando los controles de acceso adecuados y manteniendo la eficiencia operativa.

- Las restricciones de validación representan otra limitación notable porque el sistema automatizado tiene una capacidad limitada para validar la lógica empresarial y los requisitos específicos del entorno. Las dependencias complejas y las interacciones entre servicios suelen requerir la supervisión humana, ya que la validación automatizada no puede captar plenamente todos los matices contextuales y las reglas empresariales.
- Los problemas de escalabilidad y rendimiento surgen cuando se trata de cambios de infraestructura a gran escala. El sistema debe funcionar dentro de los límites de la GitHub API y, al mismo tiempo, gestionar numerosos repositorios simultáneamente. Las operaciones que consumen muchos recursos en una infraestructura extensa pueden crear cuellos de botella en el rendimiento que requieren una administración cuidadosa.
- Los límites de integración restringen la flexibilidad del sistema porque está diseñado principalmente para funcionar con herramientas específicas, como GitHub Slack. Es posible que las organizaciones que utilizan diferentes herramientas necesiten soluciones personalizadas y las opciones de personalización del flujo de trabajo de este patrón se limitan a los puntos de integración compatibles.

Arquitectura

En el siguiente diagrama se muestran el flujo de trabajo y los componentes de esta solución.

El flujo de trabajo consta de los pasos siguientes:

1. El desarrollador activa GitHub las acciones especificando el repositorio de Terraform.
2. La utilidad de automatización lee las configuraciones definidas.
3. La utilidad de automatización también extrae el repositorio de Terraform proporcionado.
4. La utilidad de automatización crea una nueva ramificación y actualiza las plantillas de Terraform de forma local.
5. La utilidad de automatización envía la nueva ramificación al repositorio y crea una nueva PR.
6. La utilidad de automatización utiliza notificaciones de Slack que incluyen enlaces de relaciones públicas para notificar a los desarrolladores y permite el despliegue de plantillas de Terraform. Nube de AWS

Tools (Herramientas)

- GitHubes una plataforma para desarrolladores que los desarrolladores pueden usar para crear, almacenar, administrar y compartir su código.
- GitHub Actions es una plataforma de integración y entrega continuas (CI/CD) que está estrechamente integrada con GitHub los repositorios. Puedes usar GitHub Actions para automatizar tu proceso de creación, prueba e implementación.
- HashiCorp Terraform es una herramienta de infraestructura como código (IaC) que te ayuda a crear y administrar recursos locales y en la nube.
- Slack, una oferta de Salesforce, es una plataforma conversacional basada en inteligencia artificial que permite la colaboración por chat y video, automatiza los procesos sin código y permite compartir información.

Repositorio de código

El código de este patrón está disponible en el flujo de trabajo GitHub automatizado de actualización de la infraestructura de Terraform mediante el repositorio Actions. GitHub

Prácticas recomendadas

- La gestión eficaz de los cambios es crucial para una implementación correcta. Las organizaciones deben adoptar una estrategia de despliegue gradual para los cambios a gran escala. Mantenga las convenciones de nomenclatura de las ramificaciones y las descripciones de PR coherentes y garantice una documentación exhaustiva de todos los cambios.
- Los controles de seguridad deben implementarse rigurosamente, centrándose en los principios de acceso con privilegios mínimos y en la gestión segura de las credenciales. Habilite las reglas de protección de las ramificaciones para evitar cambios no autorizados. Realice auditorías de seguridad periódicas para mantener la integridad del sistema.
- Un protocolo de prueba sólido debe incluir la ejecución de `terraform plan` automatizada en canalizaciones de integración e implementación continuas (CI/CD). El protocolo también debe incluir comprobaciones de validación previas a la confirmación y entornos de revisión específicos para los cambios críticos. Este enfoque de pruebas de varios niveles ayuda a detectar los problemas de forma temprana y garantiza la estabilidad de la infraestructura.
- La estrategia de monitoreo debe incluir mecanismos de alerta integrales, un seguimiento detallado de success/failure las métricas y mecanismos de reintento automatizados en caso de operaciones

fallidas. Esta estrategia ayuda a garantizar la visibilidad operativa y permite responder rápidamente a cualquier problema que surja.

- Los estándares de configuración deben hacer hincapié en el control de versiones de todas las configuraciones, manteniendo la modularidad para facilitar la reutilización y la escalabilidad. La documentación clara del esquema y los ejemplos ayudan a los equipos a comprender y utilizar el sistema de automatización de forma eficaz.

Epics

Instalación y configuración

Tarea	Descripción	Habilidades requeridas

Configure el repositorio.	Para clonar el repositor io, ejecute los siguientes comandos:
	`# Clone the automation tool repository`
	`git clone https://github.com/aws-samples/sample-terraform-pr-automation-utility`
	`cd sample-terraform-pr-automation-utility`
	
	`# Copy example configuration`
	`cp config.example.yaml config.yaml`
		AWS DevOps

Instale las dependencias.	Para instalar y verificar las dependencias de Python, ejecute los siguientes comandos: `# Install Python dependencies`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`pip3 install -r requirements.txt`
	
	`# Verify installation`
	`python3 -c "import github; import hcl2; import yaml; import requests; print('All packages installed successfully')"`	

Configure el GitHub token.	Para configurar el GitHub token y, a continuación, comprobar que funciona, ejecute los siguientes comandos:
	
	`# Set GitHub token environment variable`
	`export GITHUB_TOKEN="your_github_token_here"`
	
	`# Verify token works`
	`curl -H "Authorization: token $GITHUB_TOKEN" https://api.github.com/user`
		AWS DevOps

Configuración del archivo de configuración para los cambios de Terraform

Tarea	Descripción	Habilidades requeridas
Configure el archivo `config.yaml` .	Para definir los repositorios de destino y los cambios deseados, edite el archivo	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`config.yaml` de la siguiente manera:
	
	`repositories:`
	`  - owner: "your-org"`
	`  repo: "your-terraform-repo"`
	`  files:`
	`  - path: "variables.tf"`
	`  changes:`
	`  variables:`
	`  - app_version:`
	`  default:`
	
	`update:`
	`  -`
	`from: ["1.0.0"]`
	
	`to: "1.1.0"`
	
	`settings:`
	`  pr_title_template: "Infrastructure Update - {{timestamp}}"`
	`  slack:`
	`  username: "Terraform Bot"`
	`  icon_emoji: ":terraform:"`
	`  notify_on_success: true`
	`  notify_on_error: true`
	`  notify_batch_summary: true`	

Prueba y validación

Tarea	Descripción	Habilidades requeridas

Realice las pruebas previas al vuelo.	Pruebe siempre la configuración antes de ejecutarla en los repositorios de producción. Utilice los siguientes comandos:
	`# 1. Test configuration syntax`
	`python3 -c "from main import get_config_content; get_config_content()"`
	`# 2. Run in dry-run mode first`
	`DRY_RUN=true python3 main.py`
	`# 3. Test with minimal configuration`
	`# Use a simple config.yaml with just one repository and one change`
		AWS DevOps

Verifique el acceso al repositorio.	Para comprobar que el GitHub token puede acceder al repositorio, ejecute el siguiente comando:
	`# Test GitHub token access`
	`curl -H "Authorization: token $GITHUB_TOKEN" \`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`  https://api.github.com/repos/owner/repo-name`
	
	`# Should return repository information, not 404`	

Ejecución de la utilidad de automatización

Tarea	Descripción	Habilidades requeridas
Ejecute la utilidad de automatización mediante la interfaz de usuario de GitHub Actions.	Para ejecutar la utilidad de automatización mediante la interfaz de usuario de GitHub Actions, haga lo siguiente: 1. Navegue hasta su repositorio en GitHub. 2. Seleccione la pestaña Acciones. 3. Elija el flujo de trabajo de automatización de la actualización de la infraestructura de Terraform. 4. Seleccione Ejecutar flujo de trabajo. 5. Configure las siguientes entradas del flujo de trabajo: • Configuración del origen: • Seleccione la ramificación de destino para la automatización.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• Especifique la ruta al archivo de configura ción (`config.ya ml `) que contiene los cambios deseados. • Controles de vista previa: • Seleccione la opción Vista previa para revisar los cambios sin aplicarlos. • Administración de las ramificaciones: • Introduzca la ramificac ión base para crear nuevas ramificaciones de características. • Introduzca la configura ción del prefijo de la ramificación. • Seleccione la casilla Cerrar automátic amente las solicitudes de extracción obsoletas . • Configuración de las notificaciones: • Introduzca la URL del webhook de Slack para recibir notificaciones enriquecidas (anula el secreto del repositorio). • Seleccione la casilla Probar la integraci	

Tarea	Descripción	Habilidades requeridas
	ón de Slack antes de procesarla (solo en ejecución de prueba). • Introduzca su informaci ón para anular el canal de Slack predeterm inado (por ejemplo, #infrastructure-test). • Configuración avanzada: • Seleccione la casilla Habilitar el registro de depuración para la solución de problemas.	

(Alternativa) Ejecute la utilidad de automatización desde la línea de comandos.	Si lo prefiere, puede ejecutar la utilidad de automatización desde la línea de comandos en lugar de utilizar la interfaz de usuario de GitHub Actions. Utilice el siguiente comando :
	`# Run actual automation`
	`python3 main.py`
		AWS DevOps

Validación PRs y cambios

Tarea	Descripción	Habilidades requeridas
Revise lo creado PRs y los cambios.	Para supervisar los resultado s de la ejecución del GitHub flujo de trabajo, haga lo siguiente:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• Compruebe el estado del procesamiento en los registros de ejecución del flujo de trabajo. • Revise lo PRs que creó la utilidad de automatización. • Supervise las notificaciones de Slack (si están configura das).	

Limpieza

Tarea	Descripción	Habilidades requeridas
(Opcional) Limpiar PRs.	Cerrar abandonada o innecesaria PRs.	AWS DevOps

Recursos relacionados

AWS Guía prescriptiva

- Uso de Terraform como una herramienta de IaC para Nube de AWS

GitHub documentación

- Acerca de las solicitudes de extracción
- Administración de los tokens de acceso personal
- Comprensión de GitHub las acciones
- Guía de inicio rápido para las acciones GitHub

Crear automáticamente canalizaciones de CI dinámicas para proyectos de Java y Python

Aromal Raj Jayarajan, Vijesh Vijayakumaran Nair, MAHESH RAGHUNANDANAN y Amarnath Reddy, Amazon Web Services

Resumen

Este patrón muestra cómo crear automáticamente canalizaciones de integración continua (CI) dinámicas para proyectos de Java y Python mediante las herramientas para desarrolladores de AWS.

A medida que las pilas de tecnología se diversifican y las actividades de desarrollo aumentan, puede resultar difícil crear y mantener canalizaciones de CI que sean coherentes en toda la organización. Al automatizar el proceso en AWS Step Functions, puede asegurarse de que sus canalizaciones de CI sean coherentes en su uso y enfoque.

Para automatizar la creación de canalizaciones de CI dinámicas, este patrón utiliza las siguientes entradas variables:

- Lenguaje de programación (solo Java o Python)
- Nombre de canalización
- Etapas de canalización requeridas

> **Note**
>
> Step Functions orquestra la creación de canalizaciones mediante varios servicios de AWS. Para obtener más información sobre los servicios de AWS que se utilizan en esta solución, consulte la sección Herramientas de este patrón.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un bucket de Amazon S3 en la misma región de AWS en la que se está implementando esta solución

- Un director de AWS Identity and Access Management (IAM) que cuente con los CloudFormation permisos de AWS necesarios para crear los recursos necesarios para esta solución

Limitaciones

- Este patrón solo admite proyectos de Java y Python.
- Los roles de IAM aprovisionadas en este patrón siguen el principio del privilegio mínimo. Los permisos de los roles de IAM deben actualizarse en función de los recursos específicos que necesite crear su canalización de CI.

Arquitectura

Pila de tecnología de destino

- AWS CloudFormation
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- IAM
- Amazon Simple Storage Service (Amazon S3)
- AWS Systems Manager
- AWS Step Functions
- AWS Lambda
- Amazon DynamoDB

Arquitectura de destino

El siguiente diagrama muestra un ejemplo de flujo de trabajo para crear automáticamente canalizaciones de CI dinámicas para proyectos de Java y Python mediante las herramientas para desarrolladores de AWS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario de AWS proporciona los parámetros de entrada para la creación de canalizaciones de CI en formato JSON. Esta entrada inicia un flujo de trabajo de Step Functions (máquina de

estados) que crea una canalización de CI mediante las herramientas para desarrolladores de AWS.

2. Una función de Lambda lee una carpeta denominada input-reference, que está almacenada en un bucket de Amazon S3 y, a continuación, genera un archivo buildspec.yml. Este archivo generado define las etapas de la canalización de CI y se vuelve a almacenar en el mismo bucket de Amazon S3 que almacena las referencias de los parámetros.
3. Step Functions comprueba las dependencias del flujo de trabajo de creación de canalizaciones de CI para detectar cualquier cambio y actualiza la pila de dependencias según sea necesario.
4. Step Functions crea los recursos de la canalización de CI en una CloudFormation pila, que incluye un CodeCommit repositorio, un CodeBuild proyecto y una CodePipeline canalización.
5. La CloudFormation pila copia el código fuente de muestra de la pila de tecnología seleccionada (Java o Python) y el archivo buildspec.yml en el repositorio. CodeCommit
6. Los detalles del tiempo de ejecución de la canalización de CI se almacenan en una tabla de DynamoDB.

Automatizar y escalar

- Este patrón se utiliza únicamente en un entorno de desarrollo único. Se requieren cambios de configuración para su uso en varios entornos de desarrollo.
- Para añadir compatibilidad con más de una CloudFormation pila, puedes crear plantillas adicionales. CloudFormation Para obtener más información, consulte Introducción a AWS CloudFormation en la CloudFormation documentación.

Tools (Herramientas)

Herramientas

- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de Lambda AWS y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS le CodePipeline ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- El Almacén de parámetros de AWS Systems Manager proporciona un almacenamiento seguro y jerárquico para administrar los datos de configuración y los secretos.

Código

El código de este patrón está disponible en el GitHub automated-ci-pipeline-creationrepositorio. El repositorio contiene las CloudFormation plantillas necesarias para crear la arquitectura de destino descrita en este patrón.

Prácticas recomendadas

- No introduzcas credenciales (secretos), como identificadores o contraseñas, directamente en las CloudFormation plantillas o en las configuraciones de acciones de Step Functions. Si lo hace, la información se mostrará en los registros de DynamoDB. En su lugar, utilice AWS Secrets Manager para configurar y almacenar secretos. A continuación, consulte los secretos almacenados en Secrets Manager dentro de las CloudFormation plantillas y las configuraciones de acciones de Step Functions, según sea necesario. Para obtener más información, consulte ¿Qué es AWS Secrets Manager? en la documentación de AWS Secrets Manager.

- Configure el cifrado del lado del servidor para los CodePipeline artefactos almacenados en Amazon S3. Para obtener más información, consulte Configurar el cifrado del lado del servidor para los artefactos almacenados en Amazon S3 CodePipeline en la CodePipeline documentación.
- Aplique permisos de privilegios mínimos al configurar roles de IAM. Para obtener más información, consulte Aplicar permisos de privilegio mínimo en la documentación de IAM.
- Asegúrese de que su bucket de Amazon S3 no sea de acceso público. Para obtener más información, consulte Configurar la configuración de bloqueo de acceso público para sus buckets de S3 en la documentación de Amazon S3.
- Asegúrese de activar el control de versiones de su bucket de Amazon S3. Para más información, consulte Uso de control de versiones en buckets de S3 en la documentación de Amazon S3.
- Utilice IAM Access Analyzer al configurar las políticas de IAM. La herramienta proporciona recomendaciones prácticas para ayudarle a crear políticas de IAM seguras y funcionales. Para más información, consulte Utilizar el analizador de acceso de AWS Identity and Access Management en la documentación de IAM.
- Cuando sea posible, defina condiciones de acceso específicas al configurar las políticas de IAM.
- Activa el CloudWatch registro de Amazon con fines de supervisión y auditoría. Para obtener más información, consulta ¿Qué es Amazon CloudWatch Logs? en la CloudWatch documentación.

Epics

Configurar los requisitos previos

Tarea	Descripción	Habilidades requeridas
Crear un bucket de Amazon S3.	Cree un depósito de Amazon S3 (o utilice uno existente) para almacenar las CloudFormation plantillas, el código fuente y los archivos de entrada necesarios para la solución. Para obtener más informaci ón, consulte Paso 1: Crear su primer bucket de S3 en la	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	documentación de Amazon S3. **Note** El bucket de Amazon S3 debe estar en la misma región de AWS en la que está implementando la solución.	
Clona el GitHub repositorio.	Clone el GitHub automated-ci-pipeline-creationrepositorio ejecutando el siguiente comando en una ventana de terminal: `git clone https://github.com/aws-samples/automated-ci-pipeline-creation.git` Para obtener más información, consulte Clonación de un repositorio en la GitHub documentación.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Cargue la carpeta Solution Templates del GitHub repositorio clonado a su bucket de Amazon S3.	Copie el contenido de la carpeta Solution-Templates clonada y cárguelo en el bucket de Amazon S3 que creó. Para obtener más información, consulte Carga de objetos en la documentación de Amazon S3. **Note** Asegúrese de cargar únicament e el contenido de la carpeta Solution-Templates. Puede cargar los archivos únicamente en el nivel raíz del bucket de Amazon S3.	AWS DevOps

Implementar la solución

Tarea	Descripción	Habilidades requeridas
Cree una CloudFormation pila para implementar la solución mediante el archivo template. yml del repositorio clonado. GitHub	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la CloudFormation consola de AWS.	Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	2. Seleccione Creación de pila. Se muestra una lista desplegable. 3. En la lista desplegable, seleccione Con nuevos recursos (standard). Se abre la página Crear pila. 4. En la sección Especificar plantilla elija casilla allado de Cargar un archivo de plantilla. 5. Seleccione Choose file (Elegir archivo). A continuación, vaya a la carpeta raíz del GitHub repositorio clonado y seleccione el archivo template.yml. A continuación, seleccione Abrir. 6. Elija Siguiente. Se abrirá la página Especificar los detalles de la pila. 7. En la sección Parámetros, especifique los siguientes parámetros: • Para S3 TemplateBucketName, introduzca el nombre del bucket de Amazon S3 que creó anteriormente, que contiene el código fuente y las referencias de esta solución. Asegúrese de que el parámetro de	

Tarea	Descripción	Habilidades requeridas
	nombre de bucket esté en minúsculas. • Para Dynamo DBTable, introduzca un nombre para la tabla de DynamoDB que crea la pila. CloudFormation • Para StateMachineName, introduzca un nombre para la máquina de estados Step Functions que crea la CloudForm ation pila. 8. Elija Siguiente. Se abre la página Configurar opciones de pilas. 9. En la página Configura r opciones de pila, elija Siguiente. No cambie ninguno de los valores predeterminados. Se abre la página de Revisión. 10. Revise la configuración de creación de la pila. A continuación, seleccione Crear pila para lanzar su pila. **Note** Mientras se está creando la pila, aparecerá en la	

Tarea	Descripción	Habilidades requeridas
	página Pilas con un estado CREATE_IN _PROGRESS. Asegúrese de esperar a que el estado de la pila cambie a CREATE_COMPLETE antes de completar los pasos restantes de este patrón.	

Prueba de la configuración

Tarea	Descripción	Habilidades requeridas
Ejecute la función que ha creado.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la consola Step Functions. 2. Abra la función escalonada que ha creado. 3. Seleccione Iniciar ejecución . A continuación, introduzc a los valores de entrada para el flujo de trabajo en formato JSON (consulte los siguientes ejemplos de entradas). 4. Seleccione Iniciar ejecución . Formato JSON	Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas

	<pre>{
	  "details": {
	    "tech_stack":
	 "Name of the Tech Stack
	 (python/java)",
	    "project_name":
	 "Name of the Project
	 that you want to create
	 with",
	    "pre_build":
	 "Choose the step if
	 it required in the
	 buildspec.yml file
	 i.e., yes/no",
	    "build": "Choose the
	 step if it required in
	 the buildspec.yml file
	 i.e., yes/no",
	    "post_build":
	 "Choose the step if
	 it required in the
	 buildspec.yml file
	 i.e., yes/no",
	    "reports": "Choose
	 the step if it required
	 in the buildspec.yml
	 file i.e., yes/no",
	  }
	}</pre> Ejemplo de entrada JSON en Java <pre>{
	  "details": {
	    "tech_stack":
	 "java",
	    "project_name":
	 "pipeline-java-pjt",
	    "pre_build": "yes",</pre>	

Tarea	Descripción	Habilidades requeridas

	<pre> "build": "yes",
	    "post_build":
	 "yes",
	    "reports": "yes"
	  }
	}</pre>
	Ejemplo de entrada JSON en Python
	
	<pre>{
	  "details": {
	    "tech_stack":
	 "python",
	    "project_name":
	 "pipeline-python-p
	jt",
	    "pre_build": "yes",
	    "build": "yes",
	    "post_build":
	 "yes",
	    "reports": "yes"
	  }
	}</pre>	

Tarea	Descripción	Habilidades requeridas
Confirme que se creó el CodeCommit repositorio para la canalización de CI.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la CodeCommit consola. 2. En la página Repositorios, compruebe que el nombre del CodeCommit repositor io que ha creado aparece en la lista de repositorios. Al nombre del repositorio se le añade lo siguiente: -Repo pipeline-java-pjt 3. Abre el CodeCommit repositorio y comprueba que el código fuente del ejemplo junto con los archivos buildspec.yml se hayan enviado a la rama principal.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Consulte los recursos CodeBuild del proyecto.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la CodeBuild consola. 2. En la página Crear proyectos, compruebe que el nombre del CodeBuild proyecto que ha creado aparece en la lista de proyectos. Al nombre del proyecto se le añade lo siguiente: pipeline-java-pjt - Build 3. Seleccione el nombre de su CodeBuild proyecto para abrirlo. A continuación, revise y valide las siguiente s configuraciones: • Configuración del proyecto • Origen • Entorno • Buildspec • Configuración por lotes • Artefactos	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Valide las CodePipeline etapas.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la CodePipeline consola. 2. En la página Canalizaciones, verifique que el nombre de la canalización que ha creado aparece en la lista de canalizaciones. Al nombre de la canalización se le añade lo siguiente: pipeline-java-pjt -Pipeline 3. Seleccione el nombre de su canalización para abrir la canalización. A continuación, revise y valide cada etapa de la canalización, incluyendo la Confirmación y la Implementación.	AWS DevOps
Confirme que la canalización de CI se haya ejecutado correctamente.	1. En la CodePipeline consola, en la página Pipelines, seleccione el nombre de la canalización para ver el estado de la canalización. 2. Verifique que cada etapa de la canalización tenga el estado de Logrado.	AWS DevOps

Eliminación de sus recursos

Tarea	Descripción	Habilidades requeridas
Elimine la pila de recursos CloudFormation.	Elimine la pila de recursos de la canalización de CI CloudFormation. Para obtener más información, consulte Eliminar una pila en la CloudFormation consola de AWS en la CloudFormation documentación. **Note** Asegúrese de eliminar la pila denominada <project_name>-stack.	AWS DevOps
Elimine las dependencias de la canalización de CI en Amazon S3 y CloudFormation.	1. Vacíe el depósito de Amazon S3 denominado DeploymentArtifactBucket. Para más información, consulte Vaciar un bucket en la documentación de Amazon S3. 2. Elimine la pila de dependencias de la canalización de CI CloudFormation. Para obtener más información, consulte Eliminar una pila en la CloudFormation consola de AWS en la CloudFormation documentación.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Note Asegúrese de eliminar la pila nombrada pipeline-creation-dependencies-stack.	
Elimine el bucket de plantilla de Amazon S3.	Elimine el bucket de Amazon s3 que creó en la sección Configurar los requisitos previos de este patrón, que almacena las plantillas de esta solución. Para obtener más informaci ón, consulte Eliminación de un bucket en la documentación de Amazon S3.	AWS DevOps

Recursos relacionados

- Creación de una máquina de estados de Step Functions que utilice Lambda (documentación de AWS Step Functions)
- AWS Step Functions WorkFlow Studio (documentación de AWS Step Functions)
- DevOps y AWS
- ¿Cómo CloudFormation funciona AWS? (CloudFormation documentación de AWS)
- Completo CI/CD con AWS CodeCommit, AWS CodeBuild CodeDeploy, AWS y AWS CodePipeline (entrada del blog de AWS)
- Cuotas, requisitos de nombre y límites de caracteres de IAM y AWS STS (documentación de IAM)

Despliega canarios de CloudWatch Synthetics con Terraform

Dhrubajyoti Mukherjee y Jean-Francois Landreau, Amazon Web Services

Resumen

Es importante validar el estado de un sistema desde la perspectiva del cliente y confirmar que los clientes pueden conectarse. Esto resulta más difícil cuando los clientes no llaman constantemente al punto de conexión. Amazon CloudWatch Synthetics admite la creación de canarios, que pueden probar puntos de conexión públicos y privados. Al usar valores controlados, puede conocer el estado de un sistema incluso si no está en uso. Estos valores controlados son scripts de Node.js Puppeteer o scripts de Python Selenium.

Este patrón describe cómo usar HashiCorp Terraform para implementar canarios que prueben puntos de enlace privados. Incorpora un script de Puppeteer que comprueba si una URL devuelve `200-OK`. A continuación, el script de Terraform se puede integrar con el script que implementa el punto de conexión privado. También puede modificar la solución para monitorear puntos de conexión públicos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa con una nube privada virtual (VPC) y subredes privadas
- La URL del punto de conexión al que se puede acceder desde las subredes privadas
- Terraform instalado en el entorno de implementación

Limitaciones

La solución actual funciona para las siguientes versiones de tiempo de ejecución de CloudWatch Synthetics:

- syn-nodejs-puppeteer-3.4
- syn-nodejs-puppeteer-3,5
- syn-nodejs-puppeteer-3,6
- syn-nodejs-puppeteer-3,7

Cuando se publiquen nuevas versiones de tiempo de ejecución, podría tener que actualizar la solución actual. También tendrá que modificar la solución para mantenerse al día con las actualizaciones de seguridad.

Versiones de producto

- Terraform 1.3.0

Arquitectura

Amazon CloudWatch Synthetics se basa en CloudWatch Lambda y Amazon Simple Storage Service (Amazon S3). Amazon CloudWatch ofrece un asistente para crear los canarios y un panel de control que muestra el estado de los canarios. La función de Lambda ejecuta el script. Amazon S3 almacena los registros y las capturas de pantalla de las ejecuciones de valores controlados.

Este patrón simula un punto final privado a través de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) implementada en las subredes de destino. La función de Lambda requiere interfaces de red elásticas en la VPC en la que se implementa el punto de conexión privado.

En el diagrama se muestra lo siguiente:

1. El valor controlado de Synthetics inicia la función de Lambda del valor controlado.
2. La función de Lambda del valor controlado se conecta a la interfaz de red elástica.
3. La función de Lambda del valor controlado monitorea el estado del punto de conexión.
4. Synthetics Canary envía los datos de ejecución al bucket y las métricas del S3. CloudWatch
5. Se inicia una CloudWatch alarma en función de las métricas.
6. La CloudWatch alarma inicia el tema Amazon Simple Notification Service (Amazon SNS).

Tools (Herramientas)

Servicios de AWS

- Amazon le CloudWatch ayuda a monitorizar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la

capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS. Este patrón utiliza puntos de conexión de VPC e interfaces de red elásticas.

Otros servicios

- HashiCorp Terraform es una herramienta de código abierto de infraestructura como código (IaC) que le ayuda a usar el código para aprovisionar y administrar la infraestructura y los recursos de la nube. Este patrón utiliza Terraform para implementar la infraestructura.
- Puppeteer es una biblioteca de Node.js. El motor de ejecución CloudWatch Synthetics utiliza el marco Puppeteer.

Código

La solución está disponible en el repositorio en la nube. GitHub watch-synthetics-canary-terraform
Para obtener más información, consulte la sección Información adicional.

Epics

Implementar la solución para monitorear una URL privada

Tarea	Descripción	Habilidades requeridas
Reunir los requisitos para monitorear la URL privada.	Reúna la definición completa de la URL: dominio, parámetros y encabezados. Para comunicarse de forma privada con Amazon S3 y Amazon	Arquitecto de la nube, administrador de redes

Tarea	Descripción	Habilidades requeridas
	CloudWatch, utilice puntos de enlace de VPC. Observe cómo se puede acceder a la VPC y a las subredes desde el punto de conexión. Tenga en cuenta la frecuencia de las ejecuciones de valores controlados.	

Tarea	Descripción	Habilidades requeridas
Modifique la solución existente para monitorear la URL privada.	Modifique el archivo `terraform.tfvars` : • `name`: el nombre de su valor controlado. • `runtime_version` : la versión de tiempo de ejecución del valor controlado. Recomendamos usar syn-nodejs-puppeteer -3.7. • `take_screenshot` : si se debe hacer una captura de pantalla. • `api_hostname` : el nombre de host del punto de conexión que se monitorea. • `api_path`: la ruta del punto de conexión que se monitorea. • `vpc_id`: la ID de la VPC que utiliza la función de Lambda del valor controlado. • `subnet_ids` — La subred IDs que utiliza la función Lambda canaria. • `frequency` : la frecuencia de ejecución del valor controlado en minutos. • `alert_sns_topic` — El tema de SNS al que	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	se envía la notificación CloudWatch de alarma.	

Implementar y utilizar la solución.	Para implementar la solución, haga lo siguiente:
	1. Inicialice Terraform desde el directorio `cloudwatch-synthetics-canary-terraform` de su entorno de desarrollo.
	`terraform init`
	2. Planifique y revise los cambios.
	`terraform plan`
	3. Implemente la solución.
	`terraform apply`
		Arquitecto de nube, ingeniero DevOps

Resolución de problemas

Problema	Solución
La eliminación de los recursos aprovisionados se bloquea.	Elimine manualmente la función de Lambda del valor controlado, la interfaz de red elástica correspondiente y el grupo de seguridad, en ese orden.

Recursos relacionados

- Uso del monitoreo sintético

- Supervise los puntos de enlace de API Gateway con Amazon CloudWatch Synthetics (entrada del blog)

Información adicional

Artefactos del repositorio

Los artefactos del repositorio tienen la siguiente estructura.

```
.
### README.md
### main.tf
### modules
#   ### canary
#   ### canary-infra
### terraform.tfvars
### tf.plan
### variable.tf
```

El archivo `main.tf` contiene el módulo principal e implementa dos módulos secundarios:

- `canary-infra` implementa la infraestructura necesaria para los valores controlados.
- `canary` implementa los valores controlados.

Los parámetros de entrada de la solución se encuentran en el archivo `terraform.tfvars`. Puede utilizar el siguiente código de ejemplo para crear un valor controlado.

```
module "canary" {
    source = "./modules/canary"
    name   = var.name
    runtime_version = var.runtime_version
    take_screenshot = var.take_screenshot
    api_hostname = var.api_hostname
    api_path = var.api_path
    reports-bucket = module.canary_infra.reports-bucket
    role = module.canary_infra.role
    security_group_id = module.canary_infra.security_group_id
    subnet_ids = var.subnet_ids
    frequency = var.frequency
    alert_sns_topic = var.alert_sns_topic
```

```
}
```

A continuación, se muestra el archivo .var correspondiente.

```
name   = "my-canary"
runtime_version = "syn-nodejs-puppeteer-3.7"
take_screenshot = false
api_hostname = "mydomain.internal"
api_path = "/path?param=value"
vpc_id = "vpc_id"
subnet_ids = ["subnet_id1"]
frequency = 5
alert_sns_topic = "arn:aws:sns:eu-central-1:111111111111:yyyyy"
```

Limpieza de la solución

Si está haciendo las pruebas en un entorno de desarrollo, puede limpiar la solución para evitar acumular costos.

1. En la consola de administración de AWS, vaya a la consola de Amazon S3. Vacíe el bucket de Amazon S3 creado por la solución. Asegúrese de realizar una copia de seguridad de los datos en caso necesario.
2. En su entorno de desarrollo, ejecute el comando `destroy` desde el directorio `cloudwatch-synthetics-canary-terraform`.

   ```
   terraform destroy
   ```

Implemente una ChatOps solución para gestionar los resultados de los escaneos SAST mediante Amazon Q Developer en aplicaciones de chat, acciones personalizadas y CloudFormation

Anand Bukkapatnam Tirumala, Amazon Web Services

Resumen

Este patrón presenta una solución integral que utiliza Amazon Q Developer en las aplicaciones de chat para agilizar la gestión de los errores de análisis de las pruebas de seguridad de aplicaciones estáticas (SAST) notificados mediante SonarQube las pruebas de seguridad de aplicaciones (SAST). Este enfoque innovador integra acciones y notificaciones personalizadas en una interfaz conversacional, lo que permite una colaboración eficiente y procesos de toma de decisiones dentro de los equipos de desarrollo.

En el vertiginoso entorno de desarrollo de software actual, la gestión eficiente de los resultados del análisis de SAST es crucial para mantener la calidad y la seguridad del código. Sin embargo, muchas organizaciones se enfrentan a los siguientes desafíos importantes:

- Retraso en el conocimiento de las vulnerabilidades críticas debido a la ineficiencia de los sistemas de notificación
- Procesos de toma de decisiones lentos debido a flujos de trabajo de aprobación desconectados
- Falta de respuestas inmediatas y procesables a los fallos del análisis de SAST
- Comunicación y colaboración fragmentadas en torno a los resultados de seguridad
- La configuración manual de la infraestructura para las herramientas de seguridad lleva mucho tiempo y es propensa a errores

Estos problemas suelen provocar un aumento de los riesgos de seguridad, retrasos en las versiones y una reducción de la productividad del equipo. Para abordar estos desafíos de manera eficaz, se requiere una solución que pueda agilizar la gestión de los resultados de SAST, mejorar la colaboración en equipo y automatizar el aprovisionamiento de la infraestructura.

Entre las características principales de la solución se incluyen:

- Notificaciones personalizadas: las alertas y notificaciones en tiempo real se envían directamente a los canales de chat del equipo, lo que garantiza reconocimiento de las peticiones y acción en caso de vulnerabilidades o fallas en el análisis de SAST.

- Aprobaciones conversacionale: las partes interesadas pueden iniciar y completar los flujos de trabajo de aprobación de los resultados del análisis de SAST sin problemas desde la interfaz de chat, lo que acelera los procesos de toma de decisiones.
- Acciones personalizadas: los equipos pueden definir y ejecutar acciones personalizadas en función de los resultados del análisis de SAST, como desencadenar automáticamente los mensajes de correo electrónico en caso de errores en los controles de calidad y mejorar la capacidad de respuesta ante los problemas de seguridad.
- Colaboración centralizada: todas las discusiones, decisiones y acciones relacionadas con el análisis de SAST se guardan en un entorno de chat unificado, lo que fomenta una mejor colaboración y el intercambio de conocimientos entre los miembros del equipo.
- Infraestructura como código (IaC): toda la solución incluye AWS CloudFormation plantillas, lo que permite un aprovisionamiento de infraestructura más rápido y fiable y, al mismo tiempo, reduce los errores de configuración manual.

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- Un rol AWS Identity and Access Management (de IAM) con permisos para crear y administrar los recursos asociados a los que Servicios de AWS se enumeran en Herramientas.
- Un espacio de trabajo de Slack.
- Amazon Q Developer en aplicaciones de chat agregadas al espacio de trabajo de Slack requerido como complemento. Para obtener más información, consulte Cómo añadir aplicaciones a tu espacio de trabajo de Slack en la documentación de Slack. Toma nota del ID del espacio de trabajo de Slack tal y como aparece en el formulario Consola de administración de AWS después de registrarte correctamente.
- Un cliente configurado de Amazon Q Developer en aplicaciones de chat, con el ID del espacio de trabajo disponible para introducirlo en la CloudFormation consola. Para obtener instrucciones, consulte Configure a Slack client (Cómo configurar un cliente de Slack) en la Guía del administrador de aplicaciones de chat para Amazon Q Developer.
- Una cuenta de correo electrónico de origen que se crea y verifica en Amazon Simple Email Service (Amazon SES) para enviar mensajes de correo electrónico de aprobación. Para obtener instrucciones de configuración, consulte Creación y verificación de identidades de correo electrónico en la Guía para desarrolladores de Amazon Simple Email Service.

- Una dirección de correo electrónico de destino para recibir notificaciones de aprobación. Esta dirección puede ser una bandeja de entrada compartida o una lista de distribución específica del equipo.
- Una SonarQube instancia operativa a la que se puede acceder desde su Cuenta de AWS. Para obtener más información, consulte las instrucciones SonarQube de instalación.
- Un token SonarQube de usuario con permisos para activar y crear proyectos a través de la canalización.

Limitaciones

- La creación de botones de acción personalizados es un proceso manual en esta solución.
- Algunos Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

En el siguiente diagrama se muestran los componentes de la arquitectura y el flujo de trabajo de esta aplicación.

En el diagrama, se muestra el flujo de trabajo automatizado de control de calidad del código:

1. Preparación y carga del código:
   - El desarrollador comprime el código base en un archivo .zip.
   - El desarrollador carga manualmente el archivo .zip en un bucket designado de Amazon Simple Storage Service (Amazon S3).
2. AWS Step Functions Activación y organización de eventos de Amazon S3:
   - El evento de carga de Amazon S3 desencadena un flujo de trabajo de Step Functions.
   - Step Functions organiza un escaneo SAST utilizando. SonarQube
   - El flujo de trabajo supervisa el estado del AWS CodeBuild trabajo para determinar las siguientes acciones. Si CodeBuild tiene éxito (control de calidad), el flujo de trabajo finaliza. Si CodeBuild se produce un error, se invoca una AWS Lambda función para el diagnóstico. Para obtener más información, consulte Lógica de AWS Step Functions más adelante en esta sección.

3. AWS CodeBuild ejecución:
    - El CodeBuild trabajo ejecuta un SonarQube escaneo en la base de código cargada.
    - Los artefactos analizados se almacenan en un bucket de Amazon S3 independiente para su auditoría y análisis.
4. Análisis de errores (función de Lambda):
    - En CodeBuild caso de fallo, se `CheckBuildStatus` activa la función Lambda.
    - En CodeBuild caso de éxito, el proceso finaliza y no es necesario realizar ninguna otra acción.
5. La función de Lambda analiza la causa del error (error en el control de calidad u otros problemas)
    - La función `CheckBuildStatus` crea una carga útil personalizada con información detallada sobre el error.
    - La función `CheckBuildStatus` publica la carga útil personalizada en un tema de Amazon Simple Notification Service (Amazon SNS).
6. Sistema de notificaciones:
    - Amazon SNS reenvía la carga útil a Amazon Q Developer en aplicaciones de chat para la integración con Slack.
7. Integración de Slack:
    - Amazon Q Developer en aplicaciones de chat publica una notificación en el canal de Slack designado.
8. Proceso de aprobación:
    - Los aprobadores revisan los detalles del error en la notificación de Slack.
    - Los aprobadores pueden iniciar la aprobación mediante el botón Aprobar de Slack.
9. Controlador de aprobación:
    - Una función de Lambda de aprobación procesa la acción de aprobación desde Slack.
    - La función de aprobación publica el mensaje personalizado en Amazon SES.
10. Mensaje generado:
    - La función de aprobación genera un mensaje personalizado para la notificación al desarrollador.
11. Notificación para desarrolladores:
    - Amazon SES envía un mensaje de correo electrónico al desarrollador con los siguientes pasos o acciones necesarias.

Este flujo de trabajo combina la carga manual de códigos con controles de calidad automatizados, proporciona comentarios inmediatos a través de Slack y permite la intervención humana cuando es necesaria, lo que garantiza un proceso de revisión de código sólido y flexible.

Lógica de AWS Step Functions

Como se muestra en el diagrama de arquitectura anterior, si la transmisión de la puerta de calidad SonarQube falla, el flujo de trabajo pasa a la `CheckBuildStatus` función Lambda. La función `CheckBuildStatus` activa una notificación en el canal de Slack. Cada notificación incluye información con sugerencias sobre los próximos pasos. A continuación se muestran los tipos de notificaciones:

- La aplicación ha fallado en el escaneo de seguridad del código: el usuario recibe esta notificación cuando el código cargado no ha pasado el escaneo SonarQube de seguridad. El usuario puede elegir APROBAR para aceptar la compilación. Sin embargo, la notificación aconseja al usuario que tenga cuidado con los posibles riesgos de seguridad y de mala calidad del código. La notificación incluye la siguiente información:
  - Próximos pasos: Error: Quality gate status: FAILED: consulte los detalles en la URL proporcionada.
  - Clasifique las vulnerabilidades tal y como se menciona en el documento en la URL proporcionada.
  - CodeBuild los detalles están disponibles en la ubicación de la URL proporcionada.
- La canalización de análisis de aplicaciones ha fallado por alguna otra razón: el usuario recibe esta notificación cuando la canalización ha fallado por alguna razón distinta del error en el análisis de seguridad del código. La notificación incluye la siguiente información:
  - Para ver los siguientes pasos, visite el enlace proporcionado para obtener más información sobre la solución de problemas.

Para ver las capturas de pantalla de las notificaciones tal y como aparecen en un canal de Slack, ve a la carpeta assets del repositorio de GitHub chatops-slack.

En el siguiente diagrama se muestra un ejemplo del estado del paso de Step Functions después de que se produzca un error en el pase del control de calidad.

Tools (Herramientas)

Servicios de AWS

- Amazon Q Developer en aplicaciones de chat le permite usar los canales de chat de Amazon Chime, Microsoft Teams y Slack para monitorear y responder a los eventos operativos en sus aplicaciones. AWS Aviso de fin de soporte: el 20 de febrero de 2026, AWS finalizará el soporte para el servicio Amazon Chime. Después del 20 de febrero de 2026, ya no podrá acceder a la consola ni a los recursos de la aplicación de Amazon Chime. Para obtener más información, visite esta entrada en el blog. Esto no afecta a la disponibilidad del servicio Amazon Chime SDK.
- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y administrarlos a lo largo de su ciclo de vida en todo el país Cuentas de AWS . Regiones de AWS
- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Secrets Manager lo ayuda a reemplazar las credenciales codificadas en su código, incluidas contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- Amazon Simple Email Service (Amazon SES) facilita poder enviar y recibir mensajes de correo electrónico a través de los dominios y direcciones de correo electrónico propios.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Step Functionses un servicio de organización sin servidor que le ayuda a combinar AWS Lambda funciones y otras Servicios de AWS para crear aplicaciones críticas para la empresa.

Otras herramientas

- Slack, una oferta de Salesforce, es una plataforma conversacional basada en inteligencia artificial que permite la colaboración por chat y video, automatiza los procesos sin código y permite compartir información.
- SonarQubees una herramienta de análisis local diseñada para detectar problemas de codificación en más de 30 lenguajes, marcos y plataformas IaC.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub chatops-slack.

Prácticas recomendadas

- CloudFormation administración de la pila: si encuentra algún error durante la ejecución de la CloudFormation pila, le recomendamos que elimine la pila fallida. A continuación, vuelva a crearla con los valores de parámetros correctos. Este enfoque permite una implementación limpia y ayuda a evitar posibles conflictos o implementaciones parciales.
- Configuración de correo electrónico con bandeja de entrada compartida: al configurar el parámetro `SharedInboxEmail`, utilice una lista de distribución común a la que puedan acceder todos los desarrolladores pertinentes. Este enfoque promueve la transparencia y ayuda a que las notificaciones importantes lleguen a los miembros pertinentes del equipo.
- Flujo de trabajo de aprobación de la producción: en el caso de los entornos de producción, restrinja el acceso al canal de Slack que se utiliza para la aprobación de las compilaciones. Solo los aprobadores designados deben ser miembros de este canal. Esta práctica mantiene una cadena de responsabilidad clara y mejora la seguridad al limitar quién puede aprobar los cambios críticos.
- Permisos de IAM: siga el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Realización de la configuración inicial

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Para clonar el repositorio de chatops-slack para este	AWS DevOps, jefe de construcción, DevOps

Tarea	Descripción	Habilidades requeridas
	patrón, use el siguiente comando. `git clone "git@github.com:aws-samples/chatops-slack.git"`	ingeniero, administrador de la nube

Cree un archivo .zip que incluya el código de Lambda.	Cree los archivos.zip para el código de la AWS Lambda `ApprovalEmail` función `CheckBuildStatus` y. Para crear `notification.zip` y `approval.zip` , utilice los comandos siguientes.
	`cd chatops-slack/src`
	`chmod -R 775 *`
	`zip -r approval.zip approval`
	`zip -r notification.zip notification`
		AWS DevOps, jefe de construcción, DevOps ingeniero, administrador de la nube

Implementación del archivo de pila pre-requisite.yml

Tarea	Descripción	Habilidades requeridas
Ejecute el archivo de pila `pre-requisite.yml` .	El archivo de `pre-requisite.yml` CloudFormation pila despliega los recursos iniciales necesarios antes de ejecutar el archivo de `app-`	Administrador de AWS DevOps, jefe de construcción, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`security.yml` pila. Para ejecutar el archivo `pre-requisite.yml` , haga lo siguiente: 1. Inicie sesión en la Consola de administración de AWSCloudFormationconsola y ábrala. Elija Crear pila, y, a continuación, elija Con nuevos recursos (estándar) en la lista desplegable. 2. En la página Crear pila, seleccione Elegir una plantilla existente y Cargar un archivo de plantilla. A continuación, seleccione Elegir archivo y seleccione pre-requisite.yml. Elija Siguiente. 3. En la página Especificar los detalles de la pila, introduzca los valores de los parámetros tal y como se describe en Información adicional. A continuación, elija Siguiente. 4. En la página Configurar las opciones de pila, elija el rol de IAM para crear los recursos, tal y como se describe en Requisito	

Tarea	Descripción	Habilidades requeridas
	s previos. A continuación, elija Siguiente. 5. En la página Revisar y crear, elija Enviar. 6. En la página de detalles de la pila, seleccione las pestañas Recursos y Salidas. Anote los valores de los parámetros `S3Lambda`, `CKMSKeyArn` y `CKMSKeyId` que se utilizan en los pasos siguientes.	
Cargue los archivos .zip en el bucket de Amazon S3.	Cargue los archivos `notification.zip` y `approval.zip` que creó anteriormente en el bucket de Amazon S3 denominado `S3LambdaBucket`. El archivo de `app-security.yml` CloudFormation pila se utiliza `S3LambdaBucket` para aprovisionar la función Lambda.	AWS DevOps, jefe de construcción, DevOps ingeniero, administrador de sistemas de AWS

Ejecute el archivo de pila app-security.yml

Tarea	Descripción	Habilidades requeridas
Ejecute el archivo de pila `app-security.yml`.	Los archivos de pila `app-security.yml` implementan la infraestructura restante para el sistema de notificación	AWS DevOps, administrador de sistemas de AWS, DevOps ingeniero, jefe de construcción

Tarea	Descripción	Habilidades requeridas
	y aprobación. Para ejecutar el archivo `app-security.yml` , haga lo siguiente: 1. Inicie sesión en la Consola de administración de AWS CloudFormation consola y ábrala. Elija Crear pila, y, a continuación, elija Con nuevos recursos (estándar) en la lista desplegable. 2. En la página Crear pila, seleccione Elegir una plantilla existente y Cargar un archivo de plantilla. Luego, seleccione Elegir archivo y app-security.yml. Elija Siguiente. 3. En la página Especificar los detalles de la pila, introduzca los valores de los parámetros tal y como se describe en Información adicional. A continuación, elija Siguiente. 4. En la página Configurar las opciones de pila, elija el rol de IAM para crear los recursos, tal y como se describe en Requisitos previos. A continuación, elija Siguiente.	

Tarea	Descripción	Habilidades requeridas
	5. En la página Revisar y crear, elija Enviar.	

Tarea	Descripción	Habilidades requeridas
Pruebe la configuración de la notificación.	Para probar la configuración de la notificación, haga lo siguiente: 1. Abra la consola de Amazon SNS. En el panel de navegación izquierdo, elija Topics (Temas). 2. Selecciona el nombre del tema que termina en LambdaToAWSSlackChatbot. 3. En la página de detalles del tema, seleccione Publicar mensaje. 4. En la página Publicar mensaje en tema, en el cuerpo del mensaje que se va a enviar al punto de conexión, ingrese lo siguiente: `{ "version": "1.0", "source": "custom", "content": { "description": ":warning: This is a test notification" } }` 5. Elija Publish message (Publicar mensaje).	AWS DevOps, administrador de sistemas de AWS, DevOps ingeniero, jefe de construcción

Tarea	Descripción	Habilidades requeridas
	Cuando el mensaje de prueba se entregue correctamente, debería ver una notificación en el canal de Slack. Para obtener más información, consulta Probar las notificaciones desde Slack en la Guía del administrador de aplicaciones de chat Servicios de AWS para desarrolladores de Amazon Q.	

Configuración del flujo de aprobación

Tarea	Descripción	Habilidades requeridas
Configure una acción de Lambda personalizada.	Para configurar la AWS Lambda acción personalizada, haga lo siguiente: 1. Pulse el botón de puntos suspensivos verticales en la parte inferior de la notificación de entrega en su canal de Slack. 2. En Administrar acciones, seleccione Crear. 3. Introduzca un nombre de acción personalizado, por ejemplo, Aprobar. Este nombre es un identificador único para la acción personalizada.	Administrador de AWS DevOps, jefe de construcción, DevOps ingeniero, administrador de Slack

Tarea	Descripción	Habilidades requeridas
	4. Introduzca un nombre para el botón de acción personalizado, por ejemplo, Aprobar. Este nombre aparece en un botón de la notificación. Este nombre debe tener 20 caracteres o menos y puede incorporar emojis. 5. En Tipo de acción personalizada, seleccione Acción de Lambda. 6. Elija Siguiente. 7. Seleccione el Región de AWS lugar Cuenta de AWS y el lugar en el que desee implementar esta acción. 8. Elija Cargar Lambda. 9. En Definir función Lambda, seleccione una función Lambda que termine en. ApprovalEmailLambdaA continuación, elija Siguiente . 10. Para crear el botón Aprobar, seleccione Guardar en la página Mostrar criterios.	

Tarea	Descripción	Habilidades requeridas
Valide el flujo de aprobación.	Para validar que el flujo de aprobación funciona según lo esperado, seleccione el botón Aprobar en Slack. Slackbot debería enviar una notificación en el hilo de mensajes con la cadena de confirmación El correo electrónico de aprobación se envió correctamente.	Administrador de AWS, DevOps ingeniero de AWS DevOps, administrador de Slack

Resolución de problemas

Problema	Solución
Configuraciones incorrectas de Slack	Para obtener información sobre cómo solucionar problemas relacionados con errores de configuración de Slack, consulte Solución de problemas de Amazon Q Developer en la Guía del administrador de aplicaciones de chat de Amazon Q Developer.
El análisis falló por algún otro motivo	Este error significa que se ha producido un error en la tarea de compilación de código. Para solucionar el problema, vaya al enlace que aparece en el mensaje. El error de la tarea de compilación de código puede deberse a las siguientes causas posibles: • La aplicación no está empaquetada correctamente. El comando `sonar-scanner` no encuentra el archivo `sonar.project.env.properties` .

Problema	Solución
	• Los valores de los parámetros `SonarFileName` , `SonarFileDirectory` o `SonarToken` son incorrectos. Compruebe los valores y, a continuación, vuelva a ejecutar los archivos de pila. • No se puede llegar al host de Sonar. • Otras cuestiones para las que puede utilizar los registros para solucionar problemas.

Recursos relacionados

AWS documentación

- Configuración de un cliente de Slack
- Crear una acción personalizada
- Procedimiento de creación de una identidad de dirección de correo electrónico
- Tutorial: Cómo empezar a usar Slack

Otros recursos

- Adición de aplicaciones al espacio de trabajo de Slack (documentación de Slack)
- Generación y uso de fichas (SonarQube documentación)
- Introducción a la instalación del servidor (SonarQube documentación)

Información adicional

Esta solución hace hincapié en Amazon Q Developer en las acciones personalizadas de las aplicaciones de chat con fines de administración de versiones. Sin embargo, para reutilizar la solución, modifique el código de Lambda para su caso de uso específico y desarrolle a partir de él.

Parámetros de los archivos CloudFormation apilados

La siguiente tabla muestra los parámetros y sus descripciones para el archivo de CloudFormation pila`pre-requisite.yml`.

Clave	Descripción
`StackName`	El nombre de la CloudFormation pila.
`S3LambdaBucket`	El nombre del bucket de Amazon S3 en el que cargó el código de Lambda. El nombre debe ser único de forma global.
`SonarToken`	El token SonarQube de usuario, tal y como se describe en los requisitos previos.

En la siguiente tabla se muestran los parámetros y sus descripciones para el archivo `app-security.yml` de CloudFormation pila.

Clave	Descripción
`CKMSKeyArn`	El nombre de recurso de AWS KMS key Amazon (ARN) que se utiliza en las funciones de IAM y Lambda creadas en esta pila.
`CKMSKeyId`	El AWS KMS key ID que se utiliza en el tema de Amazon SNS creado en esta pila.
`EnvironmentType`	El nombre del entorno del cliente para la implementación de la canalización de análisis de aplicaciones. Seleccione el nombre del entorno en la lista desplegable de valores permitidos.
`S3LambdaBucket`	Nombre del bucket de Amazon S3 que contiene los archivos `approval.zip` y `notification.zip` .
`SESEmail`	El nombre de la identidad de correo electrónico registrada en Amazon SES, tal y como se describe en Requisitos previos. Esta identidad es la dirección de correo electrónico de origen.

`SharedInboxMail`	La dirección de correo electrónico de destino a la que se envían las notificaciones de análisis.
`SlackChannelId`	El ID del canal de Slack al que quiere que se envíen las notificaciones. Para encontrar el ID del canal, haga clic con el botón derecho en el nombre del canal en la sección Detalles del canal en la aplicación de Slack. El ID del canal está en la parte inferior.
`SlackWorkspaceId`	El ID del espacio de trabajo de Slack, tal y como se describe en los requisitos previos. Para encontrar el ID del espacio de trabajo de Slack, inicia sesión en la Consola de administración de AWS consola de aplicaciones de chat para desarrolladores de Amazon Q y seleccione Clientes configurados, Slack, WorkspaceID.
`StackName`	El nombre de la pila. CloudFormation
`SonarFileDirectory`	El nombre del directorio que contiene el archivo `sonar.project.<env>.properties` .
`SonarFileName`	El nombre del archivo `sonar.project.<env>properties` .
`SourceCodeZip`	El nombre del archivo .zip que contiene el archivo `sonar.project.<env>properties` y el código fuente.

Implementación de sistemas de agentes en Amazon Bedrock con el marco CrewAI mediante Terraform

Vanitha Dontireddy, Amazon Web Services

Resumen

Este patrón demuestra cómo implementar sistemas de IA multiagente escalables mediante el marco CrewAI integrado con Amazon Bedrock y Terraform. La solución permite a las organizaciones crear, implementar y administrar flujos de trabajo sofisticados de agentes de IA mediante la infraestructura como código (IaC). En este patrón, las capacidades de orquestación multiagente de CrewAI se combinan con los modelos fundacionales de Amazon Bedrock y la automatización de la infraestructura de Terraform. Como resultado, los equipos pueden crear sistemas de IA listos para la producción que aborden tareas complejas con una supervisión humana mínima. El patrón implementa las prácticas recomendadas operativas de escalabilidad y de seguridad de nivel empresarial.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS con los permisos adecuados para acceder a los modelos de Amazon Bedrock Foundation
- La versión 1.5 o posterior de Terraform instalada
- Python versión 3.9 o posterior instalada
- Marco CrewAI instalado

Limitaciones

- Las interacciones entre los agentes están limitadas por las ventanas de contexto del modelo.
- Las consideraciones de administración del estado de Terraform para las implementaciones a gran escala se aplican a este patrón.
- Algunas Servicios de AWS no están disponibles en todas Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

En este patrón, se producen las siguientes interacciones:

- Amazon Bedrock proporciona la base para la inteligencia de los agentes a través de su conjunto de modelos básicos (FMs). Ofrece a los agentes de IA capacidades de procesamiento de lenguaje natural (NLP), razonamiento y toma de decisiones, a la vez que mantiene una alta disponibilidad y escalabilidad.
- El marco CrewAI sirve como capa central de orquestación para crear y administrar agentes de IA. Gestiona los protocolos de comunicación de los agentes, la delegación de tareas y la administración del flujo de trabajo a la vez que se integra con Amazon Bedrock.
- Terraform administra toda la infraestructura mediante código, incluidos los recursos de cómputo, las redes, los grupos de seguridad y las funciones AWS Identity and Access Management (IAM). Garantiza implementaciones consistentes y con control de versiones en todos los entornos. La implementación de Terraform crea lo siguiente:
  - AWS Lambda función para ejecutar la aplicación CrewAI
  - Buckets de Amazon Simple Storage Service (Amazon S3) para código e informes
  - Roles de IAM con los permisos adecuados
  - CloudWatch Registro de Amazon
  - Ejecución programada por parte de Amazon EventBridge

En el siguiente diagrama, se ilustra la arquitectura para la implementación de sistemas de agentes múltiples de CrewAI mediante el uso de Amazon Bedrock y Terraform.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El usuario clona el repositorio.
2. El usuario ejecuta el comando `terraform apply` para implementar los AWS recursos.
3. La configuración del modelo de Amazon Bedrock incluye la especificación del modelo fundacional (FM) que se utilizará para configurar los agentes de CrewAI.
4. Se establece una EventBridge regla para activar la función Lambda de acuerdo con el programa definido.
5. Cuando se activa (de forma programada o manual), la función Lambda se inicializa y asume la función de IAM con permisos de acceso y Servicios de AWS Amazon Bedrock.

6. El marco CrewAI carga las configuraciones de los agentes desde archivos YAML y crea agentes de IA especializados (el equipo de auditoría de seguridad de la infraestructura de AWS). La función Lambda ejecuta estos agentes de forma secuencial para analizar los AWS recursos, analizar las vulnerabilidades de seguridad y generar informes de auditoría completos.
7. CloudWatch Los registros recopilan información de ejecución detallada de la función Lambda con un período de retención de 365 días y AWS Key Management Service (AWS KMS) cifrado para cumplir con los requisitos de conformidad. Los registros proporcionan visibilidad de las actividades de los agentes, el seguimiento de los errores y las métricas de rendimiento, lo que permite una supervisión eficaz del proceso de auditoría de seguridad y la solución de problemas.
8. El informe de auditoría de seguridad se genera y almacena automáticamente en el bucket de Amazon S3 designado. La configuración automatizada ayuda a mantener una supervisión de seguridad coherente con una sobrecarga operativa mínima.

Tras la implementación inicial, el flujo de trabajo proporciona auditorías e informes de seguridad continuos para su AWS infraestructura sin intervención manual.

Información general de los agentes de IA

Este patrón crea varios agentes de IA, cada uno con roles, objetivos y herramientas únicos:

- El agente analista de seguridad recopila y analiza la información sobre AWS los recursos.
- El agente probador de penetración identifica las vulnerabilidades en AWS los recursos.
- El agente experto en conformidad comprueba las configuraciones con respecto a las normas de conformidad.
- El agente redactor de informes recopila los resultados en informes exhaustivos.

Estos agentes colaboran en una serie de tareas y aprovechan sus habilidades colectivas para realizar auditorías de seguridad y generar informes exhaustivos. (El archivo `config/agents.yaml` describe las capacidades y configuraciones de cada agente de este equipo).

El procesamiento del análisis de seguridad consiste en las siguientes acciones:

1. El agente analista de seguridad examina los datos recopilados sobre AWS los recursos, como los siguientes:
   - Instancias y grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2)
   - Configuraciones y buckets de Amazon S3

- Roles, políticas y permisos de IAM
- Configuraciones de nube privada virtual (VPC) y configuración de red
- Bases de datos y configuración de seguridad de Amazon RDS
- Configuraciones y funciones de Lambda
- Otros Servicios de AWS dentro del ámbito de la auditoría

2. El agente que realiza pruebas de penetración identifica las posibles vulnerabilidades.
3. Los agentes colaboran a través del marco CrewAI para compartir sus resultados.

La generación de informes consiste en las siguientes acciones:

1. El agente redactor del informe recopila los resultados de todos los demás agentes.
2. Los problemas de seguridad se organizan por servicio, gravedad e impacto en la conformidad.
3. Se generan recomendaciones de corrección para cada problema identificado.
4. Se crea un informe completo de auditoría de seguridad en formato markdown y se carga en el bucket de Amazon S3 designado. Los informes históricos se conservan para hacer un seguimiento de la conformidad y mejorar la postura de seguridad.

Las actividades de registro y supervisión incluyen:

- CloudWatch los registros capturan los detalles de la ejecución y cualquier error.
- Las métricas de ejecución de Lambda se registran para su supervisión.

> **Note**
>
> El código proviene `aws-security-auditor-crew` del repositorio GitHub 3P-Agentic_Frameworks, disponible en la colección Samples. AWS

Disponibilidad y escala

Puede ampliar los agentes disponibles a más de los cuatro agentes principales. Para escalar con más agentes especializados, considere los siguientes tipos de agentes nuevos:

- Un agente especialista en inteligencia de amenazas puede hacer lo siguiente:
  - Supervisa las fuentes de amenazas externas y las correlaciona con los resultados internos

    - Proporciona un contexto sobre las amenazas emergentes relevantes para su infraestructura
    - Prioriza las vulnerabilidades en función de su explotación activa en el entorno natural
- Los agentes del marco de conformidad pueden centrarse en áreas reguladoras específicas, como las siguientes:
    - Agente de conformidad con el estándar de seguridad de datos del sector de tarjetas de pago (PCI DSS)
    - Agente de conformidad con la Ley de Portabilidad y Responsabilidad de Seguros Médicos de EE. UU de 1996 (Health Insurance Portability and Accountability Act of 1996, HIPAA).
    - Agente de conformidad con los Controles del Sistema y Organizaciones 2 (SOC 2)
    - Agente de conformidad con el Reglamento General de Protección de Datos (RGPD)

Al ampliar cuidadosamente los agentes disponibles, esta solución puede proporcionar información de seguridad más profunda y especializada, al tiempo que mantiene la escalabilidad en entornos de gran tamaño. AWS Para obtener más información sobre el enfoque de implementación, el desarrollo de herramientas y las consideraciones de escalado, consulte Información adicional.

Tools (Herramientas)

Servicios de AWS

- Amazon Bedrock es un servicio de IA totalmente gestionado que permite que los modelos básicos de alto rendimiento (FMs) estén disponibles para su uso a través de una API unificada.
- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas y aplicaciones Servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, AWS Lambda funciones, puntos finales de invocación HTTP que utilizan destinos de API o buses de eventos en otros. Cuentas de AWS En este patrón, se utiliza para programar y organizar los flujos de trabajo de los agentes.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

- AWS SDK para Python (Boto3)es un kit de desarrollo de software que le ayuda a integrar su aplicación, biblioteca o script de Python con Servicios de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos. En este patrón, proporciona almacenamiento de objetos para los artefactos de los agentes y la administración del estado.

Otras herramientas

- CrewAI es un marco de código abierto basado en Python para crear sistemas de IA multiagéntica
- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.

Repositorio de código

El código de este patrón está disponible en el repositorio. GitHub deploy-crewai-agents-terraform

Prácticas recomendadas

- Implemente una administración de estado adecuada para Terraform mediante un backend de Amazon S3 con bloqueo de Amazon DynamoDB. Para obtener más información, consulta las mejores prácticas de backend en Prácticas recomendadas para usar el proveedor de Terraform AWS .
- Utilice los espacios de trabajo para separar los entornos de desarrollo, almacenamiento provisional y producción.
- Siga el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.
- Habilite el registro y la supervisión detallados a través CloudWatch de los registros.
- Implemente mecanismos de reintento y gestión de errores en las operaciones de los agentes.

Epics

Implementación de marcos CrewAI

Tarea	Descripción	Habilidades requeridas

Clonar el repositorio.	Para clonar un repositorio de este patrón en su máquina local, ejecute el siguiente comando:
	`git clone "git@github.com:aws-samples/deploy-crewai-agents-terraform.git"`
	`cd deploy-crewai-agents-terraform`
		DevOps ingeniero

Edite las variables de entorno.	Para editar las variables de entorno, haga lo siguiente: 1. Cree un archivo `terraform.tfvars` a partir del ejemplo `terraform.tfvars.example` en el directorio de terraform. 2. Edite las variables de entorno para usar su propia información.	DevOps ingeniero

Cree la infraestructura.	Para crear la infraestructura, ejecute los comandos siguientes:
	`cd terraform`
	`terraform init`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	`terraform plan`
	
	Revise el plan de ejecución detenidamente. Si los cambios planificados son aceptables, ejecute el comando siguiente:
	
	`terraform apply --auto-approve`	

Acceso a los agentes de CrewAI

Tarea	Descripción	Habilidades requeridas
Acceda a los agentes.	Los agentes del equipo de auditoría e informes de seguridad de la AWS infraestructura se despliegan como una función Lambda. Para acceder a los agentes, siga estos pasos: 1. Inicie sesión en Consola de administración de AWS y abra la AWS Lambda consola en https://console.aws.amazon.com/lambda/. 2. En la página Funciones, busque y, a continuación, seleccione la función denominada `{project_name}` \function (tal como se define en las variables de Terraform).	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	3. En la página de la función puede realizar las siguientes acciones: • Ver los detalles de la configuración. • Supervisar las métricas de ejecución. • Ver CloudWatch los registros. • Probar la función de forma manual.	

Tarea	Descripción	Habilidades requeridas
(Opcional) Configure la ejecución manual de los agentes.	Los agentes están configura dos para ejecutarse automátic amente según una programac ión diaria (medianoche UTC). Sin embargo, puede desencadenarlos manualmen te mediante los siguientes pasos: 1. En la consola de Lambda, seleccione la función denominada `{project_ name}` . 2. En la página de la función, seleccione la pestaña Prueba. 3. Cree un nuevo evento de prueba con un objeto JSON `{}` vacío. 4. Para ejecutar el evento, seleccione Prueba. Para obtener más información, consulte Prueba de funciones de Lambda en la consola en la documentación de Lambda.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Acceda a los registro del agente para la depuración.	Los agentes de CrewAI se ejecutan en un entorno de Lambda con los permisos necesarios para realizar auditorías de seguridad y almacenar informes en Amazon S3. El resultado es un informe de rebajas que proporciona un análisis exhaustivo de la seguridad de su AWS infraestructura. Para facilitar la depuración detallada del comportamiento del agente, haga lo siguiente: 1. En el Consola de administración de AWS, vaya a CloudWatch Registros. 2. Busque el grupo de registro para la función de Lambda. 3. Busque entradas de registro con los nombres de los agentes (por ejemplo, especialista en asignación de infraestructuras y analista de seguridad exploratorio). 4. Revise los registros para obtener información sobre las acciones de cada agente.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Vea los resultados de la ejecución de los agentes.	Para ver los resultados de la ejecución de un agente, haga lo siguiente: 1. En Consola de administración de AWS, navegue hasta Amazon S3. 2. Abra el bucket de Amazon S3 denominado `{project_name}-reports-{random_suffix}` (tal y como se define en las variables de Terraform). Los informes se almacenan con nombres de archivo basados en marcas de tiempo de la siguiente manera: `security-audit-report-YYYY-MM-DD-HH-MM-SS.md)`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Supervise la ejecución de los agentes.	Para supervisar la ejecución de los agentes a través de los CloudWatch registros, haga lo siguiente: 1. En el Consola de administración de AWS, navegue hasta. CloudWatch 2. Vaya a Grupos de registros. 3. Seleccione el grupo de registro denominado `/aws/lambda/{project_name}-function` . 4. En Flujos de registro, elija el flujo de registro más reciente para ver información de ejecución detallada.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Personalice el comportamiento del agente.	Para modificar los agentes o sus tareas, haga lo siguiente:
	1. Actualice los archivos de configuración en su repositorio local:
	• El siguiente archivo define el rol, las capacidades y la configuración de cada agente: `src/aws_infrastructure_security_audit_and_reporting/config/agents.yaml`
	• El siguiente archivo define las tareas y los flujos de trabajo de los agentes: `src/aws_infrastructure_security_audit_and_reporting/config/tasks.yaml`
	2. Para volver a empaquetar y actualizar la función de Lambda, utilice los siguientes comandos:
	`cd terraform`
	`terraform apply`
		DevOps ingeniero

Eliminar recursos

Tarea	Descripción	Habilidades requeridas

Elimine los recursos creados.	Para eliminar toda la infraestructura creada por este patrón, ejecute el comando siguiente:
	`terraform plan -destroy`
	Warning
	El comando siguiente eliminará de forma permanente todos los recursos creados por este patrón. El comando solicitará una confirmación antes de eliminar cualquier recurso.
	Revise el plan de eliminación detenidamente. Si las eliminaciones planificadas son aceptables, ejecute el comando siguiente:
	`terraform destroy`
		DevOps ingeniero

Resolución de problemas

Problema	Solución
Comportamiento del agente	Para obtener información sobre este problema, consulte Prueba y solución de problemas del comportamiento de los agentes en la documentación de Amazon Bedrock.
Problemas de la red de Lambda	Para obtener información sobre estos problemas, consulte Solución de problemas de red en Lambda en la documentación de Lambda.
Permisos de IAM	Para obtener información sobre estos problemas, consulte Solución de problemas de IAM en la documentación de IAM.

Recursos relacionados

AWS Blogs

- Compilación de sistemas de agentes con CrewAI y Amazon Bedrock

AWS documentación

- Documentación de Amazon Bedrock
- Cómo funciona Amazon Bedrock Agents
- AWS Marco de buena arquitectura

Otros recursos

- Documentación de CrewAI
- Documentación para proveedores de Terraform AWS

Información adicional

Esta sección contiene información sobre el enfoque de implementación, el desarrollo de herramientas y las consideraciones de escalado relacionadas con el análisis anterior sobre Automatización y escalabilidad.

Enfoque de implementación

Considere el siguiente enfoque para añadir agentes:

1. Configuración del agente:
   - Añada nuevas definiciones de agentes al archivo `config/agents.yaml`.
   - Defina historias de fondo, objetivos y herramientas especializados para cada agente.
   - Configure las capacidades de memoria y análisis en función de la especialidad del agente.
2. Orquestación de la tarea:
   - Actualice el archivo `config/tasks.yaml` para incluir nuevas tareas específicas del agente.
   - Cree dependencias entre las tareas para garantizar un flujo de información adecuado.
   - Implemente la ejecución paralela de tareas cuando sea apropiado.

Implementación técnica

A continuación se incluye una adición al archivo `agents.yaml` de un agente especialista en inteligencia de amenazas propuesto:

```
Example new agent configuration in agents.yaml
threat_intelligence_agent:
 name: "Threat Intelligence Specialist"
 role: "Cybersecurity Threat Intelligence Analyst"
 goal: "Correlate AWS security findings with external threat intelligence"
 backstory: "Expert in threat intelligence with experience in identifying emerging
 threats and attack patterns relevant to cloud infrastructure."
verbose: true
allow_delegation: true
tools:
- "ThreatIntelligenceTool"
- "AWSResourceAnalyzer"
```

Desarrollo de herramientas

Con el marco CrewAI, puede tomar las siguientes medidas para mejorar la eficacia del equipo de auditoría de seguridad:

- Cree herramientas personalizadas para los nuevos agentes.
- Intégrelo con dispositivos externos APIs para obtener información sobre amenazas.
- Desarrolle analizadores especializados para diferentes tipos. Servicios de AWS

Consideraciones de escalado

Al ampliar su sistema de informes y auditorías de seguridad de la AWS infraestructura para gestionar entornos más grandes o auditorías más exhaustivas, aborde los siguientes factores de escalamiento:

- Recursos computacionales
  - Aumente la asignación de memoria de Lambda para gestionar agentes adicionales.
  - Considere la posibilidad de dividir las cargas de trabajo de los agentes en varias funciones de Lambda.
- Administración de costos
  - Supervise el uso de la API de Amazon Bedrock a medida que aumenta el número de agentes.
  - Implemente la activación selectiva de los agentes en función del alcance de la auditoría.
- Eficiencia de colaboración
  - Optimice el intercambio de información entre los agentes.
  - Implemente estructuras jerárquicas de agentes para entornos complejos.
- Mejora de la base de conocimientos
  - Proporcione a los agentes bases de conocimiento especializadas para sus dominios.
  - Actualice periódicamente los conocimientos sobre los agentes con las nuevas prácticas recomendadas de seguridad.

Implemente un trabajo de AWS Glue con una canalización de CodePipeline CI/CD de AWS

Bruno Klein y Luis Henrique Massao Yamada, Amazon Web Services

Resumen

Este patrón demuestra cómo puede integrar AWS CodeCommit y AWS CodePipeline con AWS Glue y utilizar AWS Lambda para lanzar trabajos tan pronto como un desarrollador envíe sus cambios a un repositorio remoto de AWS. CodeCommit

Cuando un desarrollador envía un cambio a un repositorio de extracción, transformación y carga (ETL) y envía los cambios a AWS CodeCommit, se invoca una nueva canalización. La canalización inicia una función de Lambda que lanza un trabajo de AWS Glue con estos cambios. El trabajo de AWS Glue lleva a cabo la tarea de ETL.

Esta solución resulta útil en situaciones en las que las empresas, los desarrolladores y los ingenieros de datos desean lanzar sus trabajos tan pronto como se implementan los cambios y se envíen a los repositorios de destino. Facilita poder lograr un mayor nivel de automatización y reproducibilidad y, por lo tanto, evita errores durante el lanzamiento y el ciclo de vida del trabajo.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Git instalado en el equipo local
- Kit de desarrollo en la nube de Amazon (Amazon CDK) instalado en el equipo local
- Python instalado en el equipo local
- El código de la sección Attachments

Limitaciones

- La canalización finaliza en cuanto el trabajo de AWS Glue se inicia correctamente. No espera a que finalice el trabajo.
- El código que se proporciona en el archivo adjunto está destinado únicamente a fines de demostración.

Arquitectura

Pila de tecnología de destino

- AWS Glue
- AWS Lambda
- AWS CodePipeline
- AWS CodeCommit

Arquitectura de destino

El proceso consta de estos pasos:

1. El desarrollador o el ingeniero de datos realiza una modificación en el código ETL, confirma y envía el cambio a AWS CodeCommit.
2. El envío inicia la canalización.
3. La canalización inicia una función de Lambda, que llama a `codecommit:GetFile` en el repositorio y carga el archivo en Amazon Simple Storage Service (Amazon S3).
4. La función de Lambda lanza un nuevo trabajo de AWS Glue con el código ETL.
5. La función de Lambda finaliza la canalización.

Automatizar y escalar

En el ejemplo adjunto se muestra cómo puede integrar AWS Glue con AWS CodePipeline. Proporciona un ejemplo básico que se puede personalizar o ampliar para el propio uso. Para más información, consulte la sección Epics.

Tools (Herramientas)

- AWS CodePipeline: AWS CodePipeline es un servicio de entrega continua totalmente gestionado que le ayuda a automatizar sus procesos de lanzamiento para obtener actualizaciones rápidas y fiables de las aplicaciones y la infraestructura.
- AWS CodeCommit: AWS CodeCommit es un servicio de control de código fuente totalmente gestionado que aloja repositorios seguros basados en Git.

- AWS Lambda: AWS Lambda es un servicio informático sin servidor que permite ejecutar código sin aprovisionar ni administrar servidores.
- AWS Glue: AWS Glue es un servicio de integración de datos sin servidor que facilita la detección, preparación y combinación de datos para análisis, machine learning y desarrollo de aplicaciones.
- Cliente Git: Git proporciona herramientas de GUI, o puedes usar la línea de comandos o una herramienta de escritorio para comprobar los artefactos necesarios GitHub.
- AWS CDK: AWS CDK es un marco de desarrollo de software de código abierto que ayuda a definir los recursos de las aplicaciones en la nube mediante lenguajes de programación conocidos.

Epics

Implementar el código de muestra

Tarea	Descripción	Habilidades requeridas
Configure la AWS CLI.	Configure la interfaz de la línea de comandos de AWS (AWS CLI) para señalar y autenticarse con su cuenta de AWS actual. Para obtener instrucciones, consulte la documentación de AWS CLI.	Desarrollador, DevOps ingeniero
Extraiga los archivos de muestra del proyecto.	Extraiga los archivos del adjunto para crear una carpeta que contenga los archivos del proyecto de muestra.	Desarrollador, DevOps ingeniero

Implemente el código de muestra.	Después de extraer los archivos, ejecute los comandos siguientes desde la ubicación de extracción para crear un ejemplo de referenci a:
	`cdk bootstrap`
	`cdk deploy`
		Desarrollador, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	``` git init git remote add origin <code-commit-repos itory-url> git stage . git commit -m "adds sample code" git push --set-upstream origin main ``` Una vez emitido el último comando, puede supervisar el estado de la canalización y el trabajo de AWS Glue.	
Personalice el código.	Personalice el código del archivo etl.py de acuerdo con los requisitos de su empresa. Puede revisar el código ETL, modificar las etapas del proceso o ampliar la solución.	Ingeniero de datos

Recursos relacionados

- Getting started with the AWS CDK (Introducción a los AWS CDK)
- Adding jobs in AWS Glue (Cómo agregar trabajos a AWS Glue)
- Integraciones de acciones fuente en CodePipeline
- Invoque una función de AWS Lambda en una canalización en CodePipeline
- AWS Glue programming (Programación con AWS Glue)
- CodeCommit GetFile API DE AWS

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Implemente código en varias regiones de AWS mediante AWS CodePipeline CodeCommit, AWS y AWS CodeBuild

Anand Krishna Varanasi, Amazon Web Services

Resumen

Este patrón demuestra cómo crear una infraestructura o arquitectura en varias regiones de Amazon Web Services (AWS) mediante AWS CloudFormation. Incluye integración continua (CI) e implementación continua (CD) en varias regiones de AWS para lograr implementaciones más rápidas. Por ejemplo, se probaron los pasos de este patrón para crear un CodePipeline trabajo de AWS para implementarlo en tres regiones de AWS. Puede cambiar el número de regiones en función del caso de uso.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- • Un CodeBuild puesto en Amazon S3 FullAccess y en CloudWatchFullAccesslas políticas. Estas políticas permiten CodeBuild ver eventos de AWS a CodeCommit través de Amazon CloudWatch y utilizar Amazon Simple Storage Service (Amazon S3) como almacén de artefactos.
  - Un CloudFormation rol de AWS con las siguientes políticas, que permiten a AWS CloudFormation, en la fase final de creación, crear o actualizar las funciones de AWS Lambda, enviar o ver CloudWatch los registros de Amazon y crear y actualizar conjuntos de cambios.
    - AWSLambdaFullAccess
    - AWSCodeDeployFullAccess
    - CloudWatchFullAccess
    - AWSCloudFormationFullAccess
    - AWSCodePipelineFullAccess

> **Note**
>
> Dos funciones de AWS Identity and Access Management (IAM) para AWS CodeBuild y AWS CloudFormation con las políticas adecuadas CodeBuild para realizar las tareas de CI consistentes en probar, agrupar, empaquetar los artefactos e implementarlos en varias

regiones de AWS en paralelo. Compruebe las políticas creadas por CodePipeline para comprobar que CodeBuild AWS cuenta con los CloudFormation permisos adecuados en las fases de CI y CD.

Arquitectura

La arquitectura y el flujo de trabajo de varias regiones de este patrón comprenden los siguientes pasos.

1. Envía el código a un CodeCommit repositorio.
2. Al recibir cualquier actualización o confirmación de código, CodeCommit invoca un CloudWatch evento que, a su vez, inicia un CodePipeline trabajo.
3. CodePipeline activa el CI gestionado por. CodeBuild Se realizan las siguientes tareas.
   - Prueba de las CloudFormation plantillas de AWS (opcional)
   - Empaquetado de las CloudFormation plantillas de AWS para cada región incluidas en la implementación. Por ejemplo, este patrón se implementa en paralelo en tres regiones de AWS, por lo que CodeBuild empaqueta las CloudFormation plantillas de AWS en tres grupos de S3, uno en cada región especificada. Los depósitos de S3 se utilizan únicamente CodeBuild como repositorios de artefactos.
4. CodeBuild empaqueta los artefactos como entrada para la siguiente fase de implementación, que se ejecuta en paralelo en las tres regiones de AWS. Si especifica un número diferente de regiones, CodePipeline se desplegará en esas regiones.

Tools (Herramientas)

Herramientas

- AWS CodePipeline: CodePipeline es un servicio de entrega continua que puede utilizar para modelar, visualizar y automatizar los pasos necesarios para publicar los cambios de software de forma continua.
- AWS CodeBuild: CodeBuild es un servicio de compilación totalmente gestionado que compila el código fuente, ejecuta pruebas unitarias y produce artefactos listos para su implementación.

- AWS CodeCommit: CodeCommit es un servicio de control de versiones hospedado por Amazon Web Services que puede utilizar para almacenar y gestionar activos (como código fuente y archivos binarios) en la nube de forma privada.
- AWS CloudFormation: AWS CloudFormation es un servicio que le ayuda a modelar y configurar sus recursos de Amazon Web Services para que pueda dedicar menos tiempo a gestionar esos recursos y más a centrarse en las aplicaciones que se ejecutan en AWS.
- AWS Identity and Access Management: AWS Identity and Access Management (IAM) es un servicio web que le ayuda a controlar de forma segura el acceso a los recursos de AWS.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet. Está diseñado para facilitar a los desarrolladores recursos de computación escalables basados en Web.

Código

El siguiente código de ejemplo es para el archivo `BuildSpec.yaml` (fase de compilación).

```
---
artifacts:
discard-paths: true
files:
- packaged-first-region.yaml
- packaged-second-region.yaml
- packaged-third-region.yaml
phases:
build:
commands:
- echo "********BUILD PHASE - CF PACKAGING**********"
- "aws cloudformation package --template-file sam-template.yaml --s3-bucket
 $S3_FIRST_REGION --output-template-file packaged-first-region.yaml --region
 $FIRST_REGION"
- "aws cloudformation package --template-file sam-template.yaml --s3-bucket
 $S3_SECOND_REGION --output-template-file packaged-second-region.yaml --region
 $SECOND_REGION"
- "aws cloudformation package --template-file sam-template-anand.yaml --s3-bucket
 $S3_THIRD_REGION --output-template-file packaged-third-region.yaml --region
 $THIRD_REGION"
install:
commands:
- echo "********BUILD PHASE - PYTHON SETUP**********"
runtime-versions:
```

```
python: 3.8
post_build:
commands:
- echo "********BUILD PHASE - PACKAGING COMPLETION**********"
pre_build:
commands:
- echo "********BUILD PHASE - DEPENDENCY SETUP**********"
- "npm install --silent --no-progress"
- echo "********BUILD PHASE - DEPENDENCY SETUP DONE**********"
version: 0.2
```

Epics

Prepare el código y el CodeCommit repositorio

Tarea	Descripción	Habilidades requeridas
Seleccione la región de AWS principal para la implement ación.	Inicie sesión en su cuenta de AWS y elija la región principal para la implementación. El CodeCommit repositorio estará en la región principal.	DevOps
Cree el CodeCommit repositor io.	Cree el CodeCommit repositor io e introduzca el código necesario en él. Por lo general, el código incluye las plantillas de AWS CloudForm ation o AWS SAM, el código Lambda, si lo hubiera, y los CodeBuild `buildspec .yaml` archivos como entrada a AWS. CodePipeline	DevOps
Inserte el código en el CodeCommit repositorio.	En la sección de adjuntos, descargue el código de este ejemplo y, a continuación, inserte el código necesario en él. Por lo general, el código	DevOps

Tarea	Descripción	Habilidades requeridas
	puede incluir plantillas de AWS CloudFormation o AWS SAM, código Lambda y los CodeBuild `buildspec.yaml` archivos como entrada a la canalización.	

Fase de origen: Crear la canalización

Tarea	Descripción	Habilidades requeridas
Cree el CodePipeline trabajo.	En la CodePipeline consola, selecciona Crear canalización.	DevOps
Asigne un nombre al CodePipeline trabajo y elija la configuración del rol de servicio.	Introduzca un nombre para el trabajo y mantenga la configuración de rol de servicio predeterminada para CodePipeline crear el rol con las políticas necesarias adjuntas.	DevOps
Especifique la ubicación del almacén de artefactos.	En Configuración avanzada, mantenga la opción predeterminada para CodePipeline crear un bucket de S3 que se utilizará como almacenamiento de artefactos de código. Si en su lugar utiliza un bucket de S3 existente, el bucket debe estar en la región principal que especificó en la primera épica.	DevOps

Tarea	Descripción	Habilidades requeridas
Especifique la clave de cifrado.	Elimine la opción predeterminada, clave administrada de AWS predeterminada o utilice la clave administrada por el cliente de AWS Key Management Service (AWS KMS).	DevOps
Especifique el proveedor de origen.	En Proveedor de código fuente, elija AWS CodeCommit.	DevOps
Especifique el repositorio.	Elige el CodeCommit repositorio que creaste en la primera epopeya. Si ha colocado el código en una ramificación, elija la rama.	DevOps
Especifique cómo se detectan los cambios en el código.	Mantenga el valor predeterminado, Amazon CloudWatch Events, como activador del cambio CodeCommit para iniciar el CodePipeline trabajo.	DevOps

Fase de creación: configure la canalización

Tarea	Descripción	Habilidades requeridas
Especifique el proveedor de compilación.	Para el proveedor de compilación, elija AWS CodeBuild.	DevOps
Especifique la Región de AWS.	Elija la región principal que especificó en la primera épica.	DevOps

Fase de compilación: cree y configure el proyecto

Tarea	Descripción	Habilidades requeridas
Creación del proyecto	Elija Crear proyecto e especifique un nombre para el proyecto.	DevOps
Especifique la imagen del entorno.	Para esta demostración del patrón, utilice la imagen CodeBuild gestionada por defecto. También tiene la opción de utilizar una imagen de Docker personalizada si tiene una.	DevOps
Especifique el sistema operativo.	Elija Amazon Linux 2 o Ubuntu. **Note** Se acerca el fin de la compatibilidad de Amazon Linux 2. Para obtener más informaci ón, consulte Amazon Linux 2 FAQs.	DevOps
Especifique el rol de servicio.	Elija el rol para el que creó CodeBuild antes de empezar a crear el CodePipeline trabajo. (Consulte la sección Requisitos previos.)	DevOps
Establezca opciones adicional es.	Para Tiempo de espera y el Tiempo de espera en cola, mantenga los valores predeterminados. En el caso	DevOps

Tarea	Descripción	Habilidades requeridas
	del certificado, mantenga la configuración predeterminada a menos que desee utilizar un certificado personalizado.	
Crear las variables de entorno.	Para cada región de AWS en la que desee realizar la implementación, cree variables de entorno proporcionando el nombre del bucket de S3 y el nombre de la región (por ejemplo, us-east-1).	DevOps
Proporcione el nombre del archivo buildspec, si no es buildspec.yml.	Mantenga este campo en blanco si el nombre del archivo es el predeterminado, `buildspec.yaml` . Si ha cambiado el nombre del archivo buildspec, introdúzcalo aquí. Asegúrese de que coincide con el nombre del archivo que está en el CodeCommit repositorio.	DevOps
Especifique el registro.	Para ver los registros de Amazon CloudWatch Events, mantenga la configuración predeterminada. O bien, puede definir cualquier nombre de grupo o registrador específico.	DevOps

Omitir la fase de implementación

Tarea	Descripción	Habilidades requeridas
Omita la fase de implement ación y complete la creación de la canalización.	Al configurar la canalización, CodePipeline permite crear solo una etapa en la fase de implementación. Para realizar la implementación en varias regiones de AWS, omita esta fase. Una vez creada la canalización, puede añadir varias etapas de la fase de implementación.	DevOps

Fase de implementación: configure la canalización para la implementación en la primera región

Tarea	Descripción	Habilidades requeridas
Agregue una etapa a la fase de implementación.	Edite la canalización y elija Agregar etapa en la fase de implementación. Esta primera etapa es para la región principal.	DevOps
Proporcione un nombre de acción para la etapa.	Introduzca un nombre único que refleje la primera etapa (principal) y la región. Por ejemplo, introduzca primary_<region>_deploy.	DevOps
Especifique el proveedor de acciones.	En Action provider, elija AWS CloudFormation.	DevOps
Configure la región para la primera etapa.	Elija la primera región (principal), la misma región en CodePipeline la CodeBuild	DevOps

Tarea	Descripción	Habilidades requeridas
	que están configuradas. Esta es la región principal en la que desea implementar la pila.	
Especifique el artefacto de entrada.	Elija BuildArtifact. Este es el resultado de la fase de construcción.	DevOps
Especifique la acción que se va a realizar.	Para Modo acción, elija Crear o actualizar una pila.	DevOps
Introduzca un nombre para la CloudFormation pila.		DevOps
Especifique la plantilla para la primera región.	Seleccione el nombre del paquete específico de la región que empaquetó CodeBuild y descargó en el depósito de S3 de la primera región (principal).	DevOps
Especifique las capacidades.	Las capacidades son necesarias si la plantilla de pila incluye recursos de IAM o si se crea una pila directamente a partir de una plantilla que contiene macros. Para este patrón, utilice CAPABILITY_IAM, CAPABILITY_NAMED_IAM y CAPABILITY_AUTO_EXPAND.	DevOps

Fase de despliegue: configure la canalización para la implementación en la segunda región

Tarea	Descripción	Habilidades requeridas
Añada la segunda etapa a la fase de despliegue.	Para añadir una etapa para la segunda región, edite la canalización y elija Añadir etapa en la fase de despliegue. Importante: el proceso de creación de la segunda región es el mismo que el de la primera región, excepto por los siguientes valores.	DevOps
Proporcione un nombre de acción para la segunda etapa.	Introduzca un nombre único que refleje la segunda etapa y la segunda región.	DevOps
Configure la región para la segunda etapa.	Elija la segunda región en la que desea implementar la pila.	DevOps
Especifique la plantilla para la segunda región.	Seleccione el nombre del paquete específico de la región que empaquetó CodeBuild y descargó en el depósito de S3 de la segunda región.	DevOps

Fase de implementación: configure la canalización para la implementación en la tercera región

Tarea	Descripción	Habilidades requeridas
Añada la tercera etapa a la fase de implementación.	Para añadir una etapa para la tercera región, edite la canalización y elija Añadir etapa en la fase de implementación. Importante: el proceso	DevOps

Tarea	Descripción	Habilidades requeridas
	de creación de la segunda región es el mismo que el de las dos regiones anteriores, excepto por los siguientes valores.	
Proporcione un nombre de acción para la tercera etapa.	Introduzca un nombre único que refleje la tercera etapa y la tercera región.	DevOps
Configure la región para la tercera etapa.	Elija la tercera región en la que desea implementar la pila.	DevOps
Especifique la plantilla para la tercera región.	Seleccione el nombre del paquete específico de la región que empaquetó CodeBuild y descargó en el depósito de S3 de la tercera región.	DevOps

Eliminar la implementación

Tarea	Descripción	Habilidades requeridas
Eliminación de los recursos de AWS.	Para limpiar la implement ación, elimine las CloudForm ation pilas de cada región. A continuación CodeCommi t, elimine los CodePipeline recursos CodeBuild, y de la región principal.	DevOps

Recursos relacionados

- ¿Qué es AWS CodePipeline?

- Modelo de aplicación sin servidor de AWS
- AWS CloudFormation
- Referencia de estructura de CloudFormation arquitectura de AWS para AWS CodePipeline

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Implemente cargas de trabajo desde DevOps canalizaciones de Azure a clústeres privados de Amazon EKS

Mahendra Revanasiddappa, Amazon Web Services

Resumen

Este patrón demuestra cómo implementar la integración continua y la entrega continua (CI/CD) desde DevOps canalizaciones de Azure a clústeres privados de Amazon Elastic Kubernetes Service (Amazon EKS). Aborda un desafío fundamental al que se enfrentan las organizaciones que están mejorando su postura de seguridad mediante la transición a puntos de conexión de servidores de API privados para sus clústeres de Amazon EKS.

Un punto de conexión público expone el servidor de API de Kubernetes directamente a Internet, lo que crea una mayor superficie expuesta a ataques a la que podrían dirigirse actores maliciosos. Al cambiar a un punto de conexión privado, el acceso al plano de control del clúster está restringido a la nube privada virtual (VPC) del cliente.

Si bien la transición de un clúster de Amazon EKS a un punto final de API privado mejora considerablemente la seguridad, presenta desafíos de conectividad para CI/CD plataformas externas como Azure DevOps. Solo se puede acceder al punto de conexión privado desde la VPC o las redes interconectadas del clúster. Por lo tanto, los DevOps agentes de Azure estándar alojados en Microsoft, que operan fuera de la red AWS privada, no pueden acceder directamente al servidor API de Kubernetes. Esto interrumpe los flujos de trabajo de implementación típicos que dependen de herramientas como kubectl o Helm que se ejecutan en estos agentes porque no logran establecer una conexión con el clúster.

Para superar este problema, este patrón muestra un enfoque eficiente mediante el uso de DevOps agentes de Azure autohospedados dentro de clústeres privados de Amazon EKS. Esta solución ofrece una optimización de costos, una eficiencia operativa y una escalabilidad superiores, a la vez que preserva los requisitos de seguridad. Este enfoque beneficia especialmente a las empresas que buscan optimizar sus DevOps procesos multicloud sin comprometer el rendimiento ni la seguridad.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.
- AWS Command Line Interface (AWS CLI) versión 2.13.17 o posterior, instalada.

- La versión 1.25.1 o posterior de kubectl instalada.
- Un clúster privado de Amazon EKS versión 1.24 o posterior creado, con permisos para crear espacios de nombres, secretos e implementaciones.
- Nodos de trabajo en un clúster de Amazon EKS con conectividad saliente a Internet para que el DevOps agente de Azure que se ejecute en ellos pueda conectarse al grupo de DevOps agentes de Azure.
- GitHub cuenta creada.
- Se creó un DevOps proyecto de Azure con acceso para configurar las conexiones de servicio, que son conexiones autenticadas entre Azure Pipelines y servicios externos o remotos.
- La AWS Toolkit for Azure DevOps versión 1.15 o posterior instalada para el DevOps proyecto de Azure descrito en el punto anterior. Para obtener instrucciones de instalación, consulte AWS Toolkit for Azure DevOps en Visual Studio Marketplace.

Limitaciones

- Algunas Servicios de AWS no están disponibles en todas Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

Este patrón crea lo siguiente:

- Repositorio Amazon ECR: el repositorio Amazon Elastic Container Registry (Amazon ECR) almacena la imagen de Docker con el DevOps agente de Azure y la aplicación de muestra que se implementa.
- Grupo de DevOps agentes de Azure: un grupo de agentes DevOps autohospedados de Azure registra el agente que se ejecuta en el clúster privado de Amazon EKS.
- Función de IAM: una función AWS Identity and Access Management (IAM) para la conexión del servicio de Azure que proporciona el acceso necesario al agente que se ejecuta en un clúster privado de Amazon EKS.
- Conexión DevOps de servicio de Azure: una conexión de servicio en una DevOps cuenta de Azure para utilizar la función de IAM que proporciona el acceso necesario para que accedan los trabajos en proceso. Servicios de AWS

El siguiente diagrama muestra la arquitectura de implementación de un DevOps agente de Azure autohospedado en un clúster privado de Amazon EKS y de implementación de una aplicación de muestra en el mismo clúster.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Implemente un DevOps agente de Azure autohospedado como una implementación dentro de un clúster de Amazon EKS.
2. Un DevOps agente de Azure se conecta al grupo de agentes de una DevOps cuenta de Azure mediante un token de acceso personal (PAT) para la autenticación.
3. Azure Pipelines configura una canalización para implementarla mediante código de un GitHub repositorio.
4. La canalización se ejecuta en el agente desde el grupo de agentes que se configuró en la configuración de canalización. El DevOps agente de Azure obtiene la información de trabajo de la canalización consultando constantemente la cuenta de Azure DevOps .
5. El DevOps agente de Azure crea una imagen de Docker como parte del trabajo en proceso y envía la imagen al repositorio de Amazon ECR.
6. El DevOps agente de Azure implementa la aplicación de muestra en un clúster privado de Amazon EKS en un espacio de nombres denominado. `webapp`

Tools (Herramientas)

Herramientas

- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar AWS Kubernetes sin necesidad de instalar o mantener su propio plano de control o nodos de Kubernetes.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.

Otras herramientas

- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización a nivel del sistema operativo para entregar software en contenedores.

- kubectl: una interfaz de la línea de comandos que le ayuda en la ejecución de comandos en clústeres de Kubernetes.

Repositorio de código

- El código de este patrón está disponible en el repositorio GitHub deploy-kubernetes-resources-to-amazon-eks-using-azure -devops.

Prácticas recomendadas

- Para Amazon EKS, consulte la Guía de prácticas recomendadas de Amazon EKS.
- Siga el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Creación de una conexión de servicio

Tarea	Descripción	Habilidades requeridas
Busque el GUID de la DevOps organización de Azure.	Inicie sesión en su DevOps cuenta de Azure y, a continuación, utilice la siguiente URL para buscar el GUID de la organización: `https://dev.azure.com/{DevOps_Org_ID}/_apis/projectCollections?api-version=6.0` En la URL, `{DevOps_org_ID}` sustitúyalo por el ID de su DevOps organización de Azure.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Configure un IdP en la Cuenta de AWS.	Para configurar un proveedor de identidad (IdP) en una conexión Cuenta de AWS de servicio de Azure, siga estos pasos: 1. Inicie sesión en la consola Consola de administración de AWS de IAM y ábrala en. https://console.aws.amazon.com/iam/ 2. En el panel izquierdo, elija Proveedores de identidades. 3. Elija Add Provider (Agregar proveedor). 4. Elija OpenID Connect como Tipo de proveedor. 5. En la URL del proveedor, introduzca la URL del DevOps emisor de Azure. Cada arrendatario de Azure DevOps tiene un formato único `OrganizationGUID` que suele utilizar el siguiente formato: `https://vstoken.dev.azure.com/{OrganizationGUID}` Sustitúyalo por `{OrganizationGUID}` el ID de su DevOps organización de Azure.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	6. Para Audience, escriba api: //Azure ADToken Exchange. Se trata de un valor fijo para Azure DevOps. 7. Elija Add Provider (Agregar proveedor). 8. Tome nota del ARN del proveedor recién creado para usarlo en la siguiente tarea. Para obtener más informaci ón, consulte Cómo federarse AWS desde Azure DevOps mediante OpenID Connect.	

Tarea	Descripción	Habilidades requeridas
Cree una política de IAM en la Cuenta de AWS.	Para crear una política de IAM que proporcione los permisos necesarios para la función de IAM utilizada por la DevOps canalización de Azure, siga estos pasos: 1. En la consola de IAM, en el panel izquierdo, elija Políticas. 2. Seleccione Crear política. 3. En la página Especificar permisos, en el editor de políticas, seleccione JSON. Reemplace el texto JSON predeterminado por el siguiente JSON: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "Statement1", "Effect": "Allow", "Action": [ "ecr:*", "eks:DescribeCluster", "eks:ListClusters" ],`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	<pre>"Resource
	": "*"
	}
	]
	}</pre>
	4. Elija Siguiente.
	5. En Nombre de política, escriba un nombre para la política de IAM. Este patrón usa el nombre ADO-policy.
	6. Elija Crear política.	

Tarea	Descripción	Habilidades requeridas
Cree un rol de IAM role en la Cuenta de AWS.	Para configurar un rol de IAM en Cuenta de AWS la conexión del servicio de Azure, siga estos pasos: 1. En la consola de IAM, en el panel izquierdo, elija Roles. 2. Elija Crear rol. 3. En Tipo de entidad de confianza, seleccione Identidad web. 4. Seleccione el IdP correcto del menú desplegable. El nombre del IdP comienza por `vstoken.dev.azure.com/{OrganizationGUID}` . 5. En la lista desplegable Audiencia, seleccione api: ADToken //Azure Exchange. 6. Para limitar este rol a una sola conexión de servicio, añada una condición. En Condición, seleccione Añadir condición y, en Clave, seleccione vstoken.dev.azure.com/{OrganizationGUID}:sub. En Condición, seleccione. StringEquals Para Valor, utilice el siguiente formato: `sc://{OrganizationName}/{Pr`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	ojectName}/{ServiceConnectionName} . Para ServiceConnectionName , utilice aws-sc. Creará esta conexión de servicio en la siguiente tarea. 7. Elija Siguiente. 8. En Añadir permisos, seleccione ADO-Policy, que es la política que creó en una tarea anterior. 9. Elija Siguiente y, para Nombre del rol, introduzca ado-role. En Seleccionar entidades de confianza, use la siguiente política de confianza: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Federated": "arn:aws:iam::{account_id}:oidc-provider/vstoken.dev.azure.com/{OrganizationGUID}" }, "Action": "sts:AssumeRoleWithWebIdentity",`	

Tarea	Descripción	Habilidades requeridas

	<pre>"Condition": {
	"StringEquals":
	{
	"vstoken.
	dev.azure.com/{Org
	anizationGUID}:aud
	": "api://AzureADToke
	nExchange",
	"vstoken.
	dev.azure.com/{Org
	anizationGUID}:sub
	": "sc://{Organizatio
	nName}/{ProjectNam
	e}/{ServiceConnect
	ionName}"
	}
	}
	}
	]
	}</pre> En la política, proporcione su información para los siguientes marcadores de posición:
	• `{account_id}` - Cuenta de AWS ID
	• `{OrganizationGUID}` - GUID de DevOps organización de Azure
	• `{OrganizationName}` - Nombre de la DevOps organización de Azure
	• `{ProjectName}` - Nombre DevOps del proyecto de Azure	

Tarea	Descripción	Habilidades requeridas
	• `{ServiceConnection Name}` - Nombre de la conexión DevOps al servicio de Azure. Utilice aws-sc. Creará esta conexión de servicio en la siguiente tarea.	

Tarea	Descripción	Habilidades requeridas
Cree una conexión de servicio en la DevOps cuenta de Azure.	Para configurar una conexión de servicio de Azure, siga estos pasos: 1. En su DevOps proyecto de Azure, seleccione Configuración del proyecto y Conexiones de servicio. 2. Elija Nueva conexión de servicio, seleccione el tipo de conexión de servicio como aws y, a continuación, seleccione Siguiente. 3. En Rol que se va a asumir, introduzca el ARN para el rol de IAM ado-role. Creó el ado-role en la tarea anterior Cree un rol de IAM en la Cuenta de AWS. 4. Seleccione la casilla de verificación Usar OIDC. 5. En Nombre de la conexión de servicio, introduzca aws-sc en las propiedades de la tarea. 6. Seleccione Save. Para obtener más información, consulte Crear una conexión de servicio en la documentación de Microsoft.	AWS DevOps

Tarea	Descripción	Habilidades requeridas

Añada el rol de IAM al archivo de configuración de Amazon EKS.	El rol de IAM debe tener permisos para realizar las operaciones requeridas en el clúster de Amazon EKS. Como se trata de un rol de canalización, el rol de IAM debe poder administrar casi todos los tipos de recursos del clúster. Por lo tanto, el permiso de grupo `system:masters` es adecuado para este rol.
	
	Para añadir la configuración necesaria al `aws-auth ConfigMap` en Kubernetes, use el siguiente código:
	
	`- groups:`
	`  - system:masters`
	`  rolearn: arn:aws:iam::{account_id}:role/ADO-role`
	`  username: ADO-role`
	
	`{account_id}` Sustitúyalo por su Cuenta de AWS ID.
	
	Para obtener más información, consulte la sección sobre cómo funciona Amazon EKS con IAM en la documentación de Amazon EKS.
		AWS DevOps

Creación de un grupo de agentes

Tarea	Descripción	Habilidades requeridas
Cree un grupo de agentes autoalojado.	Para configurar un grupo de agentes autohospedados en la DevOps cuenta de Azure, siga estos pasos: 1. Inicie sesión en la organización de su DevOps cuenta de Azure. 2. Elija Azure DevOps Organization. 3. Elija su DevOps proyecto de Azure. 4. Seleccione Configuración del proyecto. 5. Elija Grupos de agentes. 6. Elija Añadir grupo. 7. Seleccione Autoalojado. 8. En Nombre, escriba eks-agent. 9. Seleccione la casilla de verificación Conceder permiso de acceso a todas las canalizaciones. 10. Seleccione Crear. Para obtener más información, consulte Crear y administrar grupos de agentes en la documentación de Microsoft.	

Cree una imagen de DevOps agente de Azure y envíela a Amazon ECR

Tarea	Descripción	Habilidades requeridas
Cree un repositorio de Amazon ECR.	Las imágenes de Docker que se utilizan para implementar el DevOps agente de Azure y la aplicación de muestra (`webapp`) en el clúster privado de Amazon EKS deben almacenarse en un repositorio de Amazon ECR. Para crear un repositorio de Amazon ECR, complete los pasos siguientes. 1. Abra la consola Amazon ECR en los https://console.aws.amazon.com/ecr/repositorios. 2. En la barra de navegación, elija la Región de AWS en la que va a crear el repositorio. 3. En la página Repositorios, elija Repositorios privados y, a continuación, Crear repositorio. 4. En el nombre del repositorio, introduzca webapp. Para que la aplicación de ejemplo de este patrón funcione, el nombre del repositorio de Amazon ECR debe usar webapp. Si utiliza un nombre diferente	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	para el repositorio, consulte Solución de problemas. Para obtener más información, consulte Creación de un repositorio privado de Amazon ECR para almacenar imágenes en la documentación de Amazon ECR.	

Tarea	Descripción	Habilidades requeridas

Cree un Dockerfile para crear el agente de Azure DevOps .	Cree un Dockerfile para crear la imagen de Docker que tiene instalado el agente de Azure. DevOps Almacene el siguiente contenido en un archivo denominado `Dockerfile` :
	
	`FROM ubuntu:22.04`
	`ENV TARGETARCH="linux-x64"`
	`RUN apt update && apt upgrade -y && apt install -y curl git jq libicu70 unzip wget`
	
	`RUN curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"`
	`RUN unzip awscliv2.zip`
	`RUN ./aws/install`
	`RUN rm -rf aws awscliv2.zip`
	
	`RUN curl -sSL https://get.docker.com/ | sh`
	
	`RUN curl -sL https://aka.ms/InstallAzureCLIDeb | bash`
	`RUN mkdir -p azp`
	`WORKDIR /azp/`
	
	`COPY ./start.sh ./`
	`RUN chmod +x ./start.sh`
	
	`RUN useradd -m -d /home/agent agent`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`RUN chown -R agent:agent /azp /home/agent`
	`RUN groupadd -f docker`
	`RUN usermod -aG docker agent`
	`USER agent`
	
	`ENTRYPOINT [ "./start.sh" ]`	

Cree un script para el DevOps agente de Azure.	Para crear el script `start.sh`, siga estos pasos: 1. Vaya al procedimiento Crear y compilar el Dockerfile en la documentación de Microsoft y desplácese hasta el paso 5. Guarde el siguiente contenido `~/azp-agent-in-docker/start.sh` , de forma que se asegure de utilizar finales de línea de estilo Unix (LF). 2. Copie el contenido del script y guárdelo en un archivo denominado `start.sh` en el mismo directorio que el Dockerfile.	AWS DevOps

Tarea	Descripción	Habilidades requeridas

Cree una imagen de Docker con el DevOps agente de Azure.	Para crear una imagen de Docker para instalar el DevOps agente de Azure, utilice el Dockerfile que creó anteriormente para crear la imagen. En el mismo directorio en el que almacenó el Dockerfile, ejecute el comando siguiente.
	`aws ecr get-login-password --region region | docker login --username AWS --password-stdin aws_account_id.dkr.ecr.region.amazonaws.com`
	`docker build --platform linux/amd64 -t ado-agent:latest .`
	`docker tag ado-agent:latest aws_account_id.dkr.ecr.region.amazonaws.com/webapp:latest`
	`docker push aws_account_id.dkr.ecr.region.amazonaws.com/webapp:latest`
	Sustituya `aws_account_id` y por su `region` Cuenta de AWS ID y. Región de AWS
		AWS DevOps

Implemente el DevOps agente de Azure en un clúster privado de Amazon EKS

Tarea	Descripción	Habilidades requeridas
Genere un token de acceso personal de Azure.	El agente que se ejecuta en el clúster privado de Amazon EKS necesita un token de acceso personal (PAT) para poder autenticarse con la DevOps cuenta de Azure. Para generar un PAT, siga estos pasos: 1. Inicie sesión con la cuenta de usuario que planea usar en su DevOps organización de Azure (`https://dev.azure.com/{Your_Organization}`). 1. En la página de inicio, abra la configuración de usuario y, a continuación, seleccione Tokens de acceso personal. 2. Elija Nuevo token. 3. Ingrese un nombre para el token. 4. Seleccione Mostrar todos los ámbitos. 5. En el caso de los grupos de agentes, seleccione la casilla de verificación Leer y administrar. 6. Seleccione Crear.	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	7. Para crear un secreto en el clúster privado de Amazon EKS, utilice la siguiente configuración:
	
	`apiVersion: v1`
	`kind: Secret`
	`metadata:`
	`  name: azdevops-pat`
	`  namespace: default`
	`type: Opaque`
	`stringData:`
	`  AZP_TOKEN: <PAT Token>`
	
	1. Almacene la configuración en un archivo denominado `ado-secret.yaml` . Sustituya `<PAT Token>` por el token de acceso personal que acaba de crear. Para crear el secreto, ejecute el siguiente comando:
	
	`kubectl create -f ado-secret.yaml`
	
	Para obtener más información, consulte Registrar un agente mediante un token de acceso personal (PAT) en la documentación de Microsoft.	

Tarea	Descripción	Habilidades requeridas

Use el archivo de manifiesto de Kubernetes para la implementación del agente.	Para implementar el DevOps agente de Azure en el clúster privado de Amazon EKS, copie el siguiente archivo de manifiesto y guárdelo como `agent-deployment.yaml` :
	
	`apiVersion: apps/v1`
	`kind: Deployment`
	`metadata:`
	`  name: azure-pipelines-agent-eks`
	`  labels:`
	`  app: azure-pipelines-agent`
	`spec:`
	`  replicas: 1`
	`  selector:`
	`  matchLabels:`
	`  app: azure-pipelines-agent`
	`  template:`
	`  metadata:`
	`  labels:`
	`  app: azure-pipelines-agent`
	`  spec:`
	`  containers:`
	`  - name: docker`
	`  image: docker:dind`
	`  securityContext:`
	`  privileged: true`
	`  volumeMounts:`
	`  - name: shared-workspace`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	mountPath: /workspace - name: dind-storage mountPath: /var/lib/docker env: - name: DOCKER_TLS_CERTDIR value: "" - name: azure-pipelines-agent image: aws_account_id.dkr.ecr.region.amazonaws.com/webapp:latest env: - name: AZP_URL value: "<Azure account URL>" - name: AZP_POOL value: "eks-agent" - name: AZP_TOKEN valueFrom: secretKeyRef: name: azdevops-pat key: AZP_TOKEN - name: AZP_AGENT_NAME valueFrom: fieldRef: fieldPath: metadata.name - name: DOCKER_HOST value: tcp://localhost:2375	

Tarea	Descripción	Habilidades requeridas

	<pre>volumeMounts:
	- mountPath: /workspace
	name: shared-workspace
	volumes:
	- name: dind-storage
	emptyDir: {}
	- name: shared-workspace
	emptyDir: {}</pre>
	Sustituya `aws_account_id` y `<Azure account URL>` por su Cuenta de AWS ID y la URL de su DevOps cuenta de Azure.	

Implemente el agente en el clúster privado de Amazon EKS.	Para implementar el agente de Azure DevOps en el clúster privado de Amazon EKS, use el siguiente comando: `kubectl create -f agent-deployment.tf`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

Compruebe que el agente se está ejecutando.	Para comprobar que el DevOps agente de Azure se está ejecutando, utilice el siguiente comando:
	`kubectl get deploy azure-pipelines-agent-eks`
	La salida debería tener un aspecto similar al siguiente:
	`NAME READY UP-TO-DATE AVAILABLE AGE azure-pipelines-agent-eks 1/1 1 1 58s`
	Asegúrese de que la columna `READY` muestre `1/1`.
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
Compruebe que el agente esté registrado en el grupo de DevOps agentes de Azure.	Para comprobar que el agente está implementado en el clúster privado de Amazon EKS y registrado en el grupo de agentes `eks-agent` , siga estos pasos: 1. Inicie sesión en su DevOps organización de Azure (`https://dev.azure.com/{Your_Organization}`). 2. Seleccione Configuración del proyecto. 3. Elija Grupos de agentes. 4. Seleccione el grupo eks-agent y, a continuación, consulte la pestaña Agentes. Debería ver un agente en la lista con el estado en línea y el nombre del agente debería empezar por azure-pipelines-agent-eks-*.	AWS DevOps

Implementación de la aplicación de ejemplo

Tarea	Descripción	Habilidades requeridas
Transfiera el repositorio de aplicaciones de muestra a su GitHub cuenta.	Transfiera el siguiente repositorio de AWS muestras a su GitHub cuenta:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	https://github.com/aws-samples/deploy-kubernetes-resources-to- amazon-eks-using-azure -devops	

Tarea	Descripción	Habilidades requeridas
Crear una canalización.	Para crear una canalización en su DevOps cuenta de Azure, siga estos pasos: 1. Inicie sesión con la cuenta de usuario que planea usar en su DevOps organización de Azure (`https://dev.azure.com/{Your_Organization}`). 2. Vaya a la consola de proyectos y canalizaciones. 3. Elija Nueva canalización. 4. En Dónde está su código, elija GitHub. 5. Proporciona las credenciales necesarias para que la canalización se conecte a tu GitHub cuenta 6. Selecciona el repositorio deploy-kubernetes-resources-to: amazon-eks-using-azure -devops. 7. En Configurar su canalización, seleccione el archivo YAML de Azure Pipelines existente. 8. En Seleccionar un archivo YAML existente, seleccione main para Ramificación y azure_pipelines.yaml para ruta. 9. Elija Continuar.	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	10 En Revisar la canalización YAML, sustituya los valores de los parámetros de entrada `awsRegion` y `awsEKSClusterName` por tu información:
	
	`pool:`
	`  name: eks-agent`
	`#pool: self-hosted # If you are running self-hosted Azure DevOps Agents`
	
	`stages:`
	`# Refering the pipeline template, input parameter that are not specified will be added with defaults`
	`- template: ./pipeline_templates/main_template.yaml`
	`  parameters:`
	`  serviceConnectionName: aws-sc`
	`  awsRegion: <your region>`
	`  awsEKSClusterName: <name of your EKS cluster>`
	`  projectName: webapp`
	
	1. Seleccione EJECUTAR.	

Tarea	Descripción	Habilidades requeridas
Verifique que la aplicación de muestra se ha implementado.	Una vez finalizada la canalización, compruebe que la implementación de la aplicación de muestra se ha realizado correctamente; para ello, consulte tanto el repositorio de Amazon ECR como el clúster de Amazon EKS. Para verificar los artefactos en el repositorio de Amazon ECR, siga estos pasos: 1. Vaya al repositorio `webapp` de Amazon ECR. 2. Confirme la presencia de los siguientes artefactos nuevos: • Imagen de Docker: `<date>.<build_number>-image` • Gráfico de Helm: `<date>.<build_number>-helm` Por ejemplo, `20250501.1-image` y `20250501.1-helm`. Para verificar la implementación en el clúster privado de Amazon EKS del espacio	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	de nombres `webapp`, use el siguiente comando:
	`kubectl get deploy -n webapp`
	El resultado esperado es el siguiente:
	`NAME READY UP-TO-DATE AVAILABLE`
	`webapp 1/1 1 1`
	Nota: Si esta es la primera vez que ejecuta una canalización, es posible que deba autorizar la conexión del servicio y el grupo de agentes. Busque las solicitudes de permiso en la interfaz de DevOps canalización de Azure y apruebelas para continuar.	

Resolución de problemas

Problema	Solución
La canalización falla cuando el nombre del repositorio de Amazon ECR no coincide con `webapp`	La aplicación de ejemplo espera que el nombre del repositorio de Amazon ECR coincida con el parámetro `projectName: webapp` en `azure_pipeline.yml` .

Problema	Solución
	Para resolver este problema, cambie el nombre de su repositorio de Amazon ECR a `webapp` o actualice lo siguiente: • Cambie el nombre del `webapp` directorio de su repositorio bifurcado para que coincida con el nombre de su GitHub repositorio de Amazon ECR. • Actualice el parámetro `projectName` en `azure_pipeline.yml` para que coincida con el nombre de su repositorio de Amazon ECR.
Error: Kubernetes cluster unreachable: the server has asked for the client to provide credentials	Si encuentra este error en el paso “Extraer e implementar gráfico de Helm” de su canalizac ión de Azure, la causa principal suele deberse a una configuración incorrecta de los roles de IAM en el `aws-auth ConfigMap` del clúster de Amazon EKS. Para resolver este problema, compruebe lo siguiente: • Verifique la configuración de `aws-auth ConfigMap` . • Compruebe la configuración de autentica ción de su clúster de Amazon EKS: abra la consola de Amazon EKS, los detalles del clúster y la configuración de acceso. Asegúrese de que el modo de autentica ción esté configurado en la API de EKS y ConfigMap (no solo en la API de EKS).

Recursos relacionados

AWS Blogs

- Cómo federarse AWS desde Azure DevOps mediante OpenID Connect

Servicios de AWS documentación

- Amazon ECR
- Amazon EKS

Documentación de Microsoft

- ¿Qué es Azure DevOps?
- ¿Qué es Azure Pipelines?

Ejecución de consultas SQL en Amazon Redshift mediante Terraform

Sylvia Qi y Aditya Ambati, Amazon Web Services

Resumen

El uso de la infraestructura como código (IaC) para la implementación y la administración de Amazon Redshift es una práctica habitual en el país. DevOps La IaC facilita la implementación y la configuración de varios recursos de Amazon Redshift, como clústeres, instantáneas y grupos de parámetros. Sin embargo, la IaC no se extiende a la administración de los recursos de las bases de datos, como tablas, esquemas, vistas y procedimientos almacenados. Estos elementos de la base de datos se administran mediante consultas SQL y las herramientas de IaC no los admiten directamente. Si bien existen soluciones y herramientas para administrar estos recursos, es posible que prefiera no introducir herramientas adicionales en su conjunto de tecnologías.

Este patrón describe una metodología que utiliza Terraform para implementar los recursos de bases de datos de Amazon Redshift, incluidas tablas, esquemas, vistas y procedimientos almacenados. El patrón distingue entre dos tipos de consultas SQL:

- Consultas no repetibles: estas consultas se ejecutan una vez durante la implementación inicial de Amazon Redshift para establecer los componentes esenciales de la base de datos.
- Consultas repetibles: estas consultas son inmutables y se pueden volver a ejecutar sin que ello afecte a la base de datos. La solución usa Terraform para supervisar los cambios en las consultas repetibles y aplicarlos en consecuencia.

Para obtener más información, consulte el tutorial de la solución en Información adicional.

Requisitos previos y limitaciones

Requisitos previos

Debe tener una máquina de implementación activa Cuenta de AWS e instalar lo siguiente:

- AWS Command Line Interface (AWS CLI)
- Un AWS CLI perfil configurado con permisos de Amazon Redshift read/write
- La versión 1.6.2 o posterior de Terraform
- Python 3
- Boto3

Limitaciones

- Esta solución admite una única base de datos de Amazon Redshift porque Terraform solo permite la creación de una base de datos durante la creación del clúster.
- Este patrón no incluye pruebas para validar los cambios en las consultas repetibles antes de aplicarlos. Le recomendamos que incorpore dichas pruebas para mejorar la fiabilidad.
- Para ilustrar la solución, este patrón proporciona un archivo `redshift.tf` de muestra que utiliza un archivo de estado local de Terraform. Sin embargo, para los entornos de producción, le recomendamos encarecidamente que utilice un archivo de estado remoto con un mecanismo de bloqueo para mejorar la estabilidad y la colaboración.
- Algunos Servicios de AWS no están disponibles en todos. Regiones de AWS Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

Esta solución se ha desarrollado y probado en el parche 179 de Amazon Redshift.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub amazon-redshift-sql-deploy-terraform.

Arquitectura

El siguiente diagrama ilustra cómo Terraform administra los recursos de la base de datos de Amazon Redshift gestionando consultas SQL repetibles y no repetibles.

En el diagrama se muestran los siguientes pasos:

1. Terraform aplica consultas SQL no repetibles durante la implementación inicial del clúster de Amazon Redshift.
2. El desarrollador confirma los cambios en las consultas SQL repetibles.
3. Terraform supervisa los cambios en las consultas SQL repetibles.
4. Terraform aplica consultas SQL repetibles a la base de datos de Amazon Redshift.

La solución que proporciona este patrón se basa en el módulo de Terraform para Amazon Redshift. El módulo de Terraform aprovisiona un clúster y una base de datos de Amazon Redshift. Para mejorar el módulo, utilizamos `terraform_data` resources, que invoca un script de Python personalizado para ejecutar consultas SQL mediante la operación de la API Amazon ExecuteStatementRedshift. En consecuencia, el módulo puede hacer lo siguiente:

- Implemente cualquier cantidad de recursos de base de datos mediante consultas SQL después de aprovisionar la base de datos.
- Supervise continuamente los cambios en las consultas SQL repetibles y aplique esos cambios con Terraform.

Para obtener más información, consulte el tutorial de la solución en Información adicional.

Tools (Herramientas)

Servicios de AWS

- Amazon Redshift es un servicio de almacén de datos completamente administrado que opera a escala de petabytes en la Nube de AWS.

Otras herramientas

- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.
- Python es un lenguaje de programación de uso general que se utiliza en este patrón para ejecutar consultas SQL.

Prácticas recomendadas

- Prácticas recomendadas de Amazon Redshift
- Uso de la API de datos de Amazon Redshift para interactuar con los clústeres de Amazon Redshift

Epics

Implementaci´n de la solución mediante Terraform

Tarea	Descripción	Habilidades requeridas
Clone el repositorio.	Para clonar el repositorio de Git que contiene el código de Terraform para aprovisionar un clúster de Amazon Redshift, utilice el siguiente comando. `git clone https://github.com/aws-samples/amazon-redshift-sql-deploy-terraform.git`	DevOps ingeniero

Actualice las variables de Terraform.	Para personalizar la implementación del clúster de Amazon Redshift de acuerdo con sus requisitos específicos, actualice los siguientes parámetros del archivo `terraform.tfvars` .
	`region = "<AWS_REGION>"`
	`cluster_identifier = "<REDSHIFT_CLUSTER_IDENTIFIER>"`
	`node_type = "<REDSHIFT_NODE_TYPE>"`
	`number_of_nodes = "<REDSHIFT_NODE_COUNT>"`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	database_name = "<REDSHIFT_DB_NAME>" subnet_ids = "<REDSHIFT_SUBNET_IDS>" vpc_security_group_ids = "<REDSHIFT_SECURITY_GROUP_IDS>" run_nonrepeatable_queries = true run_repeatable_queries = true sql_path_bootstrap = "<BOOTSTRAP_SQLS_PATH>" sql_path_nonrepeatable = "<NON-REPEATABLE_SQLS_PATH>" sql_path_repeatable = "<REPEATABLE_SQLS_PATH>" sql_path_finalize = "<FINALIZE_SQLS_PATH>" create_random_password = false master_username = "<REDSHIFT_MASTER_USERNAME>"	

Tarea	Descripción	Habilidades requeridas

Implemente los recursos con Terraform.	1. Para preparar el proceso de implementación, use el siguiente comando para inicializar Terraform en el repositorio clonado.
	`terraform init`
	2. Para obtener una vista previa de los cambios que Terraform aplicará a la infraestructura, utilice el siguiente comando para crear un plan de ejecución.
	`terraform plan -var-file terraform.tfvars`
	3. Para aprovisionar el clúster de Amazon Redshift y los recursos asociados, utilice el siguiente comando para aplicar el plan de ejecución de Terraform.
	`terraform apply -var-file terraform.tfvars`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

(Opcional) Ejecute consultas SQL adicionales.	El repositorio de ejemplos proporciona varias consultas SQL con fines de demostración. Para ejecutar sus propias consultas SQL, agréguelas a las siguientes carpetas:
	`/bootstrap`
	`/nonrepeatable`
	`/repeatable`
	`/finalize`	

Supervisión de la ejecución de instrucciones SQL

Tarea	Descripción	Habilidades requeridas
Supervise la implementación de las instrucciones SQL.	Puede supervisar los resultados de las ejecuciones de SQL en un clúster de Amazon Redshift. Para ver ejemplos de resultados que muestran una ejecución de SQL fallida y correcta, consulte Ejemplos de instrucciones SQL en Información adicional.	DBA, ingeniero DevOps
Eliminación de recursos.	Para eliminar todos los recursos implementados por Terraform, ejecute el siguiente comando.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`terraform destroy`	

Validación de los resultados

Tarea	Descripción	Habilidades requeridas
Valide los datos en el clúster de Amazon Redshift.	1. Inicie sesión en la consola Consola de administr ación de AWS de Amazon Redshift y ábrala. 2. En el menú de navegació n, elija Clusters (Clústeres). Elija el nombre del clúster relevante en la lista. 3. Siga las instrucciones de Consulta de una base de datos mediante el editor de consultas V2 de Amazon Redshift en la documenta ción de Amazon Redshift.	ADMINISTRADOR DE BASES DE DATOS, AWS DevOps

Recursos relacionados

AWS documentación

- Clústeres aprovisionados por Amazon Redshift
- Solución de problemas de la API de datos de Amazon Redshift

Otros recursos

- Comando: apply(documentación de Terraform)

Información adicional

Tutorial de la solución

Para usar la solución, debe organizar las consultas SQL de Amazon Redshift de una manera específica. Todas las consultas SQL deben almacenarse en archivos con una extensión `.sql`.

En el ejemplo de código que se proporciona con este patrón, las consultas SQL se organizan en la siguiente estructura de carpetas. Puede modificar el código (`sql-queries.tf` y `sql-queries.py`) para que funcione con cualquier estructura que se adapte a su caso de uso exclusivo.

```
/bootstrap
     |- Any # of files
     |- Any # of sub-folders
/nonrepeatable
     |- Any # of files
     |- Any # of sub-folders
/repeatable
     /udf
          |- Any # of files
          |- Any # of sub-folders
     /table
          |- Any # of files
          |- Any # of sub-folders
     /view
          |- Any # of files
          |- Any # of sub-folders
     /stored-procedure
          |- Any # of files
          |- Any # of sub-folders
/finalize
     |- Any # of files
     |- Any # of sub-folders
```

Dada la estructura de carpetas anterior, durante la implementación del clúster de Amazon Redshift, Terraform ejecuta las consultas en el siguiente orden:

1. `/bootstrap`
2. `/nonrepeatable`
3. `/repeatable`
4. `/finalize`

La carpeta `/repeatable` contiene las subcarpetas `/udf`, `/table`, `/view` y `/stored-procedure`. Estas subcarpetas indican el orden en el que Terraform ejecuta las consultas SQL.

El script de Python que ejecuta las consultas SQL es `sql-queries.py`. En primer lugar, el script lee todos los archivos y subcarpetas de un directorio fuente específico, por ejemplo, el parámetro `sql_path_bootstrap`. A continuación, el script ejecuta las consultas mediante una llamada a la operación de la API Amazon ExecuteStatementRedshift. Es posible que tenga una o más consultas SQL en un archivo. El siguiente fragmento de código muestra la función de Python que ejecuta instrucciones SQL almacenadas en un archivo en un clúster de Amazon Redshift.

```
def execute_sql_statement(filename, cluster_id, db_name, secret_arn, aws_region):
    """Execute SQL statements in a file"""
    redshift_client = boto3.client(
        'redshift-data', region_name=aws_region)
    contents = get_contents_from_file(filename),
    response = redshift_client.execute_statement(
        Sql=contents[0],
        ClusterIdentifier=cluster_id,
        Database=db_name,
        WithEvent=True,
        StatementName=filename,
        SecretArn=secret_arn
    )
    ...
```

El script `sql-queries.tf` de Terraform crea los recursos terraform_data que invocan el script `sql-queries.py`. Hay un recurso `terraform_data` para cada una de las cuatro carpetas: `/bootstrap`, `/nonrepeatable`, `/repeatable` y `/finalize`. El siguiente fragmento de código muestra el recurso `terraform_data` que ejecuta las consultas SQL de la carpeta `/bootstrap`.

```
locals {
  program               = "${path.module}/sql-queries.py"
  redshift_cluster_name = try(aws_redshift_cluster.this[0].id, null)
}

resource "terraform_data" "run_bootstrap_queries" {
  count      = var.create && var.run_nonrepeatable_queries && (var.sql_path_bootstrap !
= "") && (var.snapshot_identifier == null) ? 1 : 0
  depends_on = [aws_redshift_cluster.this[0]]

  provisioner "local-exec" {
```

```
    command = "python3 ${local.program} ${var.sql_path_bootstrap}
 ${local.redshift_cluster_name} ${var.database_name} ${var.redshift_secret_arn}
 ${local.aws_region}"
  }
}
```

Puede controlar si desea ejecutar estas consultas mediante las siguientes variables. Si no desea ejecutar consultas en`sql_path_bootstrap`, `sql_path_nonrepeatable`, `sql_path_repeatable` o `sql_path_finalize`, establezca sus valores en `""`.

```
  run_nonrepeatable_queries = true
  run_repeatable_queries    = true
  sql_path_bootstrap        = "src/redshift/bootstrap"
  sql_path_nonrepeatable    = "src/redshift/nonrepeatable"
  sql_path_repeatable       = "src/redshift/repeatable"
  sql_path_finalize         = "src/redshift/finalize"
```

Cuando se ejecuta `terraform apply`, Terraform tiene en cuenta el recurso `terraform_data` agregado una vez que se ha completado el script, independientemente de los resultados del script. Si algunas consultas de SQL fallaron y desea volver a ejecutarlas, puede eliminar manualmente el recurso del estado de Terraform y volver a ejecuta `terraform apply`. Por ejemplo, el siguiente comando elimina el recurso `run_bootstrap_queries` del estado de Terraform.

```
terraform state rm module.redshift.terraform_data.run_bootstrap_queries[0]
```

El siguiente ejemplo de código muestra cómo el recurso `run_repeatable_queries` supervisa los cambios en la carpeta `repeatable` mediante el hash sha256. Si se actualiza algún archivo de la carpeta, Terraform marca todo el directorio para actualizarlo. Luego, Terraform vuelve a ejecutar las consultas en el directorio durante la siguiente `terraform apply`.

```
resource "terraform_data" "run_repeatable_queries" {
  count      = var.create_redshift && var.run_repeatable_queries &&
 (var.sql_path_repeatable != "") ? 1 : 0
  depends_on = [terraform_data.run_nonrepeatable_queries]

  # Continuously monitor and apply changes in the repeatable folder
  triggers_replace = {
    dir_sha256 = sha256(join("", [for f in fileset("${var.sql_path_repeatable}",
 "**") : filesha256("${var.sql_path_repeatable}/${f}")]))
  }
```

```
  provisioner "local-exec" {
    command = "python3 ${local.sql_queries} ${var.sql_path_repeatable}
 ${local.redshift_cluster_name} ${var.database_name} ${var.redshift_secret_arn}"
  }
}
```

Para refinar el código, puede implementar un mecanismo que detecte y aplique los cambios solo a los archivos que se hayan actualizado dentro de la carpeta `repeatable`, en lugar de aplicarlos a todos los archivos de forma indiscriminada.

Ejemplos de instrucciones SQL

El siguiente resultado muestra una ejecución fallida de SQL, junto con un mensaje de error.

```
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): Executing:
 ["/bin/sh" "-c" "python3 modules/redshift/sql-queries.py src/redshift/nonrepeatable
 testcluster-1 db1 arn:aws:secretsmanager:us-east-1:XXXXXXXXXXXX:secret:/redshift/
master_user/password-8RapGH us-east-1"]
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec):
 ----------------------------------------------------------------
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): src/redshift/
nonrepeatable/table/admin/admin.application_family.sql
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec):
 ----------------------------------------------------------------
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): Status:
 FAILED
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): SQL execution
 failed.
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): Error
 message: ERROR: syntax error at or near ")"
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec):   Position:
 244
module.redshift.terraform_data.run_nonrepeatable_queries[0]: Creation complete after 3s
 [id=ee50ba6c-11ae-5b64-7e2f-86fd8caa8b76]
```

El siguiente resultado muestra una ejecución correcta de SQL.

```
module.redshift.terraform_data.run_bootstrap_queries[0]: Provisioning with 'local-
exec'...
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec): Executing:
 ["/bin/sh" "-c" "python3 modules/redshift/sql-queries.py src/redshift/bootstrap
 testcluster-1 db1 arn:aws:secretsmanager:us-east-1:XXXXXXXXXXXX:secret:/redshift/
master_user/password-8RapGH us-east-1"]
```

```
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec):
 ----------------------------------------------------------------------
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec): src/redshift/
bootstrap/db.sql
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec):
 ----------------------------------------------------------------------
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec): Status: FINISHED
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec): SQL execution
 successful.
module.redshift.terraform_data.run_bootstrap_queries[0]: Creation complete after 2s
 [id=d565ef6d-be86-8afd-8e90-111e5ea4a1be]
```

Exportación de etiquetas para una lista de instancias de Amazon EC2 a un archivo CSV

Sida Ju y Pac Joonhyun, Amazon Web Services

Resumen

Este patrón muestra cómo exportar mediante programación las etiquetas de una lista de instancias de Amazon Elastic Compute Cloud (Amazon EC2) a un archivo CSV.

Con el ejemplo de script de Python que se proporciona, puede reducir el tiempo que se tarda en revisar y clasificar las instancias de Amazon EC2 por etiquetas específicas. Por ejemplo, puede usar el script para identificar y categorizar rápidamente una lista de instancias que su equipo de seguridad ha marcado como actualizaciones de software.

Requisitos previos y limitaciones

Requisitos previos

- Python 3 instalado y configurado
- AWS Command Line Interface (AWS CLI) instalado y configurado

Limitaciones

El script de Python de ejemplo que se proporciona en este patrón puede buscar instancias de Amazon EC2 basándose únicamente en los siguientes atributos:

- Instancia IDs
- IPv4 Direcciones privadas
- IPv4 Direcciones públicas

Tools (Herramientas)

Servicios de AWS

- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos.

Otras herramientas

- Python es un lenguaje de programación informático de uso general.
- virtualenv le ayuda a crear entornos Python aislados.

Repositorio de código

El script Python de ejemplo para este patrón está disponible en el repositorio GitHub search-ec2 -. instances-export-tags

Epics

Instalar y configurar los requisitos previos

Tarea	Descripción	Habilidades requeridas
Clona el repositorio. GitHub	**Note** Si recibes errores al ejecutar AWS CLI comandos, asegúrate de usar la AWS CLI versión más reciente. Clona el instances-export-tags repositorio GitHub search-ec2- ejecutando el siguiente comando de Git en una ventana de terminal: `git clone https://github.com/aws-samples/search-ec2-instances-export-tags.git`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Instale y active virtualenv.	1. Instale virtualenv ejecutando el siguiente comando:
	`python3 -m pip install virtualenv`
	2. Cree un nuevo entorno virtual ejecutando el siguiente comando:
	`python3 -m venv env`
	3. Active el nuevo entorno virtual ejecutando el siguiente comando:
	`source env/bin/activate`
	Para obtener más información, consulte la documentación de virtualenv.
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Instale las dependencias.	1. Abra el directorio de código ejecutando el siguiente comando en el terminal:
	`cd search-ec2-instances-export-tags`
	2. Instale el archivo `requirements.txt` ejecutando el siguiente comando pip:
	`pip3 install -r requirements.txt`
		DevOps ingeniero

Configure un perfil con AWS nombre.	Si aún no lo ha hecho, configure un perfil con AWS nombre que incluya las credenciales necesarias para ejecutar el script. Para crear un perfil con nombre, ejecute el comando aws configure. Para obtener más información, consulte Uso de perfiles con nombre en la AWS CLI documentación.	DevOps ingeniero

Configurar y ejecutar el script de Python

Tarea	Descripción	Habilidades requeridas
Cree el archivo de entrada.	Cree un archivo de entrada que contenga una lista de las instancias de Amazon	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	EC2 para las que desea que el script busque y exporte etiquetas. Puede enumerar IPv4 direcciones de instancia IDs, privadas o públicas IPv4 .
	
	Important
	Asegúrese de que cada instancia de Amazon EC2 aparezca en su propia línea en el archivo de entrada.
	
	Ejemplo de archivo de entrada
	
	`i-0547c351bdfe85b9f`
	`54.157.194.156`
	`172.31.85.33`
	`54.165.198.144`
	`i-0b6223b5914111a4b`
	`172.31.85.44`
	`54.165.198.145`
	`172.31.80.219`
	`172.31.94.199`	

Tarea	Descripción	Habilidades requeridas
Ejecutar el script de Python .	Ejecute el siguiente comando en el terminal para ejecutar el siguiente comando: `python search_instances.py -i INPUTFILE -o OUTPUTFILE -r REGION [-p PROFILE]` **Note** Sustituya `INPUTFILE` por el nombre del archivo de entrada. Cambie `OUTPUTFILE` por el nombre que desea otorgar al archivo CSV resultante. `REGION`Sustitúyalo por el Región de AWS que se encuentra n sus recursos de Amazon EC2. Si utiliza un perfil con AWS nombre, `PROFILE` sustitúyalo por el perfil con nombre que está utilizando. Para obtener una lista de parámetros compatibles y su descripción, ejecute el siguiente comando:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`python search_instances.py -h` Para obtener más información y ver un ejemplo de archivo de salida, consulta el `README.md` archivo en el repositorio GitHub search-ec2-instances-export-tags	

Recursos relacionados

- Configuración de la AWS CLI (AWS CLI documentación)

Exportar los informes de AWS Backup de toda la organización en AWS Organizations como un archivo CSV

Aromal Raj Jayarajan y Purushotham G K, Amazon Web Services

Resumen

Este patrón muestra cómo exportar los informes de trabajos de AWS Backup de toda una organización en AWS Organizations como un archivo CSV. La solución utiliza AWS Lambda y Amazon EventBridge para clasificar los informes de trabajos de AWS Backup en función de su estado, lo que puede ayudar a configurar las automatizaciones basadas en el estado.

AWS Backup ayuda a las organizaciones a administrar y automatizar de forma centralizada la protección de datos en todos los servicios de AWS, en la nube y en las instalaciones. Sin embargo, para los trabajos de AWS Backup configurados en AWS Organizations, los informes consolidados solo están disponibles en la consola de administración de AWS de la cuenta de administración de cada organización. Sacar estos informes de la cuenta de administración puede reducir el esfuerzo necesario para la auditoría y aumentar el alcance de las automatizaciones, las notificaciones y las alertas.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una organización activa en AWS Organizations que incluye al menos una cuenta de administración y una cuenta de miembro
- AWS Backup configurado a nivel organizativo en AWS Organizations (para obtener más información, consulte Automate centralized backup at scale across AWS services using AWS Backup en el blog de AWS)
- Git, instalado y configurado en su equipo local

Limitaciones

La solución proporcionada en este patrón identifica los recursos de AWS que están configurados únicamente para trabajos de AWS Backup. El informe no puede identificar los recursos de AWS que no estén configurados para realizar copias de seguridad mediante AWS Backup.

Arquitectura

Pila de tecnología de destino

- AWS Backup
- AWS CloudFormation
- Amazon EventBridge
- AWS Lambda
- AWS Security Token Service (AWS STS)
- Amazon Simple Storage Service (Amazon S3)
- AWS Identity y Access Management (IAM)

Arquitectura de destino

El siguiente diagrama muestra un ejemplo de flujo de trabajo para exportar informes de trabajos de AWS Backup de toda una organización en AWS Organizations como un archivo CSV.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Una regla de EventBridge eventos programados invoca una función Lambda en la cuenta de AWS del miembro (informante).
2. A continuación, la función de Lambda utiliza AWS STS para asumir un rol de IAM que tiene los permisos necesarios para conectarse a la cuenta de administración.
3. La función de Lambda lleva a cabo lo siguiente:
   - Solicita el informe consolidado de trabajos de AWS Backup al servicio AWS Backup
   - Clasifica los resultados según el estado del trabajo de AWS Backup
   - Convertir la respuesta en un archivo CSV
   - Carga los resultados en un bucket de Amazon S3 de la cuenta de informes, dentro de carpetas etiquetadas según su fecha de creación.

Tools (Herramientas)

Herramientas

- AWS Backup es un servicio totalmente administrado que le ayuda a centralizar y automatizar la protección de datos en todos los servicios de AWS, en la nube y en las instalaciones.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, las funciones de AWS Lambda, los puntos de conexión de invocación HTTP que utilizan destinos de API o los buses de eventos de otras cuentas de AWS.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Código

El código de este patrón está disponible en el GitHub aws-backup-report-generatorrepositorio.

Prácticas recomendadas

- Prácticas recomendadas de seguridad para Amazon S3 (Guía del usuario de Amazon S3)
- Prácticas recomendadas para trabajar con las funciones de AWS Lambda (Guía para desarrolladores de AWS Lambda)
- Prácticas recomendadas para la cuenta de administración (Guía del usuario de AWS Organizations)

Epics

Implementar los componentes de la solución

Tarea	Descripción	Habilidades requeridas
Clona el GitHub repositorio.	Clone el GitHub aws-backup-report-generatorrepositorio ejecutando el siguiente comando en una ventana de terminal: `git clone https://github.com/aws-samples/aws-backup-report-generator.git` Para obtener más información, consulta Cómo clonar un repositorio en los GitHub documentos.	AWS DevOps, DevOps ingeniero
Implemente los componentes de la solución en la cuenta de AWS del miembro (informante).	1. En la cuenta de miembro (informante), inicie sesión en la consola de administración de AWS y, a continuación, abra la CloudFormation consola. 2. Elija Create stack (Crear pila), y, a continuación, elija With new resources (standard) (Con nuevos recursos [estándar]). 3. En la página Crear pila, en la sección Especificar plantilla, seleccione Cargar un archivo de plantilla.	DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	4. Seleccione Choose file (Elegir archivo). A continuación, vaya a la carpeta raíz del GitHub repositorio clonado en su estación de trabajo local y elija template-reporting.yaml. 5. Elija Abrir y, a continuación, elija Siguiente. 6. En la página Especificar los detalles de la pila, en Nombre de la pila, introduce un nombre para la pila. CloudFormation 7. En ManagementAccountID, introduzca el ID de la cuenta de AWS de la cuenta de administración de su organización en AWS Organizations. 8. Elija Siguiente. 9. En la página Configurar opciones de pila, elija Siguiente. 10. En la página de revisión, seleccione la casilla de verificación para confirmar que ha revisado la configuración. 11. Seleccione Creación de pila. La pila muestra el estado CREATE_COMPLETE cuando los	

Tarea	Descripción	Habilidades requeridas
	componentes de la solución se implementan en la cuenta del miembro (informante).	

Pruebe la solución

Tarea	Descripción	Habilidades requeridas
Asegúrese de que la EventBridge regla se ejecute antes de la prueba.	Asegúrese de que la EventBridge regla se ejecute esperando al menos 24 horas o aumentando la frecuencia de los informes en el archivo CloudFormation template-reporting.yml de la plantilla. Para aumentar la frecuencia de los informes 1. Abra el archivo template-reporting.yml en el repositorio clonado. 2. En la regla de eventos con el identificador lógico '', busque el 'LambdaSchedule'. ScheduleExpression 3. Edita la clave ScheduleExpression'' para que incluya una expresión cron válida. Por ejemplo, la siguiente expresión cron programa la regla de eventos para que se ejecute cada cinco	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	minutos: `"cron (* /5 * * * *)"`	
Consulte el bucket de Amazon S3 para ver el informe generado.	1. En la cuenta de miembro (informante), inicie sesión en la consola de administración de AWS y, a continuación, abra la CloudFormation consola. 2. En el panel Pilas, seleccione el nombre de la pila que creó. A continuación, elija la pestaña Recursos. 3. En el panel Recursos, en la columna ID lógica, busque BackupReportS3Bucket. A continuación, abra el bucket de Amazon S3 asociado en una pestaña nueva. Para ello, seleccione el enlace en la columna ID física situada junto a ese ID lógico. 4. <Mon><yyyy>Asegúrese de que el depósito contenga un informe generado en el siguiente formato: BackupReports//// BackupReport- - - - .csv <yyyy><mm><dd><BACKUP JOB STATUS><dd>	AWS DevOps, DevOps ingeniero

Eliminación de sus recursos

Tarea	Descripción	Habilidades requeridas
Elimine los componentes de la solución de la cuenta del miembro (informante).	1. En la cuenta del miembro (informante), abra el bucket de Amazon S3 de la solución. Para obtener instrucciones, consulte los pasos 2 a 4 de la historia Comprobar el bucket de S3 para ver el informe generado de la sección Probar la solución de este patrón. 2. Elimine el contenido del bucket y vacíelo. Para obtener instrucciones, consulte Vaciar un bucket en la Guía del usuario de Amazon S3. 3. En la cuenta de miembro (informante), inicie sesión en la consola de administración de AWS y, a continuación, abra la CloudFormation consola. 4. En el panel Pilas, seleccione la casilla de verificación situada junto al nombre de la pila que creó. A continuación, elija Eliminar.	AWS DevOps, DevOps ingeniero
Elimine los componentes de la solución de la cuenta de administración.	1. En la cuenta de administración, inicie sesión en la consola de administración	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	de AWS y, a continuación, abra la CloudFormation consola. 2. En el panel Pilas, seleccione la casilla de verificación situada junto al nombre de la pila que creó. A continuación, elija Eliminar.	

Recursos relacionados

- Tutorial: Uso de AWS Lambda con eventos programados (documentación de AWS Lambda)
- Creación de eventos programados para ejecutar funciones de AWS Lambda (AWS SDK para obtener JavaScript documentación)
- Tutorial de IAM: delegue el acceso entre cuentas de AWS mediante roles de IAM (documentación de IAM)
- Terminología y conceptos de AWS Organizations (Guía del usuario de AWS Organizations)
- Creación de planes de informes mediante la consola de AWS Backup (Guía para desarrolladores de AWS Backup)
- Creación de un informe de auditoría (documentación de AWS Backup)
- Creación de informes bajo demanda (documentación de AWS Backup)
- ¿Qué es AWS Backup? (Documentación de AWS Backup)
- Automatización de las copias de seguridad centralizadas a escala en todos los servicios de AWS mediante AWS Backup (entrada en el blog de AWS)

Genere una CloudFormation plantilla de AWS que contenga las reglas administradas por AWS Config mediante Troposphere

Lucas Nation y Freddie Wilson, Amazon Web Services

Resumen

Muchas organizaciones utilizan las reglas administradas de AWS Config para evaluar la conformidad de sus recursos de Amazon Web Services (AWS) con respecto a las prácticas recomendadas habituales. Sin embargo, el mantenimiento de estas reglas puede llevar mucho tiempo y este patrón le ayuda a aprovechar Troposphere, una biblioteca de Python, para generar y administrar reglas administradas por AWS Config.

El patrón le ayuda a administrar las reglas administradas por AWS Config mediante un script de Python para convertir una hoja de cálculo de Microsoft Excel que contiene reglas administradas por AWS en una CloudFormation plantilla de AWS. Troposphere actúa como infraestructura como código (IaC), lo que significa que puede actualizar la hoja de cálculo de Excel con reglas administradas en lugar de utilizar un archivo con formato JSON o YAML. A continuación, utilice la plantilla para lanzar una CloudFormation pila de AWS que cree y actualice las reglas administradas en su cuenta de AWS.

La CloudFormation plantilla de AWS define cada regla gestionada por AWS Config mediante la hoja de cálculo de Excel y le ayuda a evitar la creación manual de reglas individuales en la consola de administración de AWS. El script establece de forma predeterminada los parámetros de cada regla administrada en un diccionario vacío y los `ComplianceResourceTypes` valores predeterminados del ámbito son. `THE_RULE_IDENTIFIER.template file` Para obtener más información sobre el identificador de la regla, consulte Creación de reglas administradas de AWS Config con CloudFormation plantillas de AWS en la documentación de AWS Config.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Familiaridad con el uso de CloudFormation plantillas de AWS para crear reglas administradas de AWS Config. Para obtener más información al respecto, consulte Creación de reglas administradas de AWS Config con CloudFormation plantillas de AWS en la documentación de AWS Config.
- Python 3, instalado y configurado. Para obtener más información, consulte la Documentación de Python.

- Un entorno de desarrollo integrado (IDE) existente.
- Identifique sus unidades organizativas (OUs) en una columna de la hoja de cálculo de `excel_config_rules.xlsx` Excel de muestra (adjunta).

Epics

Personalice y configure las reglas administradas de AWS Config

Tarea	Descripción	Habilidades requeridas
Actualice la hoja de cálculo de Excel de muestra.	Descargue la hoja de cálculo de Excel de muestra `excel_config_rules .xlsx` (adjunta) y etiquétela como `Implemented` con las reglas administradas de AWS Config que desee usar. Las reglas marcadas como se `Implemented` añadirán a la CloudFormation plantilla de AWS.	Desarrollador
(Opcional) Actualice el archivo config_rules_params.json con los parámetros de las reglas de AWS Config.	Algunas reglas administradas por AWS Config requieren parámetros y deben pasarse al script de Python como un archivo JSON mediante la opción `--param-file` . Por ejemplo, la regla administrada `access-keys-rotated` usa el siguiente parámetro `maxAccessKeyAge` : `{ "access-keys-rotated": {`	Desarrollador

Tarea	Descripción	Habilidades requeridas

	<pre>"InputPar
	ameters": {
	
	"maxAccessKeyAge": 90
	}
	}
	}</pre>
	En este parámetro de ejemplo, `maxAccessKeyAge` se establece en 90 días. El script lee el archivo de parámetros y añade cualquier `InputParameters` que encuentra.	

Tarea	Descripción	Habilidades requeridas
(Opcional) Actualice el archivo config_rules_params.json con AWS Config. ComplianceResourceTypes	De forma predeterminada, el script de Python recupera `ComplianceResourceTypes` de las plantillas definidas por AWS. Si desea anular el ámbito de una regla gestionada por AWS Config específica, debe pasarla al script de Python como un archivo JSON mediante la opción `--param-file` . Por ejemplo, el siguiente código de ejemplo muestra cómo el `ComplianceResourceTypes` para `ec2-volume-inuse-check` se establece en la lista `["AWS::EC2::Volume"]` : `{ "ec2-volume-inuse-check": { "Scope": { "ComplianceResourceTypes": [ "AWS::EC2::Volume" ] } } }`	Desarrollador

Ejecute el script de Python

Tarea	Descripción	Habilidades requeridas
Instalar los paquetes pip desde el archivo requirements.txt.	Descargue el archivo `requirements.txt` (adjunto) y ejecute el siguiente comando en su IDE para instalar los paquetes de Python: `pip3 install -r requirements.txt`	Desarrollador
Ejecutar el script de Python .	1. Descargue el archivo `aws_config_rules.py` (adjunto) en el equipo local. 2. **Note** Ejecute el comando `- python3 aws_config_rules.py --ou <OU_NAME>` . `--ou` define qué columna de UO elegir en la hoja de cálculo de Excel. También puede incluir los siguientes parámetros opcionales: • `--config-rule-option` : define las reglas a	Desarrollador

Tarea	Descripción	Habilidades requeridas
	elegir de la hoja de cálculo de Excel. El parámetro determinado es `Implemented` . • `--excel-file` : la ruta de la hoja de cálculo de Excel. El valor predeterminado es `aws_config_rules.xlsx` . • `--param-file` : la ruta del archivo JSON de parámetros. El valor predeterminado es `config_rules_params.json` . • `--max-execution-frequency` : define la frecuencia con la que se evalúan las reglas administradas de AWS Config. Las opciones son `One_Hour`, `Three_Hours` , `Six_Hours` , `Twelve_Hours` o `TwentyFour_Hours` . El valor predeterminado es `TwentyFour_Hours` .	

Implemente las reglas administradas en AWS Config

Tarea	Descripción	Habilidades requeridas
Lance la CloudFormation pila de AWS.	1. Inicie sesión en la consola de administración de AWS,	Desarrollador

Tarea	Descripción	Habilidades requeridas
	abra la CloudFormation consola de AWS y, a continuación, elija Create stack. 2. En la página Especificar plantilla, elija Cargar un archivo de plantilla y, a continuación, cargue su CloudFormation plantilla de AWS. 3. Especifique el nombre de la pila y elija Next (Siguiente). 4. Especifique las etiquetas y, a continuación, elija Next (Siguiente). 5. Seleccione Creación de pila.	

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Otorgue a las instancias de SageMaker notebook acceso temporal a un CodeCommit repositorio de otra cuenta de AWS

Helge Aufderheide, Amazon Web Services

Resumen

Este patrón muestra cómo conceder a las instancias de Amazon SageMaker Notebook y a los usuarios acceso temporal a un CodeCommit repositorio de AWS que se encuentra en otra cuenta de AWS. También indica cómo conceder permisos detallados para acciones específicas que cada entidad puede realizar en un repositorio.

Las organizaciones suelen almacenar CodeCommit los repositorios en una cuenta de AWS diferente a la cuenta que aloja su entorno de desarrollo. Esta configuración de múltiples cuentas ayuda a controlar el acceso a los repositorios y reduce el riesgo de que se eliminen accidentalmente. Para conceder estos permisos entre cuentas, se recomienda usar roles de AWS Identity and Access Management (IAM). Las identidades de IAM predefinidas en cada cuenta de AWS podrán asumir temporalmente los roles para crear una cadena de confianza controlada en todas las cuentas.

> **Note**
>
> Puede aplicar un procedimiento similar para conceder a otras identidades de IAM el acceso multicuenta a un repositorio. CodeCommit Para obtener más información, consulte Configurar el acceso multicuenta a un CodeCommit repositorio de AWS mediante roles en la Guía del CodeCommit usuario de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa con un CodeCommit repositorio (cuenta A)
- Una segunda cuenta de AWS activa con una instancia de SageMaker notebook (cuenta B)
- Un usuario de AWS con permisos suficientes para crear y modificar roles de IAM en la cuenta A
- Un segundo usuario de AWS con permisos suficientes para crear y modificar roles de IAM en la cuenta B

Arquitectura

En el siguiente diagrama se muestra un ejemplo de flujo de trabajo para conceder a una instancia de SageMaker Notebook y a los usuarios de una cuenta de AWS acceso multicuenta a un CodeCommit repositorio:

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El rol de usuario de AWS y el rol de instancia de SageMaker notebook en la cuenta B asumen un perfil con nombre.
2. La política de permisos del perfil mencionado especifica un rol de CodeCommit acceso en la cuenta A que luego asume el perfil.
3. La política de confianza del rol de CodeCommit acceso en la cuenta A permite que el perfil designado en la cuenta B asuma el rol de CodeCommit acceso.
4. La política de permisos de IAM del CodeCommit repositorio en la cuenta A permite que el CodeCommit rol de acceso acceda al CodeCommit repositorio.

Pila de tecnología

- CodeCommit
- Git
- IAM
- pip
- SageMaker

Tools (Herramientas)

- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- Git es un sistema de control de versiones distribuido que rastrea los cambios en el código fuente durante el desarrollo del software.

- git-remote-codecommites una utilidad que te ayuda a insertar y extraer código de CodeCommit los repositorios mediante la extensión de Git.
- pip es el instalador de paquetes para Python. Puede usar pip para instalar paquetes desde Python Package Index y otros índices.

Prácticas recomendadas

Cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Aplicar permisos de privilegio mínimo en la documentación de IAM.

Al implementar este patrón, asegúrese de hacer lo siguiente:

- Confirme que los principios de IAM solo tienen los permisos necesarios para realizar acciones específicas y necesarias en cada repositorio. Por ejemplo, se recomienda permitir que los principios de IAM aprobados envíen y combinen los cambios en ramificaciones específicas del repositorio, pero que solo puedan solicitar combinaciones en las ramificaciones protegidas.
- Confirme que a los principios de IAM se les asignen diferentes roles de de IAM en función de los roles y responsabilidades respectivos de cada proyecto. Por ejemplo, un desarrollador tendrá permisos de acceso diferentes a los de un administrador de versiones o un administrador de AWS.

Epics

Configuración roles de IAM

Tarea	Descripción	Habilidades requeridas
Configura el rol de CodeCommit acceso y la política de permisos.	**Note** Para automatiz ar el proceso de configuración manual documentado en esta epopeya, puede utilizar una	AWS general, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	CloudFormation plantilla de AWS.	
	En la cuenta que contiene el CodeCommit repositorio (cuenta A), haga lo siguiente: 1. Cree una función de IAM que pueda asumir la función de instancia de SageMaker bloc de notas de la cuenta B. 2. Cree una política de IAM que conceda acceso al repositorio y asocie la política al rol. Solo con fines de prueba, elija la política gestionada por AWSCodeCommitPowerUserAWS. Esta política concede todos los CodeCommit permisos excepto la posibilidad de eliminar recursos. 3. Modifique la política de confianza del rol para que la cuenta B aparezca como entidad de confianza. **Important** Antes de trasladar esta configuración	

Tarea	Descripción	Habilidades requeridas
	a su entorno de producción, se recomienda redactar su propia política de IAM que aplique permisos de privilegio mínimo. Para obtener más información, consulte la sección Información adicional de este patrón.	

Tarea	Descripción	Habilidades requeridas
Conceda permisos al rol de la instancia de SageMaker bloc de notas en la cuenta B para que asuma el rol de CodeCommit acceso en la cuenta A.	En la cuenta que contiene la función de IAM de la instancia de SageMaker bloc de notas (cuenta B), haga lo siguiente: 1. Cree una política de IAM que permita a un usuario o rol de IAM asumir el rol de CodeCommit acceso en la cuenta A. Ejemplo de política de permisos de IAM que permite a un usuario o rol de IAM asumir un rol entre cuentas `{ "Version": "2012-10-17", "Statement": [ { "Sid": "VisualEditor0", "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "arn:aws:iam:::accountA_ID:role/accountArole_ID" } }` 2. Adjunta la política a la función de la instancia de tu SageMaker bloc de notas en la cuenta B.	AWS general, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	3. Haga que la función de la instancia de SageMaker bloc de notas en la cuenta B asuma la función de CodeCommit acceso en la cuenta A. **Note** Para ver el nombre de recurso de Amazon (ARN) de su repositorio, consulte Ver detalles del CodeCommit repositorio en la Guía CodeCommit del usuario de AWS.	

Configure su instancia de SageMaker notebook en la cuenta B

Tarea	Descripción	Habilidades requeridas
Configure un perfil de usuario en la instancia de AWS SageMaker Notebook para que asuma el rol en la cuenta A.	**Important** Asegúrese de tener instalada la última versión de la interfaz de la línea de comandos de AWS (AWS CLI).	AWS general, AWS DevOps

Tarea	Descripción	Habilidades requeridas

	En la cuenta que contiene la instancia de SageMaker bloc de notas (cuenta B), haga lo siguiente:
	
	1. Inicie sesión en la consola de administración de AWS y abra la consola de SageMaker .
	2. Acceda a la instancia de su SageMaker bloc de notas. Se abrirá la interfaz de Jupyter.
	3. Seleccione Nuevo y, a continuación, seleccione Terminal. Se abrirá una nueva ventana de terminal en su entorno de Jupyter.
	4. Navegue hasta el archivo ~/.aws/config de la instancia del SageMaker bloc de notas. A continuación, añada un perfil de usuario al archivo introduciendo la siguiente instrucción:
	
	`------.aws/config-------------`
	`[profile remoterepouser]`
	`role_arn = arn:aws:iam::<ID of Account A>:role/<rolename>`	

Tarea	Descripción	Habilidades requeridas

	`role_session_name = remoteaccesssession`
	`region = eu-west-1`
	`credential_source = Ec2InstanceMetadata`
	`----------`
	`----------`	

Instale la utilidad git-remote-codecommit.	Siga las instrucciones del paso 2: Instalación de git-remote-codecommit la Guía del CodeCommit usuario de AWS.	Científico de datos

Acceda al repositorio

Tarea	Descripción	Habilidades requeridas
Acceda al CodeCommit repositorio mediante los comandos de Git o SageMaker.	Uso en Git Los directores de IAM que asumen la función de la instancia de SageMaker bloc de notas en la cuenta B ahora pueden ejecutar comandos de Git para acceder al CodeCommit repositorio de la cuenta A. Por ejemplo, los usuarios pueden ejecutar comandos como `git clonegit pull`, y. `git push` Para obtener instrucciones, consulte Conectarse a un CodeCommit repositorio	Git, consola bash

Tarea	Descripción	Habilidades requeridas
	de AWS en la Guía del CodeCommit usuario de AWS. Para obtener información sobre cómo usar Git con CodeCommit, consulte Introducción a AWS CodeCommit en la Guía del CodeCommit usuario de AWS. Para usar SageMaker Para usar Git desde la SageMaker consola, debes permitir que Git recupere las credenciales de tu CodeCommit repositor io. Para obtener instrucci ones, consulte Asociar un CodeCommit repositorio de una cuenta de AWS diferente a una instancia de notebook en la SageMaker documenta ción.	

Recursos relacionados

- Configurar el acceso multicuenta a un CodeCommit repositorio de AWS mediante roles (CodeCommit documentación de AWS)
- Tutorial de IAM: delegue el acceso entre cuentas de AWS mediante roles de IAM (documentación de IAM)

Información adicional

Restringir CodeCommit los permisos a acciones específicas

Para restringir las acciones que un responsable de IAM puede realizar en el CodeCommit repositorio, modifique las acciones que están permitidas en la política de CodeCommit acceso.

Para obtener más información sobre las operaciones de la CodeCommit API, consulte la referencia de CodeCommit permisos en la Guía del CodeCommit usuario de AWS.

> **Note**
>
> También puede editar la política gestionada por AWSCodeCommitPowerUserAWS para adaptarla a su caso de uso.

Restringir CodeCommit los permisos a repositorios específicos

Para crear un entorno multiusuario en el que solo usuarios específicos puedan acceder a más de un repositorio de código, haga lo siguiente:

1. Cree varios roles de CodeCommit acceso en la cuenta A. A continuación, configure la política de confianza de cada rol de acceso para permitir que usuarios específicos de la cuenta B asuman el rol.
2. Restrinja los repositorios de código que puede asumir cada función añadiendo una condición de «recurso» a la política de cada función de CodeCommit acceso.

Ejemplo de condición de «recurso» que restringe el acceso de un director de IAM a un repositorio específico CodeCommit

```
"Resource" : [<REPOSITORY_ARN>,<REPOSITORY_ARN> ]
```

> **Note**
>
> Para ayudar a identificar y diferenciar varios repositorios de código en la misma cuenta de AWS, puede asignar distintos prefijos a los nombres de los repositorios. Por ejemplo, puede asignar nombres a los repositorios de código con prefijos que correspondan a distintos grupos de desarrolladores, como myproject-subproject1-repo1 y myproject-subproject2-repo1. A continuación, puede crear un rol de IAM para cada grupo de desarrolladores en función de sus prefijos asignados. Por ejemplo, puede crear un rol denominado myproject-

subproject1-repoaccess y concederle acceso a todos los repositorios de código que incluyen el prefijo myproject-subproject1.

Ejemplo de condición “Recurso” que hace referencia a un ARN de repositorio de código que incluye un prefijo específico

```
"Resource" : arn:aws:codecommit:<region>:<account-id>:myproject-subproject1-*
```

Implemente una estrategia GitHub de ramificación de Flow para entornos de cuentas múltiples DevOps

Mike Stephens y Abhilash Vinod, Amazon Web Services

Resumen

Al administrar un repositorio de código fuente, las diferentes estrategias de ramificación afectan a los procesos de desarrollo y lanzamiento de software que utilizan los equipos de desarrollo. Algunos ejemplos de estrategias de ramificación comunes son Trunk, GitHub Flow y Gitflow. Estas estrategias utilizan diferentes ramificaciones y las actividades que se llevan a cabo en cada entorno son diferentes. Organismos que están implementando DevOps procesos se beneficiarían de una guía visual que les ayude a entender las diferencias entre estas estrategias de ramificación. El uso de este elemento visual en su organización ayuda a los equipos de desarrollo a alinear su trabajo y seguir los estándares de la organización. Este patrón proporciona esta imagen y describe el proceso de implementación de una estrategia de ramificación de GitHub Flow en su organización.

Este patrón forma parte de una serie de documentos sobre la elección e implementación de estrategias de DevOps ramificación para organizaciones con múltiples sucursales. Cuentas de AWS Esta serie está diseñada para ayudarlo a aplicar la estrategia correcta y las mejores prácticas desde el principio, a fin de optimizar su experiencia en la nube. GitHub El flujo es solo una posible estrategia de ramificación que su organización puede utilizar. En esta serie de documentación también se cubren los modelos de ramificación de Trunk y Gitflow. Si aún no lo has hecho, te recomendamos que revises Cómo elegir una estrategia de ramificación de Git para DevOps entornos de múltiples cuentas antes de implementar la guía de este patrón. Utilice la diligencia debida para elegir la estrategia de ramificación adecuada para su organización.

Esta guía proporciona un diagrama que muestra cómo una organización podría implementar la estrategia GitHub Flow. Se recomienda revisar la Guía de AWS DevOps Well-Architected para revisar las mejores prácticas. Este patrón incluye las tareas, los pasos y las restricciones recomendados para cada paso del DevOps proceso.

Requisitos previos y limitaciones

Requisitos previos

- Git instalado. Se utiliza como herramienta de repositorio de código fuente.
- Draw.io instalado. Esta aplicación se utiliza para ver y editar el diagrama.

Arquitectura

Arquitectura de destino

El siguiente diagrama se puede usar como un cuadro de Punnett (Wikipedia). Alinee las ramas en el eje vertical con los AWS entornos en el eje horizontal para determinar qué acciones realizar en cada escenario. Los números indican la secuencia de las acciones del flujo de trabajo. En este ejemplo, se pasa de una ramificación `feature` a la implementación en producción.

Para obtener más información sobre los Cuentas de AWS entornos y las ramas en un enfoque de GitHub flujo, consulta Cómo elegir una estrategia de ramificación de Git para entornos de múltiples cuentas DevOps .

Automatización y escala

La integración y la entrega continuas (CI/CD) is the process of automating the software release lifecycle. It automates much or all of the manual processes traditionally required to get new code from an initial commit into production. A CI/CD pipeline encompasses the sandbox, development, testing, staging, and production environments. In each environment, the CI/CD pipeline provisions any infrastructure that is needed to deploy or test the code. By using CI/CD, development teams can make changes to code that are then automatically tested and deployed. CI/CDcanalizaciones) también proporcionan control y protección a los equipos de desarrollo, ya que refuerzan la coherencia, los estándares, las mejores prácticas y unos niveles mínimos de aceptación para la aceptación y el despliegue de las funciones. Para obtener más información, consulte Practicar la integración continua y la entrega continua en. AWS

AWS ofrece un conjunto de servicios para desarrolladores diseñados para ayudarle a crear CI/CD canalizaciones. Por ejemplo, AWS CodePipelinees un servicio de entrega continua totalmente gestionado que le ayuda a automatizar sus procesos de lanzamiento para obtener actualizaciones rápidas y fiables de las aplicaciones y la infraestructura. AWS CodeBuildcompila el código fuente, ejecuta pruebas y produce paquetes de ready-to-deploy software. Para obtener más información, consulte Herramientas para desarrolladores en AWS.

Tools (Herramientas)

AWS servicios y herramientas

AWS proporciona un conjunto de servicios para desarrolladores que puede utilizar para implementar este patrón:

- AWS CodeArtifact es un servicio de repositorio de artefactos administrado y altamente escalable que lo ayuda a almacenar y compartir paquetes de software para el desarrollo de aplicaciones.
- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- AWS CodeDeployautomatiza las implementaciones en Amazon Elastic Compute Cloud EC2 (Amazon) o en instancias, AWS Lambda funciones locales o servicios de Amazon Elastic Container Service (Amazon ECS).
- AWS CodePipeline permite diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software y automatizar los pasos necesarios para lanzar los cambios en el software de manera continua.

Otras herramientas

- Draw.io Desktop es una aplicación para hacer diagramas y diagramas de flujo. El repositorio de código contiene plantillas en formato .drawio para Draw.io.
- Figma es una herramienta de diseño en línea diseñada para la colaboración. El repositorio de código contiene plantillas en formato .fig para Figma.

Repositorio de código

El archivo fuente del diagrama de este patrón está disponible en el repositorio GitHub Git Branching Strategy for GitHub Flow. Incluye archivos en los formatos PNG, draw.io y Figma. Puede modificar estos diagramas para respaldar los procesos de su organización.

Prácticas recomendadas

Siga las mejores prácticas y recomendaciones de AWS DevOps Well-Architected Guidance y Eligiendo una estrategia de ramificación de Git para entornos de múltiples cuentas. DevOps Te ayudan a implementar de forma eficaz el desarrollo GitHub basado en Flow, a fomentar la colaboración, a mejorar la calidad del código y a agilizar el proceso de desarrollo.

Epics

Revisión de los GitHub flujos de trabajo de Flow

Tarea	Descripción	Habilidades requeridas
Revise el proceso GitHub de flujo estándar.	1. En el entorno de pruebas, el desarrollador crea una ramificación `feature` a partir de la ramificación `main` y usa el patrón de nomenclatura `feature/<ticket>_<initials>_<short description>` . 2. El desarrollador agrega una o más confirmaciones a la ramificación `feature`, cada una de las cuales representa un cambio o mejora distintos. 3. El desarrollador abre una solicitud de combinación (MR) para combinar los cambios en la ramificación `main`. Esto inicia un proceso de revisión. 4. Durante el proceso de revisión, los desarrolladores analizan los cambios en el código y proporcionan comentarios. El objetivo es garantizar que los cambios sean de alta calidad y cumplan con los estándares del proyecto.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	5. Una vez que el desarrollador crea la solicitud de combinación, se inicia un proceso de compilación automatizado que implementa los cambios de la ramificación `feature` en el entorno de desarrollo. 6. Las pruebas automatizadas verifican la integridad y la calidad de los cambios incluidos en la solicitud de combinación. Para completar la solicitud de combinación, es necesario que la compilación, la implementación y las pruebas se lleven a cabo correctamente. 7. Cuando se completa el proceso de revisión, los cambios se combinan en la ramificación `main`. 8. Un aprobador aprueba manualmente la implementación de los artefactos de lanzamiento en el entorno de pruebas. 9. Un aprobador aprueba manualmente la implementación de los artefactos de lanzamiento en el entorno de ensayo.	

Tarea	Descripción	Habilidades requeridas
	10. Un aprobador aprueba manualmente la implementación de los artefactos de lanzamiento en el entorno de producción.	

Tarea	Descripción	Habilidades requeridas
Revise el proceso de corrección de errores GitHub Flow.	1. El desarrollador crea una ramificación `bugfix` a partir de la ramificación `main` y usa el patrón de nomenclatura `bugfix/<ticket number>_<developer initials>_<descriptor>` . 2. El desarrollador corrige el problema, confirma la corrección y crea la ramificación `bugfix`. 3. El desarrollador abre una solicitud de combinación para combinar la ramificación `bugfix` en la ramificación `main`. Esto inicia un proceso de revisión. 4. Durante el proceso de revisión, los desarrolladores analizan los cambios en el código y proporcionan comentarios. 5. Tras la finalización y la aprobación de la revisión, el desarrollador completa la solicitud de combinación de la ramificación `bugfix` en la ramificación `main`. 6. Un aprobador aprueba manualmente la implementación de los artefactos de	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	lanzamiento en entornos superiores.	

Tarea	Descripción	Habilidades requeridas
Revise el proceso de hotfix GitHub Flow.	GitHub Flow está diseñado para permitir una entrega continua, donde los cambios de código se implementan de manera frecuente y confiable en entornos superiores. La clave es que todas las ramificaciones `feature` se puedan implementar en cualquier momento. Las ramificaciones `Hotfix`, que son similares a las ramificaciones `feature` o `bugfix`, pueden seguir el mismo proceso que cualquier a de estas otras ramificac iones. Sin embargo, dada su urgencia, las revisiones suelen tener una prioridad más alta. En función de las políticas del equipo y de la inmediatez de la situación, algunos pasos del proceso podrían acelerars e. Por ejemplo, es posible acelerar las revisiones del código de las revisiones. Por lo tanto, si bien el proceso de revisión es paralelo al proceso de corrección o características, la urgencia que rodea a las revisione s puede justificar modificac iones en el cumplimiento del procedimiento. Es fundament	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	al establecer directrices sobre la administración de las revisiones para garantiza r que se gestionen de forma eficiente y segura.	

Resolución de problemas

Problema	Solución
Conflictos de ramificaciones	Un problema común que puede producirse con el modelo GitHub Flow es cuando es necesario realizar una revisión en la producción`feature`, `bugfix` pero el cambio correspondiente debe producirse en una `hotfix` rama o sucursal en la que se modifican los mismos recursos. Le recomendamos que combine con frecuenci a los cambios de `main` en las ramificaciones inferiores para evitar conflictos importantes al llevar a cabo la combinación con `main`.
Consolidación del equipo	GitHub Flow fomenta las implementaciones diarias en entornos más altos y adopta una verdadera integración y entrega continuas (CI/ CD). Es imprescindible que el equipo cuente con la consolidación en materia de ingenierí a que se necesita para desarrollar caracterí sticas y crear pruebas de automatización para ellas. El equipo debe llevar a cabo una revisión exhaustiva de las solicitudes de combinación antes de aprobar los cambios. Esto fomenta una cultura de ingeniería sólida que promueve la calidad, la responsabilidad y la eficiencia en el proceso de desarrollo.

Recursos relacionados

En esta guía no se incluye capacitación sobre Git; sin embargo, hay muchos recursos de alta calidad disponibles en Internet si necesita esta capacitación. Le recomendamos que comience con el sitio de documentación de Git.

Los siguientes recursos pueden ayudarlo en su proceso de expansión de GitHub Flow en el. Nube de AWS

AWS DevOps orientación

- AWS DevOps Indicaciones
- AWS Arquitectura de referencia para la canalización de despliegue
- ¿Qué es DevOps?
- DevOps resources

GitHub Guía de flujo

- GitHub Tutorial de inicio rápido de Flow () GitHub
- ¿Por qué GitHub Flow?

Otros recursos

- Twelve-factor app methodology (12factor.net)

Implementa una estrategia de ramificación de Gitflow para entornos de múltiples cuentas DevOps

Mike Stephens, Stephen DiCato, Abhilash Vinod y Tim Wondergem, Amazon Web Services

Resumen

Al administrar un repositorio de código fuente, las diferentes estrategias de ramificación afectan a los procesos de desarrollo y lanzamiento de software que utilizan los equipos de desarrollo. Algunos ejemplos de estrategias de ramificación habituales son Trunk, Gitflow y Flow. GitHub Estas estrategias utilizan diferentes ramificaciones y las actividades que se llevan a cabo en cada entorno son diferentes. Organismos que están implementando DevOps procesos se beneficiarían de una guía visual que les ayude a entender las diferencias entre estas estrategias de ramificación. El uso de este elemento visual en su organización ayuda a los equipos de desarrollo a alinear su trabajo y seguir los estándares de la organización. Este patrón proporciona este elemento visual y describe el proceso de implementación de una estrategia de ramificación de Gitflow en su organización.

Este patrón forma parte de una serie de documentos sobre la elección e implementación de estrategias de DevOps ramificación para organizaciones con múltiples sucursales. Cuentas de AWS Esta serie está diseñada para ayudarlo a aplicar la estrategia correcta y las prácticas recomendadas desde el principio, a fin de optimizar su experiencia en la nube. Gitflow es solo una posible estrategia de ramificación que su organización puede utilizar. Esta serie de documentación también cubre los modelos de ramificación de Trunk y GitHub Flow. Si aún no lo has hecho, te recomendamos que revises Cómo elegir una estrategia de ramificación de Git para DevOps entornos de múltiples cuentas antes de implementar la guía de este patrón. Utilice la diligencia debida para elegir la estrategia de ramificación adecuada para su organización.

En esta guía se proporciona un diagrama en el que se muestra cómo una organización podría implementar la estrategia de Gitflow. Se recomienda revisar la Guía de AWS DevOps Well-Architected para revisar las mejores prácticas. Este patrón incluye las tareas, los pasos y las restricciones recomendados para cada paso del DevOps proceso.

Requisitos previos y limitaciones

Requisitos previos

- Git instalado. Se utiliza como herramienta de repositorio de código fuente.
- Draw.io instalado. Esta aplicación se utiliza para ver y editar el diagrama.

- (Opcional) Plugin de Gitflow instalado.

Arquitectura

Arquitectura de destino

El siguiente diagrama se puede usar como un cuadro de Punnett (Wikipedia). Alinee las ramas en el eje vertical con los AWS entornos en el eje horizontal para determinar qué acciones realizar en cada escenario. Los números indican la secuencia de las acciones del flujo de trabajo. En este ejemplo, se pasa de una ramificación de características a la implementación en producción.

Para obtener más información sobre los Cuentas de AWS entornos y las ramas en un enfoque de Gitflow, consulta Cómo elegir una estrategia de ramificación de Git para entornos de múltiples DevOps cuentas.

Automatización y escala

La integración y la entrega continuas (CI/CD) is the process of automating the software release lifecycle. It automates much or all of the manual processes traditionally required to get new code from an initial commit into production. A CI/CD pipeline encompasses the sandbox, development, testing, staging, and production environments. In each environment, the CI/CD pipeline provisions any infrastructure that is needed to deploy or test the code. By using CI/CD, development teams can make changes to code that are then automatically tested and deployed. CI/CDcanalizaciones) también proporcionan control y protección a los equipos de desarrollo, ya que refuerzan la coherencia, los estándares, las mejores prácticas y unos niveles mínimos de aceptación para la aceptación y el despliegue de las funciones. Para obtener más información, consulte Practicar la integración continua y la entrega continua en. AWS

AWS ofrece un conjunto de servicios para desarrolladores diseñados para ayudarle a crear CI/CD canalizaciones. Por ejemplo, AWS CodePipelinees un servicio de entrega continua totalmente gestionado que le ayuda a automatizar sus procesos de lanzamiento para obtener actualizaciones rápidas y fiables de las aplicaciones y la infraestructura. AWS CodeBuildcompila el código fuente, ejecuta pruebas y produce paquetes de ready-to-deploy software. Para obtener más información, consulte Herramientas para desarrolladores en AWS.

Tools (Herramientas)

AWS servicios y herramientas

AWS proporciona un conjunto de servicios para desarrolladores que puede utilizar para implementar este patrón:

- AWS CodeArtifact es un servicio de repositorio de artefactos administrado y altamente escalable que lo ayuda a almacenar y compartir paquetes de software para el desarrollo de aplicaciones.
- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- AWS CodeDeployautomatiza las implementaciones en Amazon Elastic Compute Cloud EC2 (Amazon) o en instancias, AWS Lambda funciones locales o servicios de Amazon Elastic Container Service (Amazon ECS).
- AWS CodePipeline permite diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software y automatizar los pasos necesarios para lanzar los cambios en el software de manera continua.

Otras herramientas

- Draw.io Desktop es una aplicación para hacer diagramas y diagramas de flujo. El repositorio de código contiene plantillas en formato .drawio para Draw.io.
- Figma es una herramienta de diseño en línea diseñada para la colaboración. El repositorio de código contiene plantillas en formato .fig para Figma.
- (Opcional) El complemento de Gitflow es una colección de extensiones de Git que proporcionan operaciones de repositorio de alto nivel para el modelo de ramificación de Gitflow.

Repositorio de código

El archivo fuente del diagrama de este patrón está disponible en el GitFlow repositorio GitHub Git Branching Strategy for. Incluye archivos en los formatos PNG, draw.io y Figma. Puede modificar estos diagramas para respaldar los procesos de su organización.

Prácticas recomendadas

Siga las mejores prácticas y recomendaciones de AWS DevOps Well-Architected Guidance y Choosing a Git Branching Strategy for Multiaccount Environments. DevOps Estos recursos lo ayudan a implementar de manera efectiva el desarrollo basado en Gitflow, fomentar la colaboración, mejorar la calidad del código y agilizar el proceso de desarrollo.

Epics

Revisión de los flujos de trabajo de Gitflow

Tarea	Descripción	Habilidades requeridas
Revisar el proceso estándar de Gitflow.	1. En el entorno de pruebas, el desarrollador crea una ramificación `feature` a partir de la ramificación `develop` y usa el patrón de nomenclatura `feature/<ticket>_<initials>_<short description>` . 2. El desarrollador desarrolla el código y lo implementa en el entorno de pruebas de forma iterativa para completar el ticket. **Note** Si lo desea, el desarrollador puede crear una ramificación `sandbox` para ejecutar una canalización automatizada de compilación o implementación en el entorno de pruebas. 3. El desarrollador crea una solicitud de fusión de la	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	ramificación `feature` a la ramificación `develop` mediante una combinación de squash. 4. Una canalización de integración y entrega continuas (CI/CD) crea e implementa automátic amente la ramificación `develop` en el entorno de desarrollo. 5. (Opcional) Un desarroll ador integra ramificaciones `feature` adicionales en la ramificación de desarrollo antes de continuar con las actividades de lanzamiento. 6. Cuando tenga todo listo para lanzar las caracterí sticas de la ramificación `develop`, el desarroll ador crea una ramificación `release` con el nombre `release/v<number>` a partir de la ramificación `develop`. 7. El desarrollador crea la ramificación de lanzamien to, que publica los artefacto s para reutilizarlos en otros entornos. 8. Un aprobador aprueba manualmente la implement ación de los artefactos de	

Tarea	Descripción	Habilidades requeridas
	lanzamiento en el entorno de pruebas. 9. Un aprobador aprueba manualmente la implement ación de los artefactos de lanzamiento en el entorno de ensayo. 10. Un aprobador aprueba manualmente la implement ación de los artefactos de lanzamiento en el entorno de producción. 11. El desarrollador combina la ramificación `release` en la ramificación `main`. Lo ideal es que el desarrollador utilice un script automatiz ado para llevar a cabo una combinación de avance rápido. No utilice una combinación de squash. 12. El desarrollador combina la ramificación `release` en la ramificación `develop`. Lo ideal es que el desarroll ador utilice un script automatizado para llevar a cabo una combinaci ón de avance rápido. No utilice una combinación de squash.	

Tarea	Descripción	Habilidades requeridas
Revisar el proceso de Gitflow de revisión.	1. El desarrollador crea una ramificación `hotfix` a partir de la ramificación `main` y usa el patrón de nomenclatura `hotfix/<ticket>_<initials>_<short description>` . 2. El desarrollador crea una ramificación `release` a partir de la ramificación `main` y le asigna el nombre `release/v<number>` . 3. El desarrollador corrige el problema, confirma la corrección y crea la ramificación `hotfix`. 4. El desarrollador crea una solicitud de fusión de la ramificación `hotfix` a la ramificación `release/v<number>` mediante una combinación de squash. 5. El desarrollador crea la ramificación `release`, que publica los artefactos para reutilizarlos en otros entornos. 6. Un aprobador aprueba manualmente la implementación de los artefactos de lanzamiento en el entorno de pruebas.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	7. Un aprobador aprueba manualmente la implementación de los artefactos de lanzamiento en el entorno de ensayo. 8. Un aprobador aprueba manualmente la implementación de los artefactos de lanzamiento en el entorno de producción. 9. El desarrollador combina la ramificación `release` en la ramificación `main`. Lo ideal es que el desarrollador utilice un script automatizado para llevar a cabo una combinación de avance rápido. No utilice una combinación de squash. 10. El desarrollador combina la ramificación `release` en la ramificación `develop`. Lo ideal es que el desarrollador utilice un script automatizado para llevar a cabo una combinación de avance rápido. No utilice una combinación de squash. 11. Si se detecta un conflicto, los desarrolladores reciben una alerta y resuelven el conflicto con una solicitud de combinación.	

Tarea	Descripción	Habilidades requeridas
Revisar el proceso de Gitflow de corrección.	1. El desarrollador crea una ramificación `bugfix` a partir de la ramificación `release/v<number>` actual y usa el patrón de nomenclatura `bugfix/<ticket number>_<developer initials>_<descriptor>` . 2. El desarrollador corrige el problema, confirma la corrección y crea la ramificación `bugfix`. 3. El desarrollador crea una solicitud de fusión de la ramificación `bugfix` a la ramificación `release/v<number>` mediante una combinación de squash. 4. El desarrollador crea la ramificación `release`, que publica los artefactos para reutilizarlos en otros entornos. 5. Un aprobador aprueba manualmente la implementación de los artefactos de lanzamiento en el entorno de pruebas. 6. Un aprobador aprueba manualmente la implementación de los artefactos de	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	lanzamiento en el entorno de ensayo. 7. Un aprobador aprueba manualmente la implement ación de los artefactos de lanzamiento en el entorno de producción. 8. El desarrollador combina la ramificación `release` en la ramificación `main`. Lo ideal es que el desarrollador utilice un script automatiz ado para llevar a cabo una combinación de avance rápido. No utilice una combinación de squash. 9. El desarrollador combina la ramificación `release` en la ramificación `develop`. Lo ideal es que el desarroll ador utilice un script automatizado para llevar a cabo una combinaci ón de avance rápido. No utilice una combinación de squash. 10. Si se detecta un conflicto, los desarrolladores reciben una alerta y resuelven el conflicto con una solicitud de combinación.	

Resolución de problemas

Problema	Solución
Conflictos de ramificaciones	Un problema común que puede producirse con el modelo de Gitflow es cuando es necesario llevar a cabo una revisión en producción, pero el cambio correspondiente debe producirse en un entorno inferior, en el que otra ramificación modifica los mismos recursos. Le recomendamos que solo tenga una ramificación de lanzamiento activa a la vez. Si tiene más de una ramificación activa a la vez, es posible que los cambios en los entornos colisionen y que no pueda pasar una ramificación a la fase de producción.
Fusión	Las versiones deben volver a combinarse con las principales y desarrollarse lo antes posible para volver a consolidar el trabajo en las ramificaciones principales.
Combinación de squash	Use una combinación de squash solo cuando vaya a combinar de una ramificación `feature` a una ramificación `develop`. El uso de combinaciones de squash en ramificaciones superiores causa dificultades al volver a combinar cambios en las ramificaciones inferiores.

Recursos relacionados

En esta guía no se incluye capacitación sobre Git; sin embargo, hay muchos recursos de alta calidad disponibles en Internet si necesita esta capacitación. Le recomendamos que comience con el sitio de documentación de Git.

Los siguientes recursos pueden ayudarlo con su proceso de ramificaciones de Gitflow en la Nube de AWS.

AWS DevOps orientación

- AWS DevOps Indicaciones
- AWS Arquitectura de referencia para la canalización de despliegue
- ¿Qué es DevOps?
- DevOps resources

Gitflow guidance

- The original Gitflow blog (entrada en el blog de Vincent Driessen)
- Gitflow workflow (Atlassian)
- Gitflow en GitHub: Cómo usar los flujos de trabajo de Git Flow con repositorios GitHub basados (vídeo) YouTube
- Ejemplo de Git Flow Init (YouTube vídeo)
- La rama de lanzamiento de Gitflow de principio a fin (vídeo) YouTube

Otros recursos

Twelve-factor app methodology (12factor.net)

Implemente una estrategia de ramificación troncal para entornos de cuentas múltiples DevOps

Mike Stephens y Rayjan Wilson, Amazon Web Services

Resumen

Al administrar un repositorio de código fuente, las diferentes estrategias de ramificación afectan a los procesos de desarrollo y lanzamiento de software que utilizan los equipos de desarrollo. Algunos ejemplos de estrategias de ramificación comunes son Trunk, GitHub Flow y Gitflow. Estas estrategias utilizan diferentes ramificaciones y las actividades que se llevan a cabo en cada entorno son diferentes. Organismos que están implementando DevOps procesos se beneficiarían de una guía visual que les ayude a entender las diferencias entre estas estrategias de ramificación. El uso de este elemento visual en su organización ayuda a los equipos de desarrollo a alinear su trabajo y seguir los estándares de la organización. Este patrón proporciona este elemento visual y describe el proceso de implementación de una estrategia de ramificación de Trunk en su organización.

Este patrón forma parte de una serie de documentos sobre la elección e implementación de estrategias de DevOps ramificación para organizaciones con múltiples sucursales. Cuentas de AWS Esta serie está diseñada para ayudarlo a aplicar la estrategia correcta y las prácticas recomendadas desde el principio, a fin de optimizar su experiencia en la nube. Trunk es solo una posible estrategia de ramificación que su organización puede utilizar. Esta serie de documentación también cubre los modelos de ramificación de GitHub Flow y Gitflow. Si aún no lo has hecho, te recomendamos que revises Cómo elegir una estrategia de ramificación de Git para DevOps entornos de múltiples cuentas antes de implementar la guía de este patrón. Utilice la diligencia debida para elegir la estrategia de ramificación adecuada para su organización.

En esta guía se proporciona un diagrama en el que se muestra cómo una organización podría implementar la estrategia de Trunk. Se recomienda que consulte la Guía oficial de AWS DevOps Well-Architected para revisar las mejores prácticas. Este patrón incluye las tareas, los pasos y las restricciones recomendados para cada paso del DevOps proceso.

Requisitos previos y limitaciones

Requisitos previos

- Git instalado. Se utiliza como herramienta de repositorio de código fuente.
- Draw.io instalado. Esta aplicación se utiliza para ver y editar el diagrama.

Arquitectura

Arquitectura de destino

El siguiente diagrama se puede usar como un cuadro de Punnett (Wikipedia). Alinee las ramas en el eje vertical con los AWS entornos en el eje horizontal para determinar qué acciones realizar en cada escenario. Los números indican la secuencia de las acciones del flujo de trabajo. En este ejemplo, se pasa de una ramificación `feature` a la implementación en producción.

Para obtener más información sobre los Cuentas de AWS entornos y las ramas en un enfoque troncal, consulta Cómo elegir una estrategia de ramificación de Git para entornos con varias cuentas DevOps .

Automatización y escala

La integración y la entrega continuas (CI/CD) is the process of automating the software release lifecycle. It automates much or all of the manual processes traditionally required to get new code from an initial commit into production. A CI/CD pipeline encompasses the sandbox, development, testing, staging, and production environments. In each environment, the CI/CD pipeline provisions any infrastructure that is needed to deploy or test the code. By using CI/CD, development teams can make changes to code that are then automatically tested and deployed. CI/CDcanalizaciones) también proporcionan control y protección a los equipos de desarrollo, ya que refuerzan la coherencia, los estándares, las mejores prácticas y niveles mínimos de aceptación para la aceptación y el despliegue de las funciones. Para obtener más información, consulte Practicar la integración continua y la entrega continua en. AWS

AWS ofrece un conjunto de servicios para desarrolladores diseñados para ayudarle a crear CI/CD canalizaciones. Por ejemplo, AWS CodePipelinees un servicio de entrega continua totalmente gestionado que le ayuda a automatizar sus procesos de lanzamiento para obtener actualizaciones rápidas y fiables de las aplicaciones y la infraestructura. AWS CodeBuildcompila el código fuente, ejecuta pruebas y produce paquetes de ready-to-deploy software. Para obtener más información, consulte Herramientas para desarrolladores en AWS.

Tools (Herramientas)

AWS servicios y herramientas

AWS proporciona un conjunto de servicios para desarrolladores que puede utilizar para implementar este patrón:

- AWS CodeArtifact es un servicio de repositorio de artefactos administrado y altamente escalable que lo ayuda a almacenar y compartir paquetes de software para el desarrollo de aplicaciones.
- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- AWS CodeDeployautomatiza las implementaciones en Amazon Elastic Compute Cloud EC2 (Amazon) o en instancias, AWS Lambda funciones locales o servicios de Amazon Elastic Container Service (Amazon ECS).
- AWS CodePipeline permite diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software y automatizar los pasos necesarios para lanzar los cambios en el software de manera continua.

Otras herramientas

- Draw.io Desktop: una aplicación para hacer diagramas y diagramas de flujo.
- Figma es una herramienta de diseño en línea diseñada para la colaboración. El repositorio de código contiene plantillas en formato .fig para Figma.

Repositorio de código

El archivo fuente del diagrama de este patrón está disponible en el repositorio GitHub Git Branching Strategy for Trunk. Incluye archivos en los formatos PNG, draw.io y Figma. Puede modificar estos diagramas para respaldar los procesos de su organización.

Prácticas recomendadas

Siga las mejores prácticas y recomendaciones de AWS DevOps Well-Architected Guidance y Choosing a Git Branching Strategy for Multiaccount Environments. DevOps Estos recursos lo ayudan a implementar de manera efectiva el desarrollo basado en Trunk, fomentar la colaboración, mejorar la calidad del código y agilizar el proceso de desarrollo.

Epics

Revisión del flujo de trabajo de Trunk

Tarea	Descripción	Habilidades requeridas
Revisar el proceso estándar de Trunk.	1. En el entorno de pruebas, el desarrollador crea una ramificación `feature` a partir de la ramificación `main` y usa el patrón de nomenclatura `feature/<ticket>_<initials>_<short description>` . 2. El desarrollador desarrolla el código y lo implementa en el entorno de pruebas de forma iterativa para completar el ticket. **Note** Si lo desea, el desarrollador puede crear una ramificación `sandbox` para ejecutar una canalización automatizada de compilación o implementación en el entorno de pruebas. 3. El desarrollador crea una solicitud de fusión de la	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	ramificación `feature` a la ramificación `main` mediante una combinación de squash. 4. Una canalización de integración y entrega continuas (CI/CD) crea y publica automátic amente los artefactos de la ramificación `main` en el entorno de desarrollo. 5. Un aprobador aprueba manualmente la implement ación de los artefactos de lanzamiento en el entorno de desarrollo. 6. Un aprobador aprueba manualmente la implement ación de los artefactos de lanzamiento en el entorno de pruebas. 7. Un aprobador aprueba manualmente la implement ación de los artefactos de lanzamiento en el entorno de ensayo. 8. Un aprobador aprueba manualmente la implement ación de los artefactos de lanzamiento en el entorno de producción.	

Resolución de problemas

Problema	Solución
Conflictos de ramificaciones	Un problema común que puede producirse con el modelo de Trunk es cuando es necesario llevar a cabo una revisión en producción, pero el cambio correspondiente debe producirse en una ramificación `feature` en la que se modifican los mismos recursos. Le recomendamos que combine con frecuencia los cambios de `main` en las ramificaciones inferiores para evitar conflictos importantes al llevar a cabo la combinación con `main`.

Recursos relacionados

En esta guía no se incluye capacitación sobre Git; sin embargo, hay muchos recursos de alta calidad disponibles en Internet si necesita esta capacitación. Le recomendamos que comience con el sitio de documentación de Git.

Los siguientes recursos pueden ayudarlo con su proceso de ramificaciones de Trunk en la Nube de AWS.

AWS DevOps orientación

- AWS DevOps Indicaciones
- AWS Deployment Pipeline Reference Architecture
- ¿Qué es DevOps?
- DevOps resources

Guía de Trunk

- Trunk Based Development

Otros recursos

- Twelve-factor app methodology (12factor.net)

Implemente un escaneo Checkov personalizado y centralizado para aplicar la política antes de implementar AWS la infraestructura

Benjamin Morris, Amazon Web Services

Resumen

Este patrón proporciona un marco de GitHub acciones para escribir políticas de Checkov personalizadas en un repositorio que se pueden reutilizar en toda la organización. GitHub Al seguir este patrón, un equipo de seguridad de la información puede escribir, agregar y mantener políticas personalizadas según los requisitos de la empresa. Las políticas personalizadas se pueden incorporar automáticamente a todos los procesos de la GitHub organización. Este enfoque se puede utilizar para hacer cumplir los estándares de la empresa en relación con los recursos antes de que estos se implementen.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Una GitHub organización que usa GitHub Actions
- AWS infraestructura implementada con HashiCorp Terraform o AWS CloudFormation

Limitaciones

- Este patrón está escrito para GitHub Actions. Sin embargo, se puede adaptar a marcos similares de integración continua y entrega continua (CI/CD), como. GitLab No se requiere una versión de pago específica de GitHub .
- Algunas Servicios de AWS no están disponibles en todas Regiones de AWS. Para conocer la disponibilidad regional, consulta los puntos finales y las cuotas del servicio en la AWS documentación y elige el enlace correspondiente al servicio.

Arquitectura

Este patrón está diseñado para implementarse como un GitHub repositorio que contiene un flujo de trabajo GitHub reutilizable y políticas de Checkov personalizadas. El flujo de trabajo reutilizable puede escanear repositorios de Terraform y de CloudFormation infraestructura como código (IaC).

El siguiente diagrama muestra el repositorio de GitHub flujos de trabajo reutilizables y el repositorio de políticas de Custom Checkov como iconos separados. Sin embargo, puede implementar estos repositorios como repositorios separados o como un repositorio único. El código de ejemplo usa un único repositorio, con archivos para flujos de trabajo (`.github/workflows`) y archivos para políticas personalizadas (la carpeta `custom_policies` y el archivo de configuración `.checkov.yml`) en el mismo repositorio.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario crea una solicitud de extracción en un GitHub repositorio.
2. Los flujos de trabajo de Pipeline comienzan en GitHub Actions, e incluyen una referencia a un flujo de trabajo reutilizable de Checkov.
3. El flujo de trabajo de canalización descarga el flujo de trabajo reutilizable de Checkov al que se hace referencia desde un repositorio externo y ejecuta ese flujo de trabajo de Checkov mediante Actions. GitHub
4. El flujo de trabajo reutilizable de Checkov descarga las políticas personalizadas de un repositorio externo.
5. El flujo de trabajo reutilizable de Checkov evalúa el IaC del GitHub repositorio en función de las políticas de Checkov integradas y personalizadas. El flujo de trabajo reutilizable de Checkov se aprueba o no en función de si se detectan problemas de seguridad.

Automatización y escala

Este patrón permite la administración centralizada de la configuración de Checkov, de modo que las actualizaciones de políticas se puedan aplicar en un solo lugar. Sin embargo, este patrón requiere que cada repositorio utilice un flujo de trabajo que contenga una referencia al flujo de trabajo central reutilizable. Puede añadir esta referencia manualmente o utilizar scripts para insertar el archivo en la carpeta `.github/workflows` de cada repositorio.

Tools (Herramientas)

Servicios de AWS

- CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todas las regiones. Cuentas de AWS Checkov puede escanear CloudFormation.

Otras herramientas

- Checkov es una herramienta de análisis de código estático que comprueba si la IaC se ha configurado mal configurado en función de la seguridad y el cumplimiento.
- GitHub Actions está integrado en la GitHub plataforma para ayudarte a crear, compartir y ejecutar flujos de trabajo en tus GitHub repositorios. Puedes usar GitHub Actions para automatizar tareas como crear, probar e implementar tu código.
- Terraform es una herramienta de iAC HashiCorp que le ayuda a crear y administrar recursos locales y en la nube. Checkov puede analizar Terraform.

Repositorio de código

El código de este patrón está disponible en el repositorio. GitHub centralized-custom-checkov-sast

Prácticas recomendadas

- Para mantener una postura de seguridad coherente, asegúrese de que las políticas de seguridad de su empresa coinciden con las políticas de Checkov.
- En las primeras fases de la implementación de las políticas personalizadas de Checkov, puede utilizar la opción Error leve en el análisis de Checkov para poder combinar la IaC que tenga problemas de seguridad. A medida que el proceso vaya madurando, cambie de la opción Error leve a la opción Error grave.

Epics

Creación de un repositorio central de Checkov para políticas personalizadas

Tarea	Descripción	Habilidades requeridas
Cree un repositorio central de Checkov.	Cree un repositorio para almacenar las políticas de Checkov personalizadas que se utilizarán en la organizac ión. Para empezar rápidamente, puedes copiar el contenido del	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	repositorio de este patrón en tu GitHub centralized-custom-checkov-sast repositorio central de Checkov.	
Cree un repositorio para flujos de trabajo reutilizables.	Si ya existe un repositor io para flujos de trabajo reutilizables, o si planea incluir archivos de flujo de trabajo reutilizables en el mismo repositorio que las políticas personalizadas de Checkov, puede omitir este paso. Cree un GitHub repositor io para almacenar flujos de trabajo reutilizables. Las canalizaciones de otros repositorios harán referencia a este repositorio.	DevOps ingeniero

Creación de flujos de trabajo de Checkov reutilizables y de ejemplo

Tarea	Descripción	Habilidades requeridas
Añada un flujo de trabajo reutilizable de Checkov.	Cree un flujo de trabajo reutilizable de Checkov GitHub Actions (archivo YAML) en el repositorio de flujos de trabajo reutilizables. Puede adaptar este flujo de trabajo reutilizable a partir del archivo de flujo de trabajo que se proporciona en este patrón.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Como ejemplo de un cambio, es posible que quiera cambiar el flujo de trabajo reutiliza ble para utilizar la opción Error leve. Si establece `soft-fail` en `true`, el trabajo se puede completar correctamente incluso si se produce un error en el análisis de Checkov. Para obtener instrucciones, consulte Hard and soft fail en la documenta ción de Checkov.	
Añada un ejemplo de flujo de trabajo.	Añada un ejemplo de flujo de trabajo de Checkov que haga referencia al flujo de trabajo de `reusable`. Esto proporcionará una plantilla sobre cómo reutilizar el flujo de trabajo de `reusable`. En el repositorio de ejemplo, `checkov-source.yaml` es el flujo de trabajo reutiliza ble y `checkov-scan.yaml` es el ejemplo que consume `checkov-source` . Para obtener más informaci ón sobre cómo escribir un ejemplo de flujo de trabajo de Checkov, consulte Información adicional.	DevOps ingeniero

Asociación de las políticas de la empresa a las políticas personalizadas de Checkov

Tarea	Descripción	Habilidades requeridas
Determine las políticas que se pueden aplicar con Checkov.	1. Revise las políticas de la empresa relacionadas con la seguridad de la infraestructura y los requisitos que deben existir. 2. Determine qué requisitos se pueden implementar mediante las políticas personalizadas de Checkov. 3. Cree una convención de nomenclatura que asigne el control de la política a la política personalizada de Checkov. Por lo general, las políticas personalizadas de Checkov tienen un identificador con un nombre de Checkov, el origen de la política (personalizado) y un número de política (por ejemplo, `CKV2_CUSTOM_123`). Para obtener más información sobre la creación de políticas personalizadas de Checkov, consulte la Custom Policies Overview en la documentación de Checkov.	Seguridad y conformidad

Tarea	Descripción	Habilidades requeridas
Agregue políticas personalizadas de Checkov.	Convierta las políticas de la empresa identificadas en políticas de Checkov personalizadas en el repositorio central. Puede escribir políticas de Checkov sencillas en Python o YAML.	Seguridad

Implemente políticas personalizadas de Checkov centralizadas

Tarea	Descripción	Habilidades requeridas
Añada el flujo de trabajo reutilizable de Checkov a todos los repositorios.	En este punto, debería tener un ejemplo de flujo de trabajo de Checkov que haga referencia al flujo de trabajo reutilizable. Copie el ejemplo del flujo de trabajo de Checkov que hace referencia al flujo de trabajo reutilizable en cada repositorio que lo requiera.	DevOps ingeniero
Cree un mecanismo para garantizar que Checkov se ejecute antes de las combinaciones.	Para asegurarte de que el flujo de trabajo de Checkov se ejecute para cada solicitud de extracción, crea una verificación de estado que requiera un flujo de trabajo de Checkov correcto antes de poder fusionar las solicitudes de extracción. GitHub te permite exigir que se ejecuten flujos de trabajo específicos antes	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	de poder fusionar las solicitud es de extracción.	
Cree un PAT para toda la organización y compártalo como un secreto.	Si su GitHub organización es visible públicamente, puede omitir este paso. Este patrón requiere que el flujo de trabajo de Checkov pueda descargar políticas personalizadas del repositor io de políticas personalizadas de su GitHub organización. Debe proporcionar permisos para que el flujo de trabajo de Checkov pueda acceder a esos repositorios. Para ello, cree un token de acceso personal (PAT) con permisos para leer los repositorios de la organizac ión. Comparta el PAT con los repositorios, ya sea como un secreto para toda la organizac ión (si tiene un plan de pago) o como un secreto en cada repositorio (versión gratuita) . En el código de ejemplo, el nombre predeterminado del secreto es `ORG_PAT`.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
(Opcional) Proteja los archivos de flujo de trabajo de Checkov para que no se modifiquen.	Para proteger los archivos de flujo de trabajo de Checkov de cambios no deseados, puede utilizar un archivo `CODEOWNERS`. Normalmente, el archivo `CODEOWNERS` se implementa en la raíz del directorio. Por ejemplo, para solicitar la aprobación del `secEng` grupo de su GitHub organización cuando se modifique el `checkov-scan.yaml` archivo, añada lo siguiente al archivo de `CODEOWNERS` un repositorio: `[Checkov] .github/workflows/checkov-scan.yaml @myOrg/secEng` Un archivo `CODEOWNERS` es específico del repositorio en el que reside. Para proteger el flujo de trabajo de Checkov que usa el repositorio, debe añadir (o actualizar) un archivo `CODEOWNERS` en cada repositorio. Para obtener más información acerca de la protección de los archivos de flujo de trabajo de Checkov, consulte Información adicional. Para obtener más	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	información sobre `CODEOWNERS` los archivos, consulta la documentación oficial de tu CI/CD proveedor (por ejemplo,). GitHub	

Recursos relacionados

- Información general de las políticas personalizadas de Checkov
- CloudFormation Escaneo de configuraciones
- GitHub Acciones: flujos de trabajo reutiliz

Información adicional

Escritura de archivos de flujo de trabajo de Checkov

Al escribir `checkov-scan.yaml`, tenga en cuenta cuándo quiere que se ejecute. La clave onde nivel superior determina cuándo se ejecuta el flujo de trabajo. En el repositorio de ejemplo, el flujo de trabajo se ejecutará cuando haya una solicitud de extracción dirigida a la rama `main` (y siempre que se modifique la rama de origen de esa solicitud de extracción). El flujo de trabajo también se puede ejecutar según sea necesario debido a la clave `workflow_dispatch`.

Puede cambiar las condiciones de activación del flujo de trabajo en función de la frecuencia con la que desee que este se ejecute. Por ejemplo, puede cambiar el flujo de trabajo para que se ejecute cada vez que se introduzca código en una rama; para ello, sustituya `pull_request` por `push` y quite la clave `branches`.

Puede modificar el archivo de flujo de trabajo de ejemplo que creó en un repositorio individual. Por ejemplo, puede ajustar el nombre de la rama de destino de `main` a `production` si el repositorio está estructurado en torno a una rama de `production`.

Protección de archivos de flujo de trabajo de Checkov

El análisis de Checkov proporciona información útil sobre posibles errores de configuración de seguridad. Sin embargo, es posible que algunos desarrolladores perciban esto como una barrera para su productividad e intenten eliminar o deshabilitar el flujo de trabajo de análisis.

Hay varias formas de abordar este problema, como enviar información más detallada sobre el valor a largo plazo del análisis de seguridad y documentar de manera más clara cómo implementar una infraestructura segura. Estos son importantes enfoques «flexibles» de DevSecOps la colaboración que pueden considerarse la solución a la causa raíz de este problema. Sin embargo, también puede utilizar controles técnicos, como un archivo `CODEOWNERS` que actúe como barrera de protección, para ayudar a los desarrolladores a seguir el camino correcto.

Prueba de un patrón en un entorno de pruebas

Para probar este patrón en un entorno de pruebas, siga estos pasos:

1. Cree una nueva GitHub organización. Cree un token con acceso de solo lectura a todos los repositorios de la organización. Como este token se usará en un entorno de pruebas y no en un entorno de pago, no podrá almacenarlo como secreto para toda la organización.
2. Cree un repositorio de `checkov` para almacenar la configuración de Checkov y un repositorio de `github-workflows` para almacenar la configuración del flujo de trabajo reutilizable. Rellene los repositorios con el contenido del repositorio de ejemplo.
3. Cree un repositorio de aplicaciones y copie y pegue el flujo de trabajo `checkov-scan.yaml` en su carpeta `.github/workflows`. Agregue un secreto al repositorio que contenga el PAT que creó para el acceso de solo lectura de la organización. El valor predeterminado del secreto es `ORG_PAT`.
4. Crea una solicitud de extracción que añada algo de Terraform o CloudFormation código al repositorio de aplicaciones. Checkov debería analizar esto y devolver un resultado.

Implementación de diagnósticos y solución de problemas de Kubernetes con tecnología de IA con la integración de K8sGPT y Amazon Bedrock

Ishwar Chauthaiwale, Muskan y Prafful Gupta, Amazon Web Services

Resumen

Este patrón demuestra cómo implementar diagnósticos y solución de problemas de Kubernetes con tecnología de IA mediante la integración de K8sGPT con el modelo Anthropic Claude v2 disponible en Amazon Bedrock. La solución proporciona un análisis en lenguaje natural y pasos para solucionar los problemas de los clústeres de Kubernetes mediante una arquitectura de host bastión segura. Al combinar la experiencia de K8sGPT en Kubernetes con las capacidades lingüísticas avanzadas de Amazon Bedrock DevOps , los equipos pueden identificar y resolver rápidamente los problemas de los clústeres. Con estas funcionalidades, es posible reducir el tiempo medio de resolución (MTTR) hasta en un 50 %.

Este patrón nativo en la nube utiliza Amazon Elastic Kubernetes Service (Amazon EKS) para la administración de Kubernetes. El patrón implementa las mejores prácticas de seguridad mediante las funciones adecuadas AWS Identity and Access Management (de IAM) y el aislamiento de la red. Esta solución es especialmente valiosa para las organizaciones que desean optimizar sus operaciones de Kubernetes y mejorar sus capacidades de solución de problemas con la ayuda de la IA.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS con los permisos adecuados
- AWS Command Line Interface (AWS CLI) instalado y configurado
- Un clúster de Amazon EKS
- Acceso al modelo Anthropic Claude 2 en Amazon Bedrock
- Un host bastión con la configuración de grupo de seguridad requerida
- K8sGPT instalado

Limitaciones

- El análisis de K8sGPT está limitado por el tamaño de la ventana de contexto del modelo Claude v2.

- Los límites de frecuencia de la API de Amazon Bedrock se aplican en función de las cuotas de su cuenta.
- Algunas Servicios de AWS no están disponibles en todas Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- Amazon EKS versión 1.31 o posteriores
- Modelo Claude 2 en Amazon Bedrock
- K8sGPT v0.4.2 o posteriores

Arquitectura

En el siguiente diagrama se muestra la arquitectura para el diagnóstico de Kubernetes con tecnología de IA mediante K8sGPT integrado con Amazon Bedrock en la Nube de AWS.

En la arquitectura se muestra el flujo de trabajo siguiente:

1. Los desarrolladores acceden al entorno a través de una conexión segura al host bastión. Esta EC2 instancia de Amazon sirve como punto de entrada seguro y contiene la instalación de la interfaz de línea de comandos (CLI) K8sgpt y las configuraciones necesarias.
2. El host bastión, configurado con roles de IAM específicos, establece conexiones seguras tanto con el clúster de Amazon EKS como con los puntos de conexión de Amazon Bedrock. K8sGPT se instala y configura en el host bastión para analizar los clústeres de Kubernetes.
3. Amazon EKS administra el plano de control de Kubernetes y los nodos de trabajo, lo que proporciona el entorno de destino para el análisis de K8sGPT. El servicio se ejecuta en varias zonas de disponibilidad dentro de una nube privada virtual (VPC), lo que ayuda a proporcionar una alta disponibilidad y resiliencia. Amazon EKS suministra datos operativos a través de la API de Kubernetes, lo que permite un análisis integral de clústeres.
4. K8sGPT envía los datos de análisis a Amazon Bedrock, que proporciona el modelo fundacional (FM) Claude v2 para el procesamiento de lenguaje natural. El servicio procesa el análisis del K8sGPT para generar explicaciones legibles para los humanos y ofrece sugerencias de corrección

detalladas basadas en los problemas identificados. Amazon Bedrock funciona como un servicio de IA sin servidor con alta disponibilidad y escalabilidad.

> **Note**
>
> A lo largo de este flujo de trabajo, IAM controla el acceso entre los componentes mediante roles y políticas, y administra la autenticación de las interacciones entre el host bastión, Amazon EKS y Amazon Bedrock. IAM implementa el principio de privilegio mínimo y permite una comunicación segura entre servicios en toda la arquitectura.

Automatización y escala

Las operaciones de K8sgpt pueden automatizarse y escalarse en varios clústeres de Amazon EKS a través de diversas herramientas. Servicios de AWS Esta solución admite la integración continua y la integración del despliegue continuo (CI/CD) mediante Jenkins, GitHub Actions o para análisis programados. AWS CodeBuild El operador K8sGPT permite la supervisión continua en el clúster con funcionalidades automatizadas de detección de problemas y generación de informes. Para despliegues a escala empresarial, puedes usar Amazon EventBridge para programar escaneos y activar respuestas automatizadas con scripts personalizados. AWS La integración del SDK permite el control programático en una gran flota de clústeres.

Tools (Herramientas)

Servicios de AWS

- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar Servicios de AWS mediante los comandos de su consola de línea de comandos.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar AWS Kubernetes sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.

Otras herramientas

- K8sGPT es una herramienta de código abierto con tecnología de IA que transforma la administración de Kubernetes. Actúa como experto virtual en ingeniería de confiabilidad del

sitio (SRE) y analiza, diagnostica y soluciona automáticamente los problemas del clúster de Kubernetes. Los administradores pueden interactuar con K8sGPT mediante un lenguaje natural y obtener información clara y práctica sobre el estado del clúster, los fallos de los pods y los fallos del servicio. Los analizadores integrados en la herramienta detectan una amplia gama de problemas, desde componentes mal configurados hasta limitaciones de recursos, y ofrecen easy-to-understand explicaciones y soluciones.

Prácticas recomendadas

- Implemente controles de acceso seguros mediante el acceso al AWS Systems Manager Session Manager host del bastión.
- Asegúrese de que la autenticación de K8sGPT utilice roles de IAM dedicados con permisos de privilegio mínimo para las interacciones de Amazon Bedrock y Amazon EKS. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.
- Configure el etiquetado de recursos, habilite el CloudWatch registro de Amazon para las pistas de auditoría e implemente la anonimización de los datos para la información confidencial.
- Haga copias de seguridad periódicas de las configuraciones de K8sGPT y, al mismo tiempo, establezca programas de análisis automatizados durante las horas de menor actividad para minimizar el impacto operativo.

Epics

Cómo agregar Amazon Bedrock a la lista de proveedores de backend de IA

Tarea	Descripción	Habilidades requeridas
Configurar Amazon Bedrock como proveedor de backend de IA para K8sGPT.	Para configurar Amazon Bedrock como el proveedor de backend de la IA r para K8sgpt, utilice el siguiente comando: AWS CLI `k8sgpt auth add -b amazonbedrock \ -r us-west-2 \`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`-m anthropic.claude-v2 \`
	`-n endpoint-name`
	
	En el comando de ejemplo se utiliza `us-west-2` para la Región de AWS. Sin embargo, puede seleccionar otra región, siempre que tanto el clúster de Amazon EKS como el modelo de Amazon Bedrock correspondiente estén disponibles y habilitados en la región seleccionada.
	
	Para comprobar si `amazonbedrock` se ha agregado a la lista de proveedores de backend de IA y si se encuentra en estado `Active`, ejecute el siguiente comando:
	
	`k8sgpt auth list`
	
	A continuación, se muestra un ejemplo de la salida esperada de este comando:
	
	`Default:`
	`> openai`
	`Active:`
	`> amazonbedrock`
	`Unused:`
	`> openai`
	`> localai`
	`> ollama`	

Tarea	Descripción	Habilidades requeridas

	`> azureopenai`
	`> cohere`
	`> amazonsagemaker`
	`> google`
	`> noopai`
	`> huggingface`
	`> googlevertexai`
	`> oci`
	`> customrest`
	`> ibmwatsonxai`	

Analizar los recursos mediante un filtro

Tarea	Descripción	Habilidades requeridas

Ver una lista de filtros disponibles.	Para ver la lista de todos los filtros disponibles, utilice el siguiente AWS CLI comando:
	`k8sgpt filters list`
	A continuación, se muestra un ejemplo de la salida esperada de este comando:
	`Active:`
	`> Deployment`
	`> ReplicaSet`
	`> PersistentVolumeCl aim`
	`> Service`
	`> CronJob`
	`> Node`
	`> MutatingWebhookCon figuration`
	`> Pod`
	`> Ingress`
	`> StatefulSet`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`> ValidatingWebhookConfiguration`	

Tarea	Descripción	Habilidades requeridas

Analizar un pod en un espacio de nombres específico mediante un filtro.	Este comando es útil para la depuración selectiva de problemas específicos de los pods dentro de un clúster de Kubernetes, utilizando las funcionalidades de IA de Amazon Bedrock para analizar y explicar los problemas que encuentra.
	
	Para escanear un pod en un espacio de nombres específic o mediante un filtro, utilice el siguiente comando: AWS CLI
	
	`k8sgpt analyze --backend amazonbedrock --explain --filter Pod -n default`
	
	A continuación, se muestra un ejemplo de la salida esperada de este comando:
	
	`100% |################################################################| (1/1, 645 it/s)`
	
	`AI Provider: amazonbedrock`
	
	`0: Pod default/crashme()`
	`- Error: the last termination reason is Error container=crashme pod=crashme`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`Error: The pod named crashme terminated because the container named crashme crashed.` `Solution: Check logs for crashme pod to identify reason for crash. Restart pod or redeploy application to resolve crash.`	

Tarea	Descripción	Habilidades requeridas

Analizar una implementación en un espacio de nombres específico mediante un filtro.	Este comando es útil para identificar y solucionar problemas específicos de la implementación, especialm ente cuando el estado real no coincide con el estado deseado.
	
	Para escanear una implement ación en un espacio de nombres específico mediante un filtro, utilice el siguiente comando: AWS CLI
	
	`k8sgpt analyze -- backend amazonbedrock --explain --filter Deployment -n default`
	
	A continuación, se muestra un ejemplo de la salida esperada de este comando:
	
	`100% |################## ################## ################## #####| (1/1, 10 it/min)`
	
	`AI Provider: amazonbed rock`
	
	`0: Deployment default/n ginx()`
	`- Error: Deployment default/nginx has 1 replicas but 2 are available`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	<pre>Error: The Deploymen
	t named nginx in the
	default namespace has
	1 replica specified
	but 2 pod replicas are
	running.
	Solution: Check if
	any other controlle
	rs like ReplicaSet
	or StatefulSet have
	created extra pods.
	Delete extra pods or
	adjust replica count to
	match available pods.</pre>	

Analizar un nodo en un espacio de nombres específico mediante un filtro.	Para escanear un nodo de un espacio de nombres específico mediante un filtro, utilice el siguiente comando: AWS CLI
	<pre>k8sgpt analyze --backend
	amazonbedrock --
	explain --filter Node -n
	default</pre>
	A continuación, se muestra un ejemplo de la salida esperada de este comando:
	<pre>AI Provider: amazonbed
	rock
	
	No problems detected</pre>
		AWS DevOps

Analizar las salidas detalladas

Tarea	Descripción	Habilidades requeridas

Obtener salidas detalladas.	Para obtener resultados detallados, utilice el siguiente AWS CLI comando:
	
	`k8sgpt analyze --backend amazonbedrock --explain --ouput json`
	
	A continuación, se muestra un ejemplo de la salida esperada de este comando:
	
	`{ "provider": "amazonbedrock", "errors": null, "status": "ProblemDetected", "problems": 1, "results": [ { "kind": "Pod", "name": "default/crashme", "error": [ { "Text": "the last termination reason is Error container=crashme pod=crashme", "Kubernetes Doc": "", "Sensitive": [] } ],`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	<pre>"details": " Error: The pod named crashme terminated because the container named crashme crashed. \nSolution: Check logs for crashme pod to identify reason for crash. Restart pod or redeploy application to resolve crash.", "parentObject": "" }] }</pre>	

Comprobar los pods problemáticos.	Para comprobar si hay pods problemáticos específicos, usa el siguiente AWS CLI comando:
	<pre>kubectl get pods --all-namespaces | grep -v Running</pre>A continuación, se muestra un ejemplo de la salida esperada de este comando:
	<pre>NAMESPACE NAME READY STATUS RESTARTS AGE
	
	default crashme 0/1 CrashLoopBackOff 260(91s ago) 21h</pre>
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

Obtener información específica de la aplicación.	Este comando resulta especialmente útil cuando:
	• Desea centrarse en una aplicación específica de su clúster.
	• Utiliza las etiquetas de forma eficaz para organizar los recursos de Kubernetes.
	• Debe comprobar rápidamente el estado de un componente de la aplicación en particular.
	
	Para obtener información específica de la aplicación, use el siguiente comando:
	`k8sgpt analyze --backend amazonbedrock --explain -L app=nginx -n default`
	
	A continuación, se muestra un ejemplo de la salida esperada de este comando:
	`AI Provider: amazonbedrock`
	
	`No problems detected`	

Recursos relacionados

Blogs de AWS

- Automate Amazon EKS troubleshooting using an Amazon Bedrock agentic workflow
- Use K8sGPT and Amazon Bedrock for simplified Kubernetes cluster maintenance

AWS documentación

- AWS CLI comandos: create-cluster y describe-cluster
- Introducción a Amazon EKS (documentación de Amazon EKS)
- Prácticas recomendadas de seguridad en IAM (documentación de IAM)

Otros recursos

- K8sGPT

Detecta automáticamente los cambios e inicia diferentes CodePipeline canalizaciones para un monorepo en CodeCommit

Helton Ribeiro, Petrus Batalha y Ricardo Morais, Amazon Web Services

Resumen

Aviso: ya no AWS Cloud9 está disponible para nuevos clientes. Los clientes actuales de AWS Cloud9 pueden seguir utilizando el servicio con normalidad. Más información

Este patrón le ayuda a detectar automáticamente los cambios en el código fuente de una aplicación basada en monorepo AWS CodeCommit y, a continuación, a iniciar una canalización AWS CodePipeline que ejecute la integración continua y la entrega continuas (CI/CD) automation for each microservice. This approach means that each microservice in your monorepo-based application can have a dedicated CI/CDcanalización), lo que garantiza una mejor visibilidad, un intercambio más sencillo del código y una mejor colaboración, estandarización y capacidad de descubrimiento.

La solución descrita en este patrón no realiza ningún análisis de dependencia entre los microservicios del monorepo. Solo detecta los cambios en el código fuente e inicia la canalización correspondiente. CI/CD

El patrón AWS Cloud9 se utiliza como entorno de desarrollo integrado (IDE) y AWS Cloud Development Kit (AWS CDK) para definir una infraestructura mediante dos CloudFormation pilas: `MonoRepoStack` y. `PipelinesStack` La `MonoRepoStack` pila crea la entrada monorepo AWS CodeCommit y la AWS Lambda función que inicia las canalizaciones. CI/CD La pila `PipelinesStack` define su infraestructura de canalizaciones.

> **Important**
>
> El flujo de trabajo de este patrón es una prueba de concepto (PoC). Le recomendamos que utilice esta opción solo en un entorno de prueba. Si desea utilizar el enfoque de este patrón en un entorno de producción, consulte las prácticas recomendadas de seguridad en IAM en la documentación AWS Identity and Access Management (IAM) y realice los cambios necesarios en sus funciones de IAM y. Servicios de AWS

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta activa. AWS
- AWS Command Line Interface (AWS CLI), instalada y configurada. Para obtener más información, consulte Instalación, actualización y desinstalación de AWS CLI en la AWS CLI documentación.
- Python 3 y `pip` instalados en su equipo local. Para obtener más información, consulte la documentación de Python.
- AWS CDK instalado y configurado Para obtener más información, consulte Introducción a AWS CDK la AWS CDK documentación.
- Un AWS Cloud9 IDE, instalado y configurado. Para obtener más información, consulte Configuración AWS Cloud9 en la AWS Cloud9 documentación.
- El repositorio de activadores multicanalización de GitHub AWS CodeCommit monorepo, clonado en su máquina local.
- Un directorio existente que contiene el código de la aplicación con el que desea crear e implementar. CodePipeline
- Familiaridad y experiencia con las DevOps mejores prácticas en el Nube de AWS. Para aumentar su familiaridad DevOps, puede utilizar el patrón Construir una arquitectura de acoplamiento flexible con microservicios utilizando DevOps prácticas y AWS Cloud9 en el AWS sitio web de orientación prescriptiva.

Arquitectura

El siguiente diagrama muestra cómo usar el AWS CDK para definir una infraestructura con dos AWS CloudFormation pilas: y. `MonoRepoStack` `PipelinesStack`

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El proceso de arranque utiliza el AWS CDK para crear las AWS CloudFormation pilas y. `MonoRepoStack` `PipelinesStack`
2. La `MonoRepoStack` pila crea el CodeCommit repositorio para la aplicación y la función `monorepo-event-handler` Lambda que se inicia después de cada confirmación.
3. La `PipelinesStack` pila crea las canalizaciones CodePipeline iniciadas por la función Lambda. Cada microservicio debe tener una canalización de infraestructura definida.
4. La canalización para `microservice-n` la inicia la función Lambda e inicia sus CI/CD etapas aisladas que se basan en el código fuente de. CodeCommit

5. La canalización para `microservice-1` la inicia la función Lambda e inicia sus CI/CD etapas aisladas que se basan en el código fuente de. CodeCommit

El siguiente diagrama muestra el despliegue de las AWS CloudFormation pilas `MonoRepoStack` y `PipelinesStack` en una cuenta.

1. Un usuario cambia el código de uno de los microservicios de la aplicación.
2. El usuario envía los cambios de un repositorio local a un CodeCommit repositorio.
3. La actividad de envío inicia la función Lambda que recibe todos los envíos al repositorio. CodeCommit
4. La función de Lambda lee un parámetro en el Almacén de parámetros, una capacidad de AWS Systems Manager, para recuperar el ID de confirmación más reciente. El parámetro tiene el formato de denominación:. `/MonoRepoTrigger/{repository}/{branch_name}/LastCommit` Si no se encuentra el parámetro, la función Lambda lee el último ID de confirmación del CodeCommit repositorio y guarda el valor devuelto en el almacén de parámetros.
5. Tras identificar el ID de confirmación y los archivos modificados, la función Lambda identifica las canalizaciones de cada directorio de microservicios e inicia la canalización requerida. CodePipeline

Tools (Herramientas)

- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software para definir la infraestructura de nube en código y aprovisionarla mediante ella. CloudFormation
- Python es un lenguaje de programación que le permite trabajar rápidamente e integrar sistemas de manera más eficaz.

Código

El código fuente y las plantillas de este patrón están disponibles en el GitHub AWS CodeCommit repositorio multipipeline triggers de monorepo.

Prácticas recomendadas

- Este ejemplo de arquitectura no incluye soluciones de supervisión para la infraestructura implementada. Si desea implementar esta solución en un entorno de producción, le

recomendamos que habilite la supervisión. Para obtener más información, consulte Supervise sus aplicaciones sin servidor con CloudWatch Application Insights en la AWS Serverless Application Model documentación ().AWS SAM

- Al editar el código de muestra que proporciona este patrón, siga las prácticas recomendadas para desarrollar e implementar la infraestructura de nube de la AWS CDK documentación.
- Al definir las canalizaciones de microservicios, revise las prácticas recomendadas de seguridad de la AWS CodePipeline documentación.
- También puede comprobar las prácticas recomendadas en su AWS CDK código mediante la utilidad cdk-nag. Esta herramienta utiliza un conjunto de reglas, agrupadas por paquetes, para evaluar el código. Estos son los paquetes disponibles:
  - AWS Biblioteca de soluciones
  - Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA), norma de seguridad
  - Instituto Nacional de Estándares y Tecnología (NIST) 800-53, rev. 4
  - NIST 800-53 rev. 5
  - La norma de seguridad de datos del sector de pagos con tarjeta (PCI DSS), versión 3.2.1

Epics

Configuración del entorno

Tarea	Descripción	Habilidades requeridas
Cree un entorno virtual de Python.	En su AWS Cloud9 IDE, cree un entorno virtual de Python e instale las dependencias necesarias ejecutando el siguiente comando: `make install`	Desarrollador
Arranca el Cuenta de AWS y Región de AWS para. AWS CDK	Inicie la región Cuenta de AWS y requerida ejecutando el siguiente comando: `make bootstrap account-id=<your-`	Desarrollador

Tarea	Descripción	Habilidades requeridas
	`AWS-account-ID> region=<required-region>`	

Cómo añadir una nueva canalización para un microservicio

Tarea	Descripción	Habilidades requeridas
Añada su código de muestra al directorio de su aplicación.	Añada el directorio que contiene el código de la aplicación de muestra al `monorepo-sample` directorio del repositorio clonado de GitHub AWS CodeCommit monorepo multi-pipeline triggers.	Desarrollador
Edite el archivo `monorepo-main.json` .	Añada el nombre del directorio del código de la aplicación y el nombre de la canalización al archivo `monorepo-main.json` del repositorio clonado .	Desarrollador
Cree la canalización.	En el directorio `Pipelines` del repositorio , añada la canalización `class` de su aplicación. El directorio contiene dos archivos de ejemplo, `pipeline_hotsite.py` y `pipeline_demo.py` . Cada archivo tiene tres etapas: código fuente, compilación e implementación.	Desarrollador

Tarea	Descripción	Habilidades requeridas
	Puede copiar uno de los archivos y modificarlo según los requisitos de su aplicació n.	

Tarea	Descripción	Habilidades requeridas

Edite el archivo `monorepo_config.py` .	En `service_map` , añada el nombre del directorio de su aplicación y la clase que creó para la canalización.
	
	Por ejemplo, en el siguiente código, se muestra una definición de canalización en el directorio `Pipelines` que usa un archivo llamado `pipeline_mysample.py` con una clase `MySampleP ipeline` :
	
	`...`
	`# Pipeline definition imports`
	`from pipelines.pipeline_demo import DemoPipeline`
	`from pipelines.pipeline_hotsite import HotsitePipeline`
	`from pipelines.pipeline_mysample import MySampleP ipeline`
	
	`### Add your pipeline configuration here`
	`service_map: Dict[str, ServicePipeline] = {`
	`# folder-name -> pipeline-class`
	`'demo': DemoPipel ine(),`
	`'hotsite': HotsitePipeline(),`
		Desarrollador

Tarea	Descripción	Habilidades requeridas
	`'mysample': MySamplePipeline() }`	

Despliega la pila MonoRepoStack

Tarea	Descripción	Habilidades requeridas
Despliegue la AWS CloudFormation pila.	Ejecute el `make deploy-core` comando para implementar la AWS CloudFormation `MonoRepoStack` pila con los valores de los parámetros predeterminados en el directorio raíz del repositorio clonado. Puede cambiar el nombre del repositorio si ejecuta el comando `make deploy-core monorepo-name=<repo_name>` . **Note** Puede implementar ambas canalizaciones simultáneamente mediante el comando `make deploy monorepo-name=<repo_name>` .	Desarrollador

Tarea	Descripción	Habilidades requeridas
Valide el CodeCommit repositorio.	Valide si sus recursos se crearon mediante la ejecución del comando `aws codecommit get-repository --repository-name <repo_name>` . **Important** Como la CloudFormation pila crea el CodeCommit repositorio en el que se almacena el monorepo, no ejecute el `cdk destroy MonoRepoStack` comando si ha empezado a introducir modificaciones en él.	Desarrollador
Valide los resultados de la CloudFormation pila.	Valide que la CloudFormation `MonoRepoStack` pila se haya creado y configurado correctamente ejecutando el siguiente comando: `aws cloudformation list-stacks --stack-status-filter CREATE_COMPLETE --query 'StackSummaries[?StackName == 'MonoRepoStack']'`	Desarrollador

Implemente la PipelinesStack pila

Tarea	Descripción	Habilidades requeridas
Despliegue la CloudFormation pila.	La AWS CloudFormation `PipelinesStack` pila debe desplegarse después de `MonoRepoStack` desplegar la. La pila aumenta de tamaño cuando se añaden nuevos microservicios al código base del monorepo y se vuelve a implementar cuando se incorpora un nuevo microserv icio. Implemente la Pipelines Stack pila ejecutando el `make deploy-pipelines` comando. **Note** También puede ejecutar el comando `make deploy monorepo-name=<rep o_name>` para implementar simultáne amente ambas canalizaciones. El siguiente ejemplo de resultado muestra cómo la `PipelinesStacks`	Desarrollador

Tarea	Descripción	Habilidades requeridas
	implementación imprime URLs los microservicios al final de la implementación: `Outputs: PipelinesStack.dem ourl = .cloudfront.net PipelinesStack.hotsi teurl = .cloudfro nt.net`	
Valide los resultados de la AWS CloudFormation pila.	Valide que la AWS CloudForm ation `PipelinesStacks` pila se haya creado y configurado correctamente ejecutando el siguiente comando: `aws cloudformation list-stacks --stack-s tatus-filter CREATE_CO MPLETE UPDATE_COMPLETE --query 'StackSum maries[?StackName == 'PipelinesStack']'`	Desarrollador

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Elimina tus AWS CloudForm ation pilas.	Ejecute el comando `make destroy`.	Desarrollador
Elimine los buckets de S3 para sus canalizaciones.	1. Inicie sesión en la Consola de administración de AWS y abra la consola de	Desarrollador

Tarea	Descripción	Habilidades requeridas
	Amazon Simple Storage Service (Amazon S3). 2. Elimine los buckets de S3 asociados a sus canalizaciones y que tengan el siguiente nombre: `pipelinesstack-codepipeline*` .	

Resolución de problemas

Problema	Solución
He encontrado AWS CDK problemas.	Consulte Solución de AWS CDK problemas comunes en la documentación de AWS CDK.
Inserté mi código de microservicio, pero la canalización de microservicios no funcionó.	Validación de la configuración Verifique la configuración de la rama: • Asegúrese de que envía su código a la rama correcta. Esta canalización está configurada para que se ejecute solo cuando se realicen cambios en la rama de `main`. Los envíos a otras ramas no inician la canalización a menos que estén configurados específicamente para ello. • Después de insertar el código, compruebe si la confirmación está visible AWS CodeCommit para asegurarse de que la inserción se ha realizado correctamente y de que la conexión entre su entorno local y el repositorio está intacta. Actualice sus credenciales si hay problemas al insertar el código.

Problema	Solución
	Valide los archivos de configuración: • Confirme que la variable `service_map` en `monorepo_config.py` refleja con precisión la estructura de directorios actual de sus microservicios. Esta variable desempeña un papel crucial a la hora de asignar la inserción del código en la canalización correspondiente. • Asegúrese de que `monorepo-main.json` esté actualizado para incluir la nueva asignación en su microservicio. Este archivo es esencial para que la canalización reconozca y gestione correctamente los cambios en el microservicio. Solución de problemas en la consola AWS CodePipeline comprueba: • En el Consola de administración de AWS, confirma que estás en el Región de AWS lugar donde está alojada tu canalización. Abre la CodePipeline consola y comprueba si se ha iniciado la canalización correspondiente a tu microservicio. Análisis de errores: si la canalización se inició pero falló, revise los mensajes de error o los registros proporcionados por usted CodePipeline para saber qué ha fallado. AWS Lambda solución de problemas: • En la consola de AWS Lambda, abra la función de Lambda `monorepo-event-`

Problema	Solución
	`handler` . Compruebe que la función se haya iniciado en respuesta a la inserción del código. Análisis de registros: examine los registros de la función de Lambda para detectar cualquier problema. Los registros pueden proporcionar información detallada sobre lo que ocurrió cuando se ejecutó la función y lo ayudarán a identificar si la función procesó el evento según lo esperado.

Problema	Solución
Necesito volver a implementar todos mis microservicios.	Existen dos métodos para volver a implementar todos los microservicios. Seleccione la opción que mejor se adapte a sus necesidades. Método 1: Eliminar un parámetro del almacén de parámetros Este método implica eliminar un parámetro específico del almacén de parámetros de Systems Manager que rastrea el último ID de confirmaciónq que se usó para la implement ación. Al eliminar este parámetro, el sistema se ve obligado a volver a implementar todos los microservicios en el siguiente desencadenador, ya que lo percibe como un estado nuevo. Pasos: 1. Busque la entrada específica del almacén de parámetros que contiene el ID de confirmac ión o un marcador de implementación relacionado con el monorepo. El formato del nombre del parámetro es el siguiente: `"/MonoRepoTrigger/{repository}/{branch_name}/LastCommit"` . 2. Puede hacer una copia de seguridad del valor del parámetro si es indispensable o si desea mantener un registro del estado de la implementación antes de restablecerlo. 3. Utilice las Consola de administración de AWS teclas AWS CLI, o SDKs para eliminar el parámetro identificado. Esta acción restablece el marcador de implementación. 4. Tras la eliminación, la siguiente inserción en el repositorio debería provocar que el

Problema	Solución
	sistema implemente todos los microserv icios, ya que buscará la última confirmación que indique la implementación. Ventajas: • Esto es sencillo y rápido de implementar con unos pasos mínimos. • No es necesario realizar cambios arbitrari os en el código para iniciar las implement aciones. Desventajas: • Control menos detallado sobre el proceso de implementación. • Potencialmente arriesgado si el almacén de parámetros se utiliza para gestionar otras configuraciones críticas. Método 2: Insertar una confirmación en cada subcarpeta de monorepo Este método implica realizar un cambio menor e insertarlo en cada subcarpeta de microserv icios del monorepo para iniciar sus canalizac iones individuales. Pasos: 1. Enumere todos los microservicios del monorepo que necesitan ser redistribuidos. 2. En cada microservicio, realice un cambio mínimo y que no afecte a la subcarpeta. Esto puede consistir en actualizar un archivo

Problema	Solución
	`README`, añadir un comentario en un archivo de configuración o realizar cualquier cambio que no afecte a la funcionalidad del servicio. 3. Confirme estos cambios con un mensaje claro (como “Iniciar la nueva implementación de los microservicios”) y envíelos al repositor io. Asegúrese de enviar los cambios a la rama que inicia la implementación. 4. Supervise las canalizaciones de cada microservicio para confirmar que se han iniciado y completado correctamente. Ventajas: • Proporciona un control detallado sobre los microservicios que se vuelven a implement ar. • Es más seguro porque no implica eliminar los parámetros de configuración que podrían usarse para otros fines. Desventajas: • Consume más tiempo, especialmente si se trabaja con una gran cantidad de microserv icios. • Requiere realizar cambios de código innecesarios que podrían saturar el historial de confirmaciones.

Recursos relacionados

- Integración y entrega continuas (CI/CD) mediante CDK Pipelines (documentación)AWS CDK

- módulo aws-cdk/pipelines (referencia de la API)AWS CDK

Integre un repositorio de Bitbucket con AWS Amplify mediante AWS CloudFormation

Alwin Abraham, Amazon Web Services

Resumen

AWS Amplify le ayuda a implementar y probar sitios web estáticos rápidamente sin tener que configurar la infraestructura que normalmente se requiere. Puede implementar el enfoque de este patrón si su organización quiere usar Bitbucket como control de código fuente, ya sea para migrar el código de una aplicación existente o para crear una nueva aplicación. Al utilizar AWS CloudFormation para configurar Amplify automáticamente, proporciona visibilidad de las configuraciones que utiliza.

Este patrón describe cómo crear una canalización y un entorno de implementación de integración y despliegue continuos (CI/CD) front-end mediante AWS CloudFormation para integrar un repositorio de Bitbucket con AWS Amplify. El enfoque del patrón significa que puede crear una canalización de frontend de Amplify para implementaciones repetibles.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa
- Una cuenta de Bitbucket activa con acceso de administrador
- Acceder a un terminal que usa cURL o la aplicación Postman
- Familiaridad con Amplify
- Familiaridad con AWS CloudFormation
- Familiaridad con los archivos con formato YAML

Arquitectura

Pila de tecnología

- Amplify

- AWS CloudFormation
- Bitbucket

Tools (Herramientas)

- AWS Amplify: Amplify ayuda a los desarrolladores a desarrollar e implementar aplicaciones móviles y web impulsadas por la nube.
- AWS CloudFormation: AWS CloudFormation es un servicio que le ayuda a modelar y configurar sus recursos de AWS para que pueda dedicar menos tiempo a gestionarlos y más a centrarse en las aplicaciones que se ejecutan en AWS.
- Bitbucket: Bitbucket es una solución de gestión de repositorios de Git diseñada para equipos profesionales. Le brinda un lugar central para administrar los repositorios de Git, colaborar en su código fuente y guiarle a través del flujo de desarrollo.

Código

El `bitbucket-amplify.yml` archivo (adjunto) contiene la CloudFormation plantilla de AWS para este patrón.

Epics

Configurar el repositorio de Bitbucket

Tarea	Descripción	Habilidades requeridas
(Opcional) Cree un repositorio de Bitbucket.	1. Inicie sesión en su cuenta de Bitbucket y crea un repositorio nuevo. Para obtener más informaci ón al respecto, consulte Crear un repositorio de Git en la documentación de Bitbucket. 2. Registrar el nombre del espacio de trabajo.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Note También puede utilizar un repositorio de Bitbucket ya existente.	
Abra la configuración del espacio de trabajo.	1. Abra el espacio de trabajo y seleccione la pestaña Repositorio. 2. Seleccione el repositorio que desee integrar con AmplifyAmplify. 3. Seleccione el nombre del espacio de trabajo que está por encima del nombre del repositorio. 4. En la barra lateral, seleccione Configuración.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Crea un OAuth consumidor.	1. En la sección Aplicaciones y funciones, selecciona OAuth consumidores y, a continuación, selecciona Añadir consumidor. 2. Escriba un nombre para la secuencia, por ejemplo, `Amplify Integration .` 3. Introduzca una URL de devolución de llamada. Aunque este campo es obligatorio, no se utiliza para completar la integración, por lo que el valor podría ser `http://localhost:3000` 4. Marque la casilla Se trata de un consumidor privado. 5. Elija los siguientes permisos: • Proyecto – `Read` • Repositorios – `Admin` • Solicitudes de extracción – `Read` • Webhooks, y `Read Write` 6. Deje las opciones predeterminadas para todos los demás campos y elija Enviar. 7. Registra la clave y el secreto que se generan.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Obtenga el token de OAuth acceso.	1. Abra una ventana del terminal y ejecute el siguiente comando: `curl -X POST -u "KEY:SECRET" https://bitbucket.org/site/oauth2/access_token -d grant_type=client_credentials` **Important** Sustituya `KEY` y `SECRET` por la clave y el secreto que registró anteriormente. 2. Registre el token de acceso sin utilizar las comillas. El token solo es válido durante un tiempo limitado y el tiempo predeterminado es de dos horas. Debe ejecutar la CloudFormation plantilla de AWS en este período de tiempo.	DevOps ingeniero

Cree e implemente el CloudFormation stack de AWS

Tarea	Descripción	Habilidades requeridas
Descargue la CloudFormation plantilla de AWS.	Descargue la CloudFormation plantilla de `bitbucket-amplify.yml` AWS (adjunta). Esta plantilla crea la CI/CD canalización en Amplify, además del proyecto y la sucursal de Amplify.	
Cree e implemente la CloudFormation pila de AWS.	1. Inicie sesión en la consola de administración de AWS en la región de AWS en la que desee realizar la implementación y abra la CloudFormation consola de AWS. 2. Seleccione Crear pila (con nuevos recursos) y, a continuación, Cargar un archivo de plantilla. 3. Cargue el archivo `bitbucket-amplify.yml` . 4. Seleccione Siguiente, introduzca un nombre de pila y, a continuación, introduzca los siguientes parámetros: • Token de acceso: pegue el token de OAuth acceso que creó anteriormente. • URL del repositorio: añada la URL del	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	repositorio del proyecto de Bitbucket. La URL tiene el siguiente formato: `https://bitbucket.org/<WORKSPACE_NAME>/<REPO_NAME>` • Nombre de la sucursal: debe coincidir con el nombre de una rama de su repositorio de Bitbucket. No es necesario que esta rama exista cuando ejecute la CloudFormation pila de AWS, pero es necesaria para implementar el código en el entorno. • Nombre del proyecto: este es el nombre que se debe asociar al proyecto Amplify. 5. Seleccione Siguiente y después Crear pilas.	

Pruebe la CI/CD tubería

Tarea	Descripción	Habilidades requeridas
Implementar el código en la rama de su repositorio.	1. Clone su repositorio de Bitbucket ejecutando el siguiente comando:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`git clone https://bitbucket.org/<WORKSPACE_NAME>/<REPO_NAME>` 2. Consulte el nombre de la rama que se utilizó al ejecutar el CloudFormation script de AWS. Para crear y comprobar una nueva rama, ejecute el comando `git checkout -b <BRANCH_NAME>` . Para revisar una rama existente , ejecute el comando `git checkout <BRANCH_NAME>` 3. Introduzca el código en la rama y envíelo a la rama remota ejecutando los comandos `git commit` y `git push`. 4. Amplify luego crea e implementa la aplicación. Para obtener más información sobre esto, consulte Comandos básicos de Git en la documentación de Bitbucket .	

Recursos relacionados

Métodos de autenticación (documentación de Atlassian)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Lance un CodeBuild proyecto en todas las cuentas de AWS mediante Step Functions y una función de proxy Lambda

Richard Milner-Watts y Amit Anjarlekar, Amazon Web Services

Resumen

Este patrón demuestra cómo lanzar de forma asíncrona un CodeBuild proyecto de AWS en varias cuentas de AWS mediante AWS Step Functions y una función de proxy de AWS Lambda. Puedes usar la máquina de estados Step Functions de muestra del patrón para probar el éxito de tu CodeBuild proyecto.

CodeBuild le ayuda a lanzar tareas operativas mediante la interfaz de línea de comandos de AWS (AWS CLI) desde un entorno de ejecución totalmente gestionado. Puede cambiar el comportamiento de su CodeBuild proyecto en tiempo de ejecución anulando las variables de entorno. Además, se puede utilizar CodeBuild para gestionar los flujos de trabajo. Para obtener más información, consulte las herramientas del catálogo de servicios en el sitio web de AWS Workshop y Programe trabajos en Amazon RDS para PostgreSQL con AWS y EventBridge Amazon en el blog de bases de datos de CodeBuild AWS.

Requisitos previos y limitaciones

Requisitos previos

- Dos cuentas de AWS activas: una cuenta de origen para invocar una función de proxy de Lambda con Step Functions y una cuenta de destino para crear un CodeBuild proyecto de muestra remoto

Limitaciones

- Este patrón no se puede utilizar para copiar artefactos entre cuentas.

Arquitectura

En el siguiente diagrama, se muestra la arquitectura que crea este patrón.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. La máquina de estado de Step Functions analiza el mapa de entrada proporcionado e invoca la función de proxy de Lambda (`codebuild-proxy-lambda`) para cada cuenta, región y proyecto que haya definido.
2. La función de proxy de Lambda usa AWS Security Token Service (AWS STS) para asumir un rol de proxy de IAM (`codebuild-proxy-role`), que está asociado a una política de IAM (`codebuild-proxy-policy`) en la cuenta de destino.
3. Con el rol asumido, la función Lambda lanza el CodeBuild proyecto y devuelve el identificador del CodeBuild trabajo. La máquina de estado Step Functions realiza un bucle y sondea el CodeBuild trabajo hasta recibir un estado de éxito o fracaso.

En la siguiente imagen se muestra la lógica de la máquina de estado.

Pila de tecnología

- AWS CloudFormation
- CodeBuild
- IAM
- Lambda
- Step Functions
- X-Ray

Tools (Herramientas)

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS CloudFormation Designer proporciona un editor JSON y YAML integrado que le ayuda a ver y editar CloudFormation plantillas.
- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la

capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de AWS Lambda y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial.
- AWS X-Ray le ayuda a recopilar datos sobre las solicitudes que atiende su aplicación y proporciona herramientas que puede utilizar para ver, filtrar y obtener información sobre esos datos para identificar problemas y oportunidades de optimización.

Código

El código de muestra para este patrón está disponible en el repositorio de GitHub Cross Account CodeBuild Proxy. Este patrón utiliza la biblioteca AWS Lambda Powertools para Python para proporcionar funciones de registro y rastreo. Para obtener más información sobre esta biblioteca y sus utilidades, consulte Powertools for AWS Lambda (Python).

Prácticas recomendadas

1. Ajuste los valores del tiempo de espera en la máquina de estado de Step Functions para minimizar las solicitudes de sondeo sobre el estado del trabajo. Utilice el tiempo de ejecución previsto para el CodeBuild proyecto.
2. Ajusta la `MaxConcurrency` propiedad del mapa en Step Functions para controlar cuántos CodeBuild proyectos se pueden ejecutar en paralelo.
3. Si es necesario, revise el código de ejemplo para ver si está listo para producción. Considera qué datos podría registrar la solución y si el CloudWatch cifrado predeterminado de Amazon es suficiente.

Epics

Crear la función proxy Lambda y el rol de IAM asociado en la cuenta de origen

Tarea	Descripción	Habilidades requeridas
Registre la cuenta de AWS IDs.	IDs Se requiere una cuenta de AWS para configurar el acceso a todas las cuentas.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Registre el ID de cuenta de AWS de sus cuentas de origen y destino. Para obtener más información, consulte Cómo encontrar el ID de su cuenta de AWS en la documentación de IAM.	

Tarea	Descripción	Habilidades requeridas
Descargue las CloudFormation plantillas de AWS.	1. Descargue la CloudFormation plantilla de `sample_target_codebuild_template.yaml` AWS del GitHub repositorio para este patrón. 2. Descargue la CloudFormation plantilla de `codebuild_lambda_proxy_template.yaml` AWS del GitHub repositorio para este patrón. **Note** En las CloudFormation plantillas de AWS, `<SourceAccountId>` es el ID de la cuenta de AWS de la cuenta de origen y `<TargetAccountId>` es el ID de la cuenta de AWS de la cuenta de destino.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Cree e implemente la CloudFormation pila de AWS.	1. Inicie sesión en la consola de administración de AWS de su cuenta de origen, abra la CloudFormation consola de AWS y, a continuación, elija Stacks. 2. Seleccione Crear pila y, a continuación, Con nuevos recursos (estándar). 3. Para Origen de plantilla, elija Cargar un archivo de plantilla. 4. En Cargar un archivo de plantilla, seleccione un archivo y, a continuac ión, el archivo descargad `ocodebuild_lambda_p roxy_template.yaml` . Seleccione Siguiente. 5. En Nombre de pila, especifique un nombre para la pila (por ejemplo, `codebuild-lambda-p roxy`). 6. **Note** Reemplace el parámetro `crossAcco untTarget RoleArn` con su `<TargetAc countId>`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	(por ejemplo, `<arn:aws:iam::123456789012:role/proxy-lambda-codebuild-role>`). : No es necesario que actualice el valor predeterminado del parámetro `targetCodeBuildProject` .	
	7. Seleccione Siguiente, acepte las opciones de creación de pilas predeterminadas y, a continuación, Siguiente. 8. Seleccione la casilla Acepto que AWS CloudFormation podría crear recursos de IAM con nombres personalizados y, a continuación, seleccione Crear pila.	
	Note Debe crear la CloudFormation pila de AWS para la función de proxy	

Tarea	Descripción	Habilidades requeridas
	Lambda antes de crear cualquier recurso en las cuentas de destino. Al crear una política de confianza en una cuenta de destino, el rol de IAM pasa del nombre del rol a un identificador interno. Es la razón por la que el rol de IAM debe existir previamente.	
Confirme la creación de la función proxy y la máquina de estado.	1. Espere a que la CloudFormation pila de AWS alcance el estado CREATE_COMPLETE. Este proceso no debería tardar más de un minuto. 2. Abra la consola de AWS Lambda, seleccione Funciones y, a continuación, encuentre la función `lambda-proxy-ProxyLambda-<GUID>` . 3. Abra la consola AWS Step Functions, seleccione máquinas de estado y, a continuación, busque la máquina de estados `sample-crossaccount-codebuild-state-machine` .	AWS DevOps

Cree un rol de IAM en la cuenta de destino y lance un proyecto de muestra CodeBuild

Tarea	Descripción	Habilidades requeridas
Cree e implemente la CloudFormation pila de AWS.	1. Inicie sesión en la consola de administración de AWS de su cuenta de destino, abra la CloudFormation consola de AWS y, a continuación, elija Stacks. 2. Seleccione Crear pila y, a continuación, Con nuevos recursos (estándar). 3. Para Origen de plantilla, elija Cargar un archivo de plantilla. 4. En Cargar un archivo de plantilla, seleccione Elegir archivo y, a continuación, seleccione el archivo `sample_target_codebuild_template.yaml` . Elija Siguiente. 5. En Nombre de pila, especifique un nombre para la pila (por ejemplo:`sample-codebuild-stack`). 6. Reemplace el parámetro `crossAccountSourceRoleArn` con su `<SourceAccountId>` (por ejemplo, `<arn:aws:iam::123456789012:role/codebuild-proxy-lambda-role>`).	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	7. Seleccione Siguiente, acepte las opciones de creación de pilas predeterminadas y, a continuación, seleccione Siguiente. 8. Seleccione la casilla Acepto que AWS CloudFormation podría crear recursos de IAM con nombres personalizados y, a continuación, seleccione Crear pila.	
Verifique la creación del CodeBuild proyecto de muestra.	1. Espere a que la CloudFormation pila de AWS alcance el estado CREATE_COMPLETE. Este proceso no debería tardar más de un minuto. 2. Abra la CodeBuild consola de AWS y busque el `sample-codebuild-project` proyecto.	AWS DevOps

Prueba de la función de proxy de Lambda entre cuentas

Tarea	Descripción	Habilidades requeridas
Lance la máquina de estado.	1. Inicie sesión en la consola de administración de AWS de su cuenta de origen, abra la consola AWS Step Functions y, a continuación, seleccione Máquinas de estado.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	2. Seleccione la máquina de estados `sample-crossaccount-codebuild-state-machine` y, a continuación, Iniciar ejecución. 3. En el editor de entrada, introduzca el siguiente JSON y `<TargetAccountID>` sustitúyalo por el ID de cuenta de AWS de la cuenta que contiene el CodeBuild proyecto. `{ "crossAccountTargetRoleArns": [ { "arn": "arn:aws:iam::<TargetAccountID>:role/proxy-lambda-codebuild-role", "region": "eu-west-1", "codeBuildProject": "sample-codebuild-project", "SampleValue1": "Value1", "SampleValue2": "Value2" } ] }`	

Tarea	Descripción	Habilidades requeridas
	Note Los pares clave-valor se pasan como variables de entorno desde la función de la cuenta de origen al CodeBuild proyecto de la cuenta de destino. 4. Seleccione Iniciar ejecución . 5. En la pestaña Detalles de la página de la máquina de estados, compruebe si el Estado de ejecución está establecido como Correcto. Esto confirma que la máquina de estado se está ejecutando. Nota: La máquina de estados puede tardar unos 30 segundos en alcanzar el estado Correcto. 6. Para ver la salida y la entrada de un paso en la máquina de estados, amplíe ese paso en la sección Historial de eventos de ejecución. Por ejemplo, amplíe el paso Lambda - CodeBuild Proxy — Start. El resultado incluye detalles	

Tarea	Descripción	Habilidades requeridas
	sobre las variables de entorno anuladas, la carga útil original y el identificador del trabajo. CodeBuild	
Valide las variables de entorno.	1. Inicie sesión en la consola de administración de AWS usando su cuenta de AWS . 2. Abra la CodeBuild consola de AWS, expanda Crear y, a continuación, elija Crear proyectos. 3. Seleccione el proyecto `sample-codebuild-project` y, a continuación, Ver detalles. 4. En la pestaña Historial de compilaciones, seleccione la compilación más reciente del proyecto y, a continuación, Ver registros. 5. En la salida del registro, compruebe que las variables de entorno impresas en STDOUT coincidan con las variables de entorno de la máquina de estados de ejemplo de Step Functions.	AWS DevOps

Resolución de problemas

Problema	Solución
La ejecución de Step Functions está tardando más de lo esperado.	Ajuste la `MaxConcurrency` propiedad del mapa en la máquina de estados Step Function para controlar cuántos CodeBuild proyectos se pueden ejecutar en paralelo.
La ejecución de los CodeBuild trabajos está tardando más de lo esperado.	1. Ajuste los valores del tiempo de espera en la máquina de estado de Step Functions para minimizar las solicitudes de sondeo sobre el estado del trabajo. Utilice el tiempo de ejecución previsto para el CodeBuild proyecto. 2. Considere si CodeBuild es la herramienta adecuada a utilizar. Por ejemplo, el tiempo necesario para inicializar un CodeBuild trabajo puede ser considerablemente superior al de AWS Lambda. Si se requiere un alto rendimiento y tiempos de finalización rápidos, considere la posibilidad de migrar la lógica empresarial a AWS Lambda y utilizar una arquitectura de distribución ramificada.

Administración de la conmutación por error de multi-AZ para clústeres de EMR mediante el Controlador de recuperación de aplicaciones

Aarti Rajput, Ashish Bhatt, Neeti Mishra y Nidhi Sharma, Amazon Web Services

Resumen

Este patrón ofrece una estrategia de recuperación ante desastres eficiente para las cargas de trabajo de Amazon EMR a fin de garantizar la alta disponibilidad y la coherencia de datos en varias zonas de disponibilidad dentro de una sola Región de AWS. El diseño utiliza el Controlador de recuperación de aplicaciones de Amazon y un equilibrador de carga de aplicación para administrar las operaciones de conmutación por error y la distribución del tráfico para un clúster EMR basado en Apache Spark.

En condiciones estándar, la zona de disponibilidad principal aloja un clúster y una aplicación de EMR activos con funcionalidad completa read/write . Si se produce un error inesperado en una zona de disponibilidad, el tráfico se redirige automáticamente a la zona de disponibilidad secundaria, donde se inicializa un nuevo clúster de EMR. Ambas zonas de disponibilidad acceden a un bucket de Amazon Simple Storage Service (Amazon S3) compartido a través de puntos de conexión de puerta de enlace dedicados, lo que garantiza una administración de datos coherente. Este enfoque minimiza el tiempo de inactividad y permite una recuperación rápida de las cargas de trabajo críticas de macrodatos durante los errores de la zona de disponibilidad. La solución resulta útil en sectores como el financiero o el minorista, donde los análisis en tiempo real son fundamentales.

Requisitos previos y limitaciones

Requisitos previos

- Una Cuenta de AWS activa.
- Amazon EMR en Amazon Elastic Compute Cloud (Amazon) EC2
- Acceda desde el nodo maestro del clúster de EMR a Amazon S3.
- AWS Infraestructura Multi-AZ

Limitaciones

- Algunas Servicios de AWS no están disponibles en todas Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- Versiones 6.x y posteriores de Amazon EMR

Arquitectura

Pila de tecnología de destino

- Clúster de Amazon EMR
- Controlador de recuperación de aplicaciones de Amazon
- Equilibrador de carga de aplicación
- Bucket de Amazon S3
- Puntos de conexión de puerta de enlace para Amazon S3

Arquitectura de destino

Esta arquitectura proporciona resiliencia a las aplicaciones mediante el uso de varias zonas de disponibilidad y la implementación de un mecanismo de recuperación automatizado a través del Controlador de recuperación de aplicaciones.

1. El equilibrador de carga de aplicación dirige el tráfico al entorno de Amazon EMR activo, que suele ser el clúster de EMR principal de la zona de disponibilidad principal.
2. El clúster de EMR activo procesa las solicitudes de las aplicaciones y se conecta a Amazon S3 a través de su punto de conexión de puerta de enlace de Amazon S3 dedicado para las operaciones de lectura y escritura.
3. Amazon S3 sirve como repositorio de datos central y se puede utilizar como punto de control o como almacenamiento compartido entre clústeres de EMR. Los clústeres de EMR mantienen la coherencia de datos cuando escriben directamente en Amazon S3 mediante el protocolo `s3://` y el sistema de archivos de EMR (EMRFS).
4. El Controlador de recuperación de aplicaciones supervisa continuamente el estado de la zona de disponibilidad principal y, cuando es necesario, administra automáticamente las operaciones de conmutación por error.
5. Si el Controlador de recuperación de aplicaciones detecta un error en el clúster de EMR principal, realiza las siguientes acciones:

- Inicia el proceso de conmutación por error al clúster de EMR secundario en la zona de disponibilidad 2.
- Actualiza las configuraciones de enrutamiento para dirigir el tráfico hacia el clúster secundario.

Tools (Herramientas)

Servicios de AWS

- Amazon Application Recovery Controller le ayuda a gestionar y coordinar la recuperación de sus aplicaciones en todas Regiones de AWS las zonas de disponibilidad. Este servicio simplifica el proceso y mejora la fiabilidad de la recuperación de las aplicaciones al reducir los pasos manuales que necesitan las herramientas y los procesos tradicionales.
- Un equilibrador de carga de aplicación trabaja en la capa de aplicación, es decir, la séptima capa del modelo de interconexión de sistemas abiertos (OSI). Distribuye el tráfico de aplicaciones entrante entre varios destinos, como EC2 instancias, en varias zonas de disponibilidad. Esto aumenta la disponibilidad de la aplicación.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar Servicios de AWS mediante los comandos de su consola de línea de comandos.
- Amazon EMR es una plataforma de macrodatos que proporciona procesamiento de datos, análisis interactivos y machine learning para marcos de código abierto como Apache Spark, Apache Hive y Presto.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- Amazon S3 ofrece una interfaz de servicios web simple que puede utilizar para almacenar y recuperar cualquier cantidad de datos, en cualquier momento y desde cualquier ubicación. Con este servicio, puede crear fácilmente aplicaciones que utilicen el almacenamiento nativo en la nube.
- Los puntos de enlace de Amazon S3 son puertas de enlace que se especifican en la tabla de enrutamiento para acceder a Amazon S3 desde la nube privada virtual (VPC) a través de la red. AWS

Prácticas recomendadas

- Siga las prácticas recomendadas de AWS en materia de seguridad, identidad y conformidad para garantizar una arquitectura sólida y segura.

- Ajuste la infraestructura al Marco de AWS Well-Architected.
- Utilice Concesiones de acceso a Amazon S3 para administrar el acceso desde su clúster de EMR basado en Spark a Amazon S3. Para obtener más información, consulte la entrada en el blog Use Amazon EMR with S3 Access Grants to Scale Spark access to Amazon S3.
- Mejore el rendimiento de Spark con Amazon S3.

Epics

Configure su entorno

Tarea	Descripción	Habilidades requeridas
Inicie sesión en Consola de administración de AWS.	Inicie sesión en la Consola de administración de AWS como usuario de IAM. Para obtener instrucciones, consulte la documentación de AWS.	AWS DevOps
Configure el AWS CLI.	Instálelo AWS CLI o actualíce lo a la última versión para poder interactuar con Servicios de AWS él Consola de administración de AWS. Para obtener instrucciones, consulte la documentación de AWS CLI.	AWS DevOps

Implementación de una aplicación de Spark en su clúster de EMR

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	1. Cree un bucket de S3 para almacenar el conjunto de datos de entrada, los registros, la aplicación y los datos de salida. Para	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	obtener instrucciones, consulte la documentación de Amazon S3. 2. Organice el bucket en carpetas separadas para los datos de entrada (`dataset`), los registros (`logs`), la aplicación de Spark (`spark-app `) y los datos de salida (`output`).	

Tarea	Descripción	Habilidades requeridas

Cree un clúster de EMR.	1. Use los siguientes AWS CLI comandos para crear un clúster de EMR (por ejemplo, versión 6.12 o posterior) con instancias que abarquen dos zonas de disponibilidad (como `us-east-1a` `us-east-1b`) para una alta disponibilidad. El comando específico el tipo de instancia `m4.large` como ejemplo.
	
	`aws emr create-cluster \ --ec2-attributes AvailabilityZone=<AZ-name-1> \ --release-label emr-6.12.0 \ --instance-groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE,InstanceCount=2,InstanceType=m4.large`
	
	`aws emr create-cluster \ --ec2-attributes AvailabilityZone=<AZ-name-2> \ --release-label emr-6.12.0 \ --instance-groups InstanceGroupType=`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	<pre>MASTER,InstanceCou
	nt=1,InstanceType=
	m4.large InstanceG
	roupType=CORE,Inst
	anceCount=2,Instan
	ceType=m4.large</pre>
	Para obtener más información, consulte el comando create-cluster y la documentación de Amazon EMR.
	2. Proporcione el par de claves, el rol de servicio y el perfil de instancia con los permisos necesarios, según sea necesario.	

Tarea	Descripción	Habilidades requeridas
Configure los ajustes de seguridad para el clúster de EMR.	1. Identifique el grupo de seguridad asociado al nodo principal del clúster de EMR mediante el comando AWS CLI describe-cluster: `aws emr describe-cluster --cluster-id j-XXXXXXXX` 2. Para mejorar la seguridad, modifique la configuración del grupo de seguridad para permitir el acceso SSH (puerto TCP 22) al nodo maestro, pero restringiéndolo a la dirección IP específica. Para obtener más información, consulte la documentación de Amazon EMR.	AWS DevOps

Tarea	Descripción	Habilidades requeridas

Conéctese al clúster de EMR.	Conéctese al nodo maestro del clúster de EMR a través de SSH mediante el par de claves proporcionado.
	
	Asegúrese de que el archivo del par de claves se encuentre en el mismo directorio que la aplicación.
	
	Ejecute los siguientes comandos para configurar los permisos correctos para el par de claves y establecer la conexión SSH:
	
	`chmod 400 <key-pair-name>`
	`ssh -i ./<key-pair-name> hadoop@<master-node-public-dns>`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

Implemente la aplicación de Spark.	Tras establecer la conexión SSH, estará en la consola de Hadoop.
	
	1. Cree o edite el archivo de la aplicación de Spark (`main.py`) con un editor de texto como vim:
	
	`vim main.py`
	
	Para obtener más informaci ón sobre cómo crear y modificar la aplicació n de Spark, consulte la documentación de Amazon EMR.
	2. Envíe la aplicación de Spark al clúster de EMR y especifique las ubicaciones de los datos de entrada y salida en el bucket de S3:
	
	`spark-submit main.py –data_source <input-data-folder-in-s3> –output_uri <output-folder-in-s3>`
	
	Este es un ejemplo basado en las carpetas que configuró anteriormente:
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`spark-submit main.py –data_source dataset –output_uri output`
	3. Compruebe los registros de la aplicación para supervisar el progreso de la aplicación:
	`yarn logs -applicationId <application-id>`	

Supervise la aplicación de Spark.	1. Abra otra ventana de terminal y establezca un túnel SSH hacia la interfaz de usuario web del administrador de recursos del clúster de EMR: `ssh -i <key-pair-name> -N -L 8157:<resource-manager-public-dns>:8088 hadoop@<resource-manager-public-dns>` 2. Para supervisar la aplicación, acceda a la interfaz de usuario web del administrador de recursos en `http://localhost:8157` en su navegador web.	AWS DevOps

Cambio del tráfico a otra zona de disponibilidad

Tarea	Descripción	Habilidades requeridas
Cree un Equilibrador de carga de aplicación.	Configure el grupo de destino que enruta el tráfico entre los nodos maestros de Amazon EMR que se implementan en dos zonas de disponibilidad dentro de una Región de AWS. Para obtener instrucciones, consulte Create a target group for your Application Load Balancer en la documentación de Elastic Load Balancing.	AWS DevOps
Configure el cambio de zona en el Controlador de recuperación de aplicaciones.	En este paso, usará la característica de cambio de zona del Controlador de recuperación de aplicaciones para cambiar el tráfico a otra zona de disponibilidad. 1. Abra la consola del Controlador de recuperación de aplicaciones. 2. En Comenzar, seleccione Cambio de zona e Iniciar cambio de zona. 3. Seleccione la zona de disponibilidad de la que desea transferir el tráfico. 4. Seleccione un recurso compatible (por ejemplo, un equilibrador de carga	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	de aplicación) para el cambio de zona en la tabla “Recursos”. 5. En Establecer caducidad de turno zonal, selecciona o introduce una caducidad para el turno zonal. Puede configurar una duración entre un minuto y tres días (72 horas). Todos los cambios de zona son temporales. Debe establecer un vencimien to, pero puede actualizar los cambios activos más adelante para establecer un vencimiento nuevo de hasta tres días. 6. Escriba un comentario sobre este cambio de zona. 7. Seleccione la casilla de verificación para confirmar que comenzar un cambio de zona reducirá la capacidad disponible de su aplicación al cambiar el tráfico de la zona de disponibilidad. 8. Elija Inicio. Para utilizarlos AWS CLI, consulte los ejemplos de uso del AWS CLI cambio zonal en	

Tarea	Descripción	Habilidades requeridas
	la documentación de Application Recovery Controller.	

Tarea	Descripción	Habilidades requeridas

Verifique la configuración y el progreso del cambio de zona.	1. Verifique los recursos que se han registrado con el cambio de zona:
	`aws arc-zonal-shift list-managed-resources --region <AWS-region-name>`
	Por ejemplo, en la siguiente salida se confirma que los recursos están en funcionamiento en ambas zonas de disponibilidad.
	`"appliedWeights": { "use1-az1": 1.0, "use1-az2": 1.0 },`
	2. Para visualizar el cambio zonal, utilice el siguiente AWS CLI comando para iniciar el cambio zonal:
	`aws arc-zonal-shift start-zonal-shift \ --resource-identifier <application-load-balancer-arn> \ --away-from <source-AZ> \ --expires-in 10m --comment "testing" \ --region <AWS-region-name>`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	En este comando, `<source-AZ>` es el identificador de la zona de disponibilidad desde la que desea cambiar el tráfico y `<application-load-balancer-arn>` es el nombre de recurso de Amazon (ARN) del equilibrador de carga de aplicación.
	3. Compruebe que el tráfico se haya cambiado a otra zona de disponibilidad.
	`aws arc-zonal-shift get-managed-resource \ --resource-identifier <application-load-balancer-arn> \ --region <AWS-region-name>`
	Puede ver el cambio de zona que confirman estas ponderaciones:
	`"appliedWeights": { "use1-az1": 0.0, "use1-az2": 1.0 },`	

Recursos relacionados

- AWS CLI comandos:
  - create-cluster
  - describe-cluster
  - arc-zonal-shift
- Configuring Amazon EMR cluster instance types and best practices for Spot instances (documentación de Amazon EMR)
- Prácticas recomendadas de seguridad en IAM (documentación de IAM)
- Utilizar perfiles de instancia (documentación de IAM)
- Use zonal shift and zonal autoshift to recovery applications in ARC (documentación del Controlador de recuperación de aplicaciones)

Gestione blue/green las implementaciones de microservicios en varias cuentas y regiones mediante los servicios de código de AWS y las claves multirregionales de AWS KMS

Balaji Vedagiri, Vanitha Dontireddy, Ashish Kumar, Faisal Shahdad, Vivek Thangamuthu y Anand Krishna Varanasi, Amazon Web Services

Resumen

Este patrón describe cómo implementar una aplicación de microservicios global desde una cuenta central de AWS a varias cuentas de carga de trabajo y regiones de acuerdo con una estrategia de blue/green implementación. El patrón es compatible con lo siguiente:

- El software se desarrolla en una cuenta central, mientras que las cargas de trabajo y las aplicaciones se distribuyen en varias cuentas y regiones de AWS.
- Se utiliza una única clave multirregional del Sistema de administración de claves de AWS (AWS KMS) para el cifrado y el descifrado a fin de permitir la recuperación de desastres.
- La clave KMS es específica de cada región y debe mantenerse o crearse en tres regiones diferentes para los artefactos del proyecto. Una clave KMS multirregional facilita poder conservar el mismo ID de clave en todas las regiones.
- El modelo de ramificación del flujo de trabajo de Git se implementa con dos ramas (de desarrollo y principal) y el código se fusiona mediante solicitudes de extracción (PRs). La función de AWS Lambda que se implementa desde esta pila crea una PR desde la rama de desarrollo hacia la rama principal. La fusión de PR con la rama principal inicia una CodePipeline canalización de AWS, que organiza el flujo de integración y entrega continuas (CI/CD) y despliega las pilas en todas las cuentas.

Este patrón proporciona un ejemplo de configuración de infraestructura como código (IaC) mediante CloudFormation pilas de AWS para demostrar este caso de uso. La blue/green implementación de microservicios se implementa mediante AWS CodeDeploy.

Requisitos previos y limitaciones

Requisitos previos

- Cuatro cuentas de AWS activas:

  - Una cuenta de herramientas para administrar la canalización de código y mantener el CodeCommit repositorio de AWS.
  - Tres cuentas de carga de trabajo (de prueba) para implementar la carga de trabajo de los microservicios.
- Este patrón utiliza las siguientes regiones. Si desea utilizar otras regiones, debe realizar las modificaciones adecuadas en las pilas multirregionales de AWS CodeDeploy y AWS KMS.
  - Cuenta Tools (AWS CodeCommit): `ap-south-1`
  - Cuenta de carga de trabajo (de prueba) 1: `ap-south-1`
  - Cuenta de carga de trabajo (de prueba) 2: `eu-central-1`
  - Cuenta de carga de trabajo (de prueba) 3: `us-east-1`
- Tres buckets de Amazon Simple Storage Service (Amazon S3) para las regiones de implementación de cada cuenta de carga de trabajo. (Se denominan `S3BUCKETNAMETESTACCOUNT1`, `S3BUCKETNAMETESTACCOUNT2` y `S3BUCKETNAMETESTACCOUNT3` más adelante en este patrón).

  A modo de ejemplo, se pueden crear estos buckets en cuentas y regiones específicas con nombres de bucket únicos de la siguiente manera (reemplazar xxxx por un número aleatorio):

```
##In Test Account 1
aws s3 mb s3://ecs-codepipeline-xxxx-ap-south-1 --region ap-south-1
##In Test Account 2
aws s3 mb s3://ecs-codepipeline-xxxx-eu-central-1 --region eu-central-1
##In Test Account 3
aws s3 mb s3://ecs-codepipeline-xxxx-us-east-1 --region us-east-1

#Example
##In Test Account 1
aws s3 mb s3://ecs-codepipeline-18903-ap-south-1 --region ap-south-1
##In Test Account 2
aws s3 mb s3://ecs-codepipeline-18903-eu-central-1 --region eu-central-1
##In Test Account 3
aws s3 mb s3://ecs-codepipeline-18903-us-east-1 --region us-east-1
```

Limitaciones

El patrón utiliza AWS CodeBuild y otros archivos de configuración para implementar un microservicio de muestra. Si tiene un tipo de carga de trabajo diferente (por ejemplo, sin servidor), debe actualizar todas las configuraciones pertinentes.

Arquitectura

Pila de tecnología de destino

- AWS CloudFormation
- AWS CodeCommit
- AWS CodeBuild
- AWS CodeDeploy
- AWS CodePipeline

Arquitectura de destino

Automatización y escala

La configuración se automatiza mediante plantillas de CloudFormation pila de AWS (IaC). Se puede escalar fácilmente para varios entornos y cuentas.

Tools (Herramientas)

Servicios de AWS

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS CodeDeploy automatiza las implementaciones en Amazon Elastic Compute Cloud (Amazon EC2) o en instancias locales, funciones de AWS Lambda o servicios de Amazon Elastic Container Service (Amazon ECS).

- AWS le CodePipeline ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores escalable y rápido que ayuda a ejecutar, detener y administrar contenedores en un clúster.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Herramientas adicionales

- Git es un sistema de control de versiones distribuido y de código abierto que funciona con el CodeCommit repositorio de AWS.
- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización del sistema operativo para entregar software en contenedores. Este patrón utiliza Docker para crear y probar imágenes de contenedores de forma local.
- cfn-lint y cfn-nag son herramientas de código abierto que le ayudan a revisar CloudFormation las pilas para detectar cualquier error o problema de seguridad.

Repositorio de código

El código de este patrón está disponible en el repositorio de despliegues GitHub globales Blue/Green en varias regiones y cuentas.

Epics

Configurar las variables de entorno

Tarea	Descripción	Habilidades requeridas

Exporte las variables de entorno para el despliegue de la CloudFormation pila.	Defina las variables de entorno que se utilizarán como entrada en las CloudForm ation pilas más adelante en este patrón.
	1. Actualice los nombres de los buckets que creó en las tres cuentas y regiones, tal y como se explicó anteriorm ente en la sección Requisito s previos:
	`export S3BUCKETN AMETESTACCOUNT1=<S 3BUCKETACCOUNT1> export S3BUCKETN AMETESTACCOUNT2=<S 3BUCKETACCOUNT2> export S3BUCKETN AMETESTACCOUNT3=<S 3BUCKETACCOUNT3>`
	2. Defina una cadena de asignación al azar para crear buckets de artefactos, ya que los nombres de los buckets deben ser únicos en todo el mundo:
	`export BUCKETSTA RTNAME=ecs-codepip`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`eline-artifacts-19992`
	
	3. Defina y exporte la cuenta IDs y las regiones:
	
	`export TOOLSACCOUNT=<TOOLSACCOUNT>`
	`export CODECOMMITACCOUNT=<CODECOMMITACCOUNT>`
	`export CODECOMMITREGION=ap-south-1`
	`export CODECOMMITREPONAME=Poc`
	`export TESTACCOUNT1=<TESTACCOUNT1>`
	`export TESTACCOUNT2=<TESTACCOUNT2>`
	`export TESTACCOUNT3=<TESTACCOUNT3>`
	`export TESTACCOUNT1REGION=ap-south-1`
	`export TESTACCOUNT2REGION=eu-central-1`
	`export TESTACCOUNT3REGION=us-east-1`
	`export TOOLSACCOUNTREGION=ap-south-1`
	`export ECRREPOSITORYNAME=web`	

Package e implemente las CloudFormation pilas para la infraestructura

Tarea	Descripción	Habilidades requeridas

Clonar el repositorio.	Clone el repositorio de muestras en un nuevo repositorio de su lugar de trabajo:
	`##In work location`
	`git clone https://github.com/aws-samples/ecs-blue-green-global-deployment-with-multiregion-cmk-codepipeline.git`
		AWS DevOps

Empaquete los recursos de Cloudformation.	En este paso, empaqueta los artefactos locales a los que hacen referencia las CloudFormation plantillas para crear los recursos de infraestructura necesarios para servicios como Amazon Virtual Private Cloud (Amazon VPC) y Application Load Balancer.
	Las plantillas están disponibles en la carpeta `Infra` del repositorio de código.
	`##In TestAccount1##`
	`aws cloudformation package \`
	`--template-file mainInfraStack.yaml \`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	--s3-bucket $S3BUCKETNAMETESTACCOUNT1 \ --s3-prefix infraStack \ --region $TESTACCOUNT1REGION \ --output-template-file infrastructure_${TESTACCOUNT1}.template ##In TestAccount2## aws cloudformation package \ --template-file mainInfraStack.yaml \ --s3-bucket $S3BUCKETNAMETESTACCOUNT2 \ --s3-prefix infraStack \ --region $TESTACCOUNT2REGION \ --output-template-file infrastructure_${TESTACCOUNT2}.template ##In TestAccount3## aws cloudformation package \ --template-file mainInfraStack.yaml \ --s3-bucket $S3BUCKETNAMETESTACCOUNT3 \ --s3-prefix infraStack \	

Tarea	Descripción	Habilidades requeridas
	`--region $TESTACCOUNT3REGION \` `--output-template-file infrastructure_${TESTACCOUNT3}.template`	

Valide las plantillas de paquetes.	Valide las plantillas de paquetes:
	`aws cloudformation validate-template \`
	`--template-body file://infrastructure_${TESTACCOUNT1}.template`
	
	`aws cloudformation validate-template \`
	`--template-body file://infrastructure_${TESTACCOUNT2}.template`
	
	`aws cloudformation validate-template \`
	`--template-body file://infrastructure_${TESTACCOUNT3}.template`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

Implemente los archivos del paquete en las cuentas de carga de trabajo,	1. Actualice los valores de los marcadores de posición y los nombres de las cuentas en el script `infraParameters.json` según su configuración.
	2. Implemente las plantillas de paquetes en sus tres cuentas de carga de trabajo.
	
	`##In TestAccount1##`
	`aws cloudformation deploy \`
	`--template-file infrastructure_${TESTACCOUNT1}.template \`
	`--stack-name mainInfrastack \`
	`--parameter-overrides file://infraParameters.json \`
	`--region $TESTACCOUNT1REGION \`
	`--capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM`
	
	`##In TestAccount2##`
	`aws cloudformation deploy \`
	`--template-file infrastructure_${TESTACCOUNT2}.template \`
	`--stack-name mainInfrastack \`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`--parameter-overrides file://infraParameters.json \`
	`--region $TESTACCOUNT2REGION \`
	`--capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM`
	
	`##In TestAccount3##`
	`aws cloudformation deploy \`
	`--template-file infrastructure_${TESTACCOUNT3}.template \`
	`--stack-name mainInfrastack \`
	`--parameter-overrides file://infraParameters.json \`
	`--region $TESTACCOUNT3REGION \`
	`--capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM`	

Insertar una imagen de muestra y escalar Amazon ECS

Tarea	Descripción	Habilidades requeridas
Pase una imagen de muestra a un repositorio de Amazon ECR.	Pase una imagen de muestra (NGINX) al repositorio Amazon Elastic Container Registry (Amazon ECR) denominado `web` (tal y como	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	se establece en los parámetros). Puede personalizar la imagen según sea necesario.
	
	Para iniciar sesión y configurar las credenciales para enviar una imagen a Amazon ECR, siga las instrucciones de la documentación de Amazon ECR.
	
	Los comandos son:
	
	`docker pull nginx`
	`docker images`
	`docker tag <imageid> aws_account_id.dkr.ecr.region.amazonaws.com/<web>:latest`
	`docker push <aws_account_id>.dkr.ecr.<region>.amazonaws.com/<web>:tag`	

Tarea	Descripción	Habilidades requeridas
Escale Amazon ECS y verifique el acceso.	1. Escale Amazon ECS para crear dos réplicas: `aws ecs update-service --cluster QA-Cluster --service Poc-Service --desired-count 2` donde `Poc-Service` se refiere a la aplicación de muestra. 2. Compruebe que se pueda acceder a los servicios desde el equilibrador de carga de aplicación mediante un nombre de dominio completo (FQDN) o un DNS desde un navegador o mediante el comando curl.	AWS DevOps

Configurar los servicios y recursos de código

Tarea	Descripción	Habilidades requeridas
Cree un CodeCommit repositorio en la cuenta de herramientas.	Cree un CodeCommit repositorio en la cuenta de herramientas mediante la `codecommit.yaml` plantilla, que se encuentra en la `code` carpeta del GitHub repositorio. Debe crear este repositorio solo en la única región en	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	la que planea desarrollar el código. `aws cloudformation deploy --stack-name codecommitrepoStack --parameter-overrides CodeCommitReponame=$CODECOMMITREPONAME \ ToolsAccount=$TOOLSACCOUNT --template-file codecommit.yaml --region $TOOLSACCOUNTREGION \ --capabilities CAPABILITY_NAMED_IAM`	

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3 para gestionar los artefactos generados por CodePipeline.	Cree un depósito de S3 para gestionar los artefacto s generados CodePipeline mediante la `pre-reqs-bucket.yaml` plantilla, que se encuentra en la `code` carpeta del GitHub repositorio. Las pilas se deben implement ar en las tres regiones y cuentas de carga de trabajo (prueba) y de herramientas. `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TESTACCOUNT1REGION --capabilities CAPABILITY_NAMED_IAM`  `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketSta`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	rtName=$BUCKETSTAR TNAME \ TestAccount1=$TE STACCOUNT1 TestAccou nt2=$TESTACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts -bucket --parameter- overrides BucketSta rtName=$BUCKETSTAR TNAME \ TestAccount1=$TE STACCOUNT1 TestAccou nt2=$TESTACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT3REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts	

Tarea	Descripción	Habilidades requeridas
	`-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TOOLSACCOUNTREGION --capabilities CAPABILITY_NAMED_IAM`	

Tarea	Descripción	Habilidades requeridas
Configure una clave KMS multirregional.	1. Cree una clave KMS multirregional con las claves principales y de réplica que CodePipeline utilizará. En nuestro ejemplo, `ToolsAccount1region - ap-south-1` será la región principal. `aws cloudformation deploy --stack-name ecs-codepipeline-pre-reqs-KMS \ --template-file pre-reqs_KMS.yaml --parameter-overrides \ TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT --region $TOOLSACCOUNTREGION` 2. Configure las variables CMKARN para transferirlas a los proyectos. CodeBuild Los valores están disponibles en la salida de la pila de plantillas ecs-codepipeline-pre-reqs -KMS (el ID de clave será el mismo en todas las regiones	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	y empezará por). `mrk-` Alternativamente, puede obtener los valores de CMKARN de la cuenta de herramientas. Expórtelos en todas las sesiones de la cuenta:
	
	`export CMKARN1=arn:aws:kms:ap-south-1:<TOOLSACCOUNTID>:key/mrk-xxx`
	`export CMKARN2=arn:aws:kms:eu-central-1:<TOOLSACCOUNTID>:key/mrk-xxx`
	`export CMKARN3=arn:aws:kms:us-east-1:<TOOLSACCOUNTID>:key/mrk-xxx`
	`export CMARNTOOLS=arn:aws:kms:ap-south-1:<TOOLSACCOUNTID>:key/mrk-xxx`	

Tarea	Descripción	Habilidades requeridas

Configure el CodeBuild proyecto en la cuenta de herramientas.	1. Utilice la `codebuild_IAM.yaml` plantilla de la `code` carpeta del GitHub repositorio para configurar AWS Identity and Access Management (IAM) para AWS CodeBuild en una sola región de la cuenta de herramientas:
	`#In ToolsAccount`
	`aws cloudformation deploy --stack-name ecs-codebuild-iam \`
	`--template-file codebuild_IAM.yaml --region $TOOLSACCOUNTREGION \`
	`--capabilities CAPABILITY_NAMED_IAM`
	2. Utilice la `codebuild.yaml` plantilla CodeBuild para configurar su proyecto de compilación. Implemente esta plantilla en las tres regiones de la manera siguiente:
	`aws cloudformation deploy --stack-name ecscodebuildstack --parameter-overrides ToolsAccount=$TOOLSACCOUNT \`
	`CodeCommitRepoName=$CODECOMMITREPONAME`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	ECRRepositoryName= $ECRREPOSITORYNAME APPACCOUNTID=$TEST ACCOUNT1 \ TestAccount3=$TE STACCOUNT3 CodeCommi tRegion=$CODECOMMI TREGION CMKARN=$C MKARN1 \ --template-file codebuild.yaml --region $TESTACCO UNT1REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name ecscodebuildstack -- parameter-overrides ToolsAccount=$TOOL SACCOUNT \ CodeCommitRepoName= $CODECOMMITREPONAME ECRRepositoryName= $ECRREPOSITORYNAME APPACCOUNTID=$TEST ACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tRegion=$CODECOMMI TREGION CMKARN=$C MKARN2 \ --template-file codebuild.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name	

Tarea	Descripción	Habilidades requeridas
	ecscodebuildstack --parameter-overrides ToolsAccount=$TOOLSACCOUNT \ CodeCommitRepoName=$CODECOMMITREPONAME ECRRepositoryName=$ECRREPOSITORYNAME APPACCOUNTID=$TESTACCOUNT3 \ CodeCommitRegion=$CODECOMMITREGION CMKARN=$CMKARN3 \ --template-file codebuild.yaml --region $TESTACCOUNT3REGION --capabilities CAPABILITY_NAMED_IAM	

Tarea	Descripción	Habilidades requeridas

Configúrelo CodeDeploy en cuentas de carga de trabajo.	Utilice la `codedeploy.yaml` plantilla de la `code` carpeta del GitHub repositorio para configurar las tres cuentas CodeDeploy de carga de trabajo. El resultado de `mainInfraStack` incluye los nombres de recursos de Amazon (ARNs) del clúster de Amazon ECS y el listener Application Load Balancer.
	
	Note
	Los valores de las pilas de infraestructura ya se han exportado, por lo que las plantillas de pila los CodeDeplo y importan.
	
	`##WorkloadAccount1##`
	`aws cloudformation deploy --stack-name ecscodedeploystack \`
	`--parameter-overrides ToolsAccount=$TOOLSACCOUNT mainInfrastackname=mainInfrastack \`
	`--template-file codedeploy.yaml --region $TESTACCOUNT1REGION --capabilities CAPABILITY_NAMED_IAM`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	``` ##WorkloadAccount2## aws cloudformation deploy --stack-name ecscodedeploystack \ --parameter-overrides ToolsAccount=$TOOL SACCOUNT mainInfra stackname=mainInfr astack \ --template-file codedeploy.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM ##WorkloadAccount3## aws cloudformation deploy --stack-name ecscodedeploystack \ --parameter-overrides ToolsAccount=$TOOL SACCOUNT mainInfra stackname=mainInfr astack \ --template-file codedeploy.yaml --region $TESTACCO UNT3REGION --capabil ities CAPABILIT Y_NAMED_IAM ```	

Configúrelo CodePipeline en la cuenta de herramientas

Tarea	Descripción	Habilidades requeridas
Cree un proyecto de código en la cuenta de herramientas.	En la cuenta de herramientas, ejecute el comando:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`aws cloudformation deploy --stack-name ecscodepipelinestack --parameter-overrides \ TestAccount1=$TESTACCOUNT1 TestAccount1Region=$TESTACCOUNT1REGION \ TestAccount2=$TESTACCOUNT2 TestAccount2Region=$TESTACCOUNT2REGION \ TestAccount3=$TESTACCOUNT3 TestAccount3Region=$TESTACCOUNT3REGION \ CMKARNTools=$CMKTROOLSARN CMKARN1=$CMKARN1 CMKARN2=$CMKARN2 CMKARN3=$CMKARN3 \ CodeCommitRepoName=$CODECOMMITREPONAME BucketStartName=$BUCKETSTARTNAME \ --template-file codepipeline.yaml --capabilities CAPABILITY_NAMED_IAM`	

Tarea	Descripción	Habilidades requeridas
Proporcione acceso CodePipeline y CodeBuild funciones en la política de claves de AWS KMS y en la política de bucket de S3.	1. Proporcione acceso CodePipeline y CodeBuild funciones en la política clave de AWS KMS: `aws cloudformation deploy --stack-name ecs-codepipeline-pre-reqs-KMS \ --template-file pre-reqs_KMS.yaml --parameter-overrides \ CodeBuildCondition=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT --region $TOOLSACCOUNTREGION` 2. Actualice la política de buckets de S3 para permitir el acceso a los CodeDeplo y roles CodePipeline y las funciones: `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TESTACCOUNT1REGION --capabilities CAPABILITY_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TESTACCOUNT2REGION --capabilities CAPABILITY_NAMED_IAM	

Tarea	Descripción	Habilidades requeridas
	`aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TESTACCOUNT3REGION --capabilities CAPABILITY_NAMED_IAM`  `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \`	

Tarea	Descripción	Habilidades requeridas
	`--template-file pre-reqs_bucket.yaml --region $TOOLSACCOUNTREGION --capabilities CAPABILITY_NAMED_IAM`	

Llamar y probar el proyecto

Tarea	Descripción	Habilidades requeridas
Envía los cambios al CodeCommit repositorio.	1. Clone el CodeCommit repositorio que se creó en el `codecommitrepoStack` mediante el `git clone` comando, tal y como se describe en la CodeCommit documentación de AWS. 2. Actualice los artefactos de entrada con los detalles necesarios: • Archivo JSON: actualice `AccountID` en el archivo en tres lugares de este archivo. Cambie el nombre de los tres archivos para incluir la cuenta IDs. • Archivos YAML: actualiza el ARN y la versión de la definición de la tarea. Cambie el nombre de los tres archivos para incluir la cuenta. IDs	

Tarea	Descripción	Habilidades requeridas

	3. Modifique el archivo `index.html` para realizar algunos cambios menores en la página de inicio.
	4. Copie los siguientes archivos en el repositorio y confirme:
	`index.html`
	`Dockerfile`
	`buildspec.yaml`
	`appspec_<accountid>.yaml (3 files - one per account )`
	`taskdef<accountid>.json (3 files - one per account)`
	5. Inicie o reinicie el proyecto y verifique los resultados.
	6. Acceda al servicio desde el equilibrador de carga de aplicación mediante un FQDN o un DNS y compruebe que se hayan implementado las actualizaciones.	

Limpieza

Tarea	Descripción	Habilidades requeridas
Limpie todos los recursos implementados.	1. Reduzca verticalmente Amazon ECS a cero instancias:	

Tarea	Descripción	Habilidades requeridas

	`aws ecs update-service --cluster QA-Cluster --service Poc-Service --desired-count 0`
	2. Elimine las CloudFormation pilas de cada cuenta y región:
	`##In Tools Account##`
	`aws cloudformation delete-stack --stack-name ecscodepipelinestack --region $TOOLSACCOUNTREGION`
	`aws cloudformation delete-stack --stack-name ecscodebuildstack --region $TESTACCOUNT1REGION`
	`aws cloudformation delete-stack --stack-name ecscodebuildstack --region $TESTACCOUNT2REGION`
	`aws cloudformation delete-stack --stack-name ecscodebuildstack --region $TESTACCOUNT3REGION`
	`aws cloudformation delete-stack --stack-name ecs-codepipeline-pre-reqs-KMS --region $TOOLSACCOUNTREGION`
	`aws cloudformation delete-stack --stack-name codecommi`	

Tarea	Descripción	Habilidades requeridas
	trepoStack --region $TOOLSACCOUNTREGION aws cloudformation delete-stack -- stack-name pre-reqs- artifacts-bucket --region $TESTACCO UNT1REGION aws cloudformation delete-stack -- stack-name pre-reqs- artifacts-bucket --region $TESTACCO UNT2REGION aws cloudformation delete-stack -- stack-name pre-reqs- artifacts-bucket --region $TESTACCO UNT3REGION aws cloudformation delete-stack -- stack-name pre-reqs- artifacts-bucket --region $TOOLSACC OUNTREGION aws cloudformation delete-stack -- stack-name ecs-codeb uild-iam --region $TOOLSACCOUNTREGION ##NOTE: Artifact buckets will not get deleted if there are artifacts so it has to be emptied manually before deleting.##	

Tarea	Descripción	Habilidades requeridas
	``` ##In Workload / Test Accounts## ##Account:1## aws cloudformation delete-stack -- stack-name ecscodede ploystack --region $TESTACCOUNT1REGION aws cloudformation delete-stack -- stack-name mainInfra stack --region $TESTACCOUNT1REGION ##Account:2## aws cloudformation delete-stack -- stack-name ecscodede ploystack --region $TESTACCOUNT2REGION aws cloudformation delete-stack -- stack-name mainInfra stack --region $TESTACCOUNT2REGION ##Account:3## aws cloudformation delete-stack -- stack-name ecscodede ploystack --region $TESTACCOUNT3REGION aws cloudformation delete-stack -- stack-name mainInfra stack --region $TESTACCOUNT3REGION ##NOTE: Amazon ECR (web) will not get deleted if the registry still includes images. It can be manually ```	

Tarea	Descripción	Habilidades requeridas
	`cleaned up if not required.`	

Resolución de problemas

Problema	Solución
Los cambios realizados en el repositorio no se están implementando.	• Comprueba los CodeBuild registros para ver si hay errores en la acción de compilación de Docker. Para obtener más información, consulte la Documentación de CodeBuild . • Compruebe la CodeDeploy implementación para ver si hay algún problema de implement ación de Amazon ECS.

Recursos relacionados

- Insertar una imagen de Docker (documentación de Amazon ECR)
- Conectarse a un CodeCommit repositorio de AWS (CodeCommit documentación de AWS)
- Solución de problemas de AWS CodeBuild (CodeBuild documentación de AWS)

Supervise los repositorios de Amazon ECR en busca de permisos comodín mediante AWS y AWS Config CloudFormation

Vikrant Telkar, Wassim Benhallam y Sajid Momin, Amazon Web Services

Resumen

En la nube de Amazon Web Services (AWS), Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedores administrado que admite repositorios privados con permisos basados en recursos mediante AWS Identity and Access Management (IAM).

IAM admite el comodín "*" en los atributos tanto de recurso como de acción, lo que facilita la selección automática de varios elementos coincidentes. En su entorno de pruebas, puede permitir que todos los usuarios autenticados de AWS accedan a un repositorio de Amazon ECR utilizando el permiso comodín `ecr:*` en un elemento de entidad principal de la declaración de política del repositorio. El permiso comodín `ecr:*` puede resultar útil a la hora de desarrollar y realizar pruebas en cuentas de desarrollo que no pueden acceder a sus datos de producción.

Sin embargo, debe asegurarse de que el permiso comodín `ecr:*` no se utilice en sus entornos de producción, ya que puede provocar graves vulnerabilidades de seguridad. El enfoque de este patrón le ayuda a identificar los repositorios de Amazon ECR que contienen el permiso comodín `ecr:*` en las declaraciones de política de repositorios. El patrón proporciona los pasos y una CloudFormation plantilla de AWS para crear una regla personalizada en AWS Config. A continuación, una función de AWS Lambda supervisa las declaraciones de política del repositorio de Amazon ECR para detectar los permisos comodín `ecr:*`. Si encuentra declaraciones de política de repositorios no conformes, Lambda notifica a AWS Config que envíe un evento a EventBridge Amazon y, a continuación, inicia un tema del EventBridge Amazon Simple Notification Service (Amazon SNS). El tema SNS le notifica por correo electrónico sobre las declaraciones no conformes con la política de repositorios.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada. Para obtener más información, consulte Instalar, actualizar y desinstalar la CLI de AWS en la documentación de la CLI de AWS.
- Un repositorio de Amazon ECR existente con una declaración de política adjunta, instalado y configurado en su entorno de pruebas. Para obtener más información al respecto, consulte

Creación de un repositorio privado y Configuración de una declaración de política de repositorio en la documentación de Amazon ECR.

- AWS Config, configurado en la región de AWS que prefiera. Para obtener más información al respecto, consulte Introducción a AWS Config en la documentación de AWS Config.
- El archivo `aws-config-cloudformation.template` (adjunto), descargado en su equipo local.

Limitaciones

- La solución de este patrón es regional y sus recursos se deben crear en la misma región.

Arquitectura

El siguiente diagrama muestra cómo AWS Config evalúa las declaraciones de política de repositorios de Amazon ECR.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. AWS Config inicia una regla personalizada.
2. La regla personalizada invoca una función de Lambda para evaluar el cumplimiento de las declaraciones de política del repositorio de Amazon ECR. A continuación, la función de Lambda identifica las declaraciones no conformes con la política del repositorio.
3. La función de Lambda envía el estado de no conformidad a AWS Config.
4. AWS Config envía un evento a EventBridge.
5. EventBridge publica las notificaciones de incumplimiento en un tema de SNS.
6. Amazon SNS le envía una alerta por correo electrónico a usted o a un usuario autorizado.

Automatizar y escalar

La solución de este patrón puede supervisar cualquier número de declaraciones de política del repositorio de Amazon ECR, pero todos los recursos que desee evaluar deben ser creados en la misma región.

Tools (Herramientas)

- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Puede administrar y aprovisionar pilas en varias cuentas y regiones de AWS.
- AWS Config: AWS Config proporciona una visión detallada de la configuración de los recursos de AWS de su cuenta de AWS. Esto incluye cómo se relacionan los recursos entre sí y cómo se han configurado en el pasado, para que pueda ver cómo las configuraciones y las relaciones cambian a lo largo del tiempo.
- Amazon ECR: Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado por AWS que es seguro, escalable y fiable. Amazon ECR admite repositorios privados con permisos basados en recursos mediante IAM.

- Amazon EventBridge: Amazon EventBridge es un servicio de bus de eventos sin servidor que puede utilizar para conectar sus aplicaciones con datos de diversas fuentes. EventBridge ofrece un flujo de datos en tiempo real desde sus aplicaciones, aplicaciones de software como servicio (SaaS) y servicios de AWS a objetivos como las funciones de AWS Lambda, los puntos de enlace de invocación HTTP que utilizan destinos de API o los buses de eventos de otras cuentas.
- AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.

Código

El código de este patrón está disponible en el archivo `aws-config-cloudformation.template` (adjunto).

Epics

Cree la CloudFormation pila de AWS

Tarea	Descripción	Habilidades requeridas
Cree la CloudFormation pila de AWS.	Cree una CloudFormation pila de AWS ejecutando el siguiente comando en la CLI de AWS: `$ aws cloudformation create-stack --stack-name=AWSConfigECR \ --template-body file://aws-config-cloudformation.template \ --parameters ParameterKey=<email>,ParameterValue=<myemail@example.com> \ --capabilities CAPABILITY_NAMED_IAM`	AWS DevOps

Probar la regla personalizada de AWS Config

Tarea	Descripción	Habilidades requeridas
Pruebe la regla personalizada de AWS Config.	1. Inicie sesión en la consola de administración de AWS, abra la consola de AWS Config y, a continuación, seleccione Recursos. 2. En la página de Inventario de recursos, puede filtrar por categoría de recurso,	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	tipo de recurso y estado de conformidad. 3. Un repositorio de Amazon ECR que contiene `ecr:*` es `NON-COMPLIANT?` y un repositorio de Amazon ECR que no contiene `ecr:*` es `COMPLIANT` . 4. La dirección de correo electrónico suscrita al tema de SNS recibe notificac iones si un repositorio de Amazon ECR contiene declaraciones de políticas no conformes.	

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Optimice las implementaciones sin servidor con varias cuentas mediante los flujos de trabajo y Actions AWS CDK GitHub

Sarat Chandra Pothula y VAMSI KRISHNA SUNKAVALLI, Amazon Web Services

Resumen

Las organizaciones que implementan una infraestructura sin servidor en múltiples entornos Cuentas de AWS y suelen enfrentarse a desafíos como la duplicación de código, los procesos manuales y las prácticas incoherentes. La solución de este patrón muestra cómo utilizar los flujos de trabajo reutilizables de AWS Cloud Development Kit (AWS CDK) In Go y GitHub Actions para agilizar la administración de la infraestructura sin servidor con varias cuentas. Esta solución demuestra cómo se pueden definir los recursos de la nube como código, implementar procesos estandarizados de integration/continuous despliegue continuo (CI/CD) y crear componentes modulares y reutilizables.

Con estas herramientas, las organizaciones pueden administrar de manera eficiente los recursos entre cuentas, implementar procesos de implementación coherentes y simplificar arquitecturas complejas sin servidor. El enfoque también mejora la seguridad y el cumplimiento al aplicar prácticas estandarizadas para su uso y, en última instancia Cuentas de AWS, mejorar la productividad y reducir los errores en el desarrollo e implementación de aplicaciones sin servidor.

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- AWS Identity and Access Management Existen funciones y permisos (IAM) para el proceso de implementación. Esto incluye permisos para acceder a los repositorios de Amazon Elastic Container Registry (Amazon ECR), AWS Lambda crear funciones y cualquier otro recurso necesario en el destino. Cuentas de AWS
- AWS Command Line Interface (AWS CLI) versión 2.9.11 o posterior, instalada y configurada.
- AWS Cloud Development Kit (AWS CDK) versión 2.114.1 o posterior, instalada y arrancada.
- Versión 1.22 o posterior de Go, instalada.
- La versión 24.0.6 o posterior de Docker instalada

Limitaciones

- Compatibilidad de lenguajes: Go es un lenguaje popular para aplicaciones sin servidor. Sin embargo, además de Go, AWS CDK es compatible con otros lenguajes de programación, incluidos C#, Java, Python y TypeScript. Si su organización ya tiene bases de código o conocimiento experto en otros lenguajes, es posible que tenga que adaptarlas o aprender Go para utilizar plenamente la solución descrita en el patrón.
- Curva de aprendizaje: la AWS CDK adopción de los flujos de trabajo GitHub reutilizables y Go Go (si son nuevos en la organización) puede implicar una curva de aprendizaje para los desarrolladores y los DevOps equipos. Es posible que se necesiten formación y documentación para garantizar una adopción fluida y un uso efectivo de estas tecnologías.

Arquitectura

En el siguiente diagrama se muestran los componentes de la arquitectura y el flujo de trabajo de esta aplicación.

Esta solución realiza los pasos que se indican a continuación:

1. El desarrollador clona el repositorio, crea una nueva rama y realiza cambios en el código de la aplicación en su entorno local.
2. El desarrollador confirma estos cambios e introduce la nueva rama en el repositorio. GitHub
3. El desarrollador crea una solicitud de incorporación de cambios en el GitHub repositorio y propone fusionar su rama de funcionalidad o nueva funcionalidad con la rama principal.
4. Esta solicitud de incorporación activa el flujo de trabajo de GitHub las acciones de integración continua (CI). Los flujos de trabajo de CI y de implementación continua (CD) de este patrón utilizan flujos de trabajo reutilizables, que son plantillas modulares predefinidas que se pueden compartir y ejecutar en diferentes proyectos o repositorios. Los flujos de trabajo reutilizables promueven la estandarización y la eficiencia de los CI/CD procesos.
5. El flujo de trabajo de CI configura el entorno necesario, genera una etiqueta de Docker para la imagen y crea la imagen de Docker utilizando el código de la aplicación.
6. El flujo de trabajo de CI se autentica AWS mediante la función central de Cuenta de AWS GitHub OIDC. Para los flujos de trabajo de CI, la función central de Cuenta de AWS GitHub OIDC utiliza AWS Security Token Service (AWS STS) para obtener credenciales temporales. Estas credenciales permiten al rol crear y enviar imágenes de Docker al repositorio Amazon ECR de la central. Cuenta de AWS
7. El flujo de trabajo de CI envía la imagen de Docker creada a Amazon ECR.

8. El flujo de trabajo de CI almacena la etiqueta de imagen en el Almacén de parámetros de Systems Manager.
9. Cuando el flujo de trabajo de CI se complete correctamente, se mostrará la etiqueta de imagen de Docker.
10. Al activar el flujo de trabajo de CD, el desarrollador introduce manualmente la etiqueta de imagen de la imagen de Docker que quiere implementar. Esta etiqueta de imagen corresponde a la etiqueta que se generó y se envió a Amazon ECR durante el flujo de trabajo de CI.
11. El desarrollador activa manualmente el flujo de trabajo de CD, que utiliza el flujo de trabajo reutilizable de CD.
12. El flujo de trabajo de CD se autentica mediante el AWS uso de la función central de OIDC Cuenta de AWS GitHub . En el caso del flujo de trabajo del CD, AWS STS se utiliza primero para asumir la función central Cuenta de AWS GitHub de OIDC. Luego, este rol asume los roles de arranque de CDK para las implementaciones de las cuentas de destino.
13. El flujo de trabajo del CD lo utiliza AWS CDK para sintetizar plantillas AWS CloudFormation .
14. El flujo de trabajo de CD despliega la aplicación en el destino Cuenta de AWS mediante CDK deploy, mediante la etiqueta de imagen especificada manualmente para la función Lambda.

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir y aprovisionar la Nube de AWS infraestructura en código.
- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todo el Cuentas de AWS mundo Regiones de AWS. CloudFormation es una parte integral del proceso de AWS CDK implementación. El CDK sintetiza CloudFormation las plantillas y, CloudFormation a continuación, las utiliza para crear o actualizar los recursos del AWS entorno.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la

capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

- AWS Systems Manager Parameter Store proporciona un almacenamiento jerárquico y seguro para la gestión de los datos de configuración y la gestión de secretos.

Otras herramientas

- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización a nivel del sistema operativo para entregar software en contenedores.
- GitHub Actions es una plataforma de integración y entrega continuas (CI/CD) que está estrechamente integrada con los repositorios. GitHub Puedes usar GitHub Actions para automatizar tu proceso de creación, prueba e implementación.
- Go es un lenguaje de programación de código abierto compatible con Google.

Repositorio de código

El código de este patrón está disponible en el cicd-github-actions repositorio GitHub aws-cdk-golang-serverless-.

Prácticas recomendadas

- Diseño modular: organice su AWS CDK código en conjuntos o pilas modulares y reutilizables, lo que promoverá la reutilización y el mantenimiento del código en múltiples cuentas y proyectos.
- Separación de preocupaciones: separe el código de la infraestructura del código de la aplicación, lo que permitirá la implementación y la administración independientes de cada componente.
- Control de versiones e inmutabilidad: trate su infraestructura como código (IaC) y utilice Git para el control de versiones. Adopte principios de infraestructura inmutables creando nuevos recursos en lugar de modificar los existentes.
- Pruebas y validación: implemente estrategias de prueba integrales, que incluyan pruebas unitarias, pruebas de integración y end-to-end pruebas, para garantizar la exactitud y confiabilidad del código y las implementaciones. AWS CDK
- Seguridad y cumplimiento: siga las mejores prácticas AWS de seguridad, como el acceso con privilegios mínimos, la comunicación segura y el cifrado de datos. Implemente comprobaciones de cumplimiento y mecanismos de auditoría para garantizar el cumplimiento de las políticas y los requisitos normativos de la organización. Implemente las prácticas recomendadas de seguridad

para las imágenes de contenedores, como hacer exámenes en busca de vulnerabilidades, imponer la firma de imágenes y cumplir con los requisitos de cumplimiento de la organización.

- Supervisión y registro: configure mecanismos de supervisión y registro para realizar un seguimiento del estado y el rendimiento de las aplicaciones y la infraestructura sin servidor. Servicios de AWS Úselo como Amazon CloudWatch AWS CloudTrail y con AWS X-Ray fines de monitoreo y auditoría.
- Automatización y CI/CD: utilice flujos de trabajo GitHub reutilizables y otras CI/CD herramientas para automatizar los procesos de creación, prueba e implementación, lo que puede ayudar a respaldar despliegues consistentes y repetibles en varias cuentas.
- Administración del entorno: mantenga entornos separados (por ejemplo, desarrollo, pruebas y producción). Implemente estrategias para promover cambios entre entornos, garantizando las pruebas y la validación adecuadas antes de las implementaciones de producción.
- Documentación y colaboración: documente el código de la infraestructura, los procesos de implementación y las prácticas recomendadas para facilitar el intercambio de conocimientos y la colaboración dentro de su equipo.
- Optimización de costos: implemente estrategias de monitoreo y optimización de costos, como ajustar el tamaño de los recursos, usar el autoescalado y aprovechar los servicios de optimización de AWS costos como y. AWS Budgets AWS Cost Explorer
- Recuperación ante desastres y copia de seguridad: planifique escenarios de recuperación ante desastres mediante la implementación de mecanismos de copia de seguridad y restauración para sus aplicaciones sin servidor y sus recursos de infraestructura.
- Mejora continua: revise y actualice periódicamente sus prácticas, herramientas y procesos para adaptarlos a las prácticas recomendadas, las recomendaciones de seguridad y los avances tecnológicos más recientes del ecosistema sin servidor.
- Mejore el nivel de seguridad: AWS PrivateLinkutilícelo para mejorar el nivel de seguridad de su nube privada virtual (VPC) mediante la configuración de los puntos de enlace de la interfaz de la VPC para Amazon ECR y Parameter Store. AWS Lambda AWS Systems Manager

Epics

Configuración de los entornos

Tarea	Descripción	Habilidades requeridas
Cree un repositorio de Amazon ECR en la central Cuenta de AWS.	Para compartir imágenes de contenedores entre varias Cuentas de AWS, debe configurar el acceso multicuenta para Amazon ECR. En primer lugar, cree un repositorio de Amazon ECR en la central Cuenta de AWS. Para crearlo, ejecute este comando: `aws ecr create-repository --repository-name sample-repo` En una tarea posterior, conceda acceso a las demás tareas Cuentas de AWS que necesiten utilizar la imagen del contenedor.	AWS DevOps
Agregue permisos entre cuentas al repositorio de Amazon ECR.	Para añadir permisos entre cuentas al repositorio de Amazon ECR en la central Cuenta de AWS, ejecute el siguiente código: `{ "Version": "2008-10-17", "Statement": [ {`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	"Sid": "LambdaECRImageRetrievalPolicy",
	"Effect": "Allow",
	"Principal": {
	"Service": "lambda.amazonaws.com"
	},
	"Action": [
	"ecr:BatchGetImage",
	"ecr:GetDownloadUrlForLayer",
	],
	"Condition": {
	"StringLike": {
	"aws:sourceArn": "arn:aws:lambda:<Target_Region>:<Target_Account_ID>:function:*"
	}
	}
	},
	{
	"Sid": "new statement",
	"Effect": "Allow",
	"Principal": {
	"AWS": "arn:aws:iam::<Target_Account_ID>:root"
	},
	"Action": [
	"ecr:BatchGetImage",
	"ecr:GetDownloadUrlForLayer",
	],
	}
	]	

Tarea	Descripción	Habilidades requeridas
	`}`	
Configure un rol para el rol GitHub de OIDC en la central. Cuenta de AWS	1. Configure AWS el OIDC GitHub de confianza como una identidad federada, lo que incluye añadir el proveedor del GitHub OIDC AWS y configurar el rol y la política de confianza en IAM. Para ello, siga las instrucciones de la documentación sobre cómo configurar OpenID Connect en Amazon Web Services. GitHub 2. Una vez creado el rol, agregue los permisos necesarios al rol. Por ejemplo, añada permisos para Amazon ECR y AWS Systems Manager Parameter Store. Para obtener más información, consulte Configuración de un rol para el proveedor de identidad del GitHub OIDC en la documentación de IAM.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Inicie el AWS entorno en el objetivo Cuentas de AWS.	Configure un entorno de CDK en una red específica Cuenta de AWS Región de AWS que permita los despliegues entre cuentas desde una cuenta central y aplique los principios de privilegios mínimos a la función de ejecución. CloudFormation Para arrancar un entorno, ejecute el siguiente comando AWS : `cdk bootstrap aws://<Target_Account_ID>/<Target_Region> --trust <Central_Account_ID> --cloudformation-execution-policies arn:aws:iam::aws:policy/<Least_Privilege_Policy>`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Conceda acceso al rol central de Cuenta de AWS OIDC a los roles de Cuenta de AWS bootstrap de destino.	El bootstrap del CDK crea las siguientes funciones de IAM, diseñadas para que las asuma la central Cuenta de AWS durante las distintas etapas del proceso de despliegue del CDK: • Rol de publicación de archivos • Rol de publicación de imágenes • Rol de búsqueda • Rol de implementación Cada rol tiene permisos específicos adaptados a su finalidad, siguiendo el principio de privilegio mínimo. El nombre «`Target_Account_ID yTarget_Region` » de cada función ayuda a indicar que estas funciones son únicas en las distintas regiones. Cuentas de AWS Este enfoque permite una identificación y una administración claras en configuraciones de varias cuentas y varias regiones. `Target Account CDK Bootstrap Roles`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	arn:aws:iam::<Target_Account_ID>:role/cdk-deploy-role-<Target_Account_ID>-<Target_Region> arn:aws:iam::<Target_Account_ID>:role/cdk-file-publishing-role-<Target_Account_ID>-<Target_Region> arn:aws:iam::<Target_Account_ID>:role/cdk-image-publishing-role-<Target_Account_ID>-<Target_Region> arn:aws:iam::<Target_Account_ID>:role/cdk-lookup-role-<Target_Account_ID>-<Target_Region> • Actualice la política de permisos del rol de OIDC en la cuenta central para que pueda asumir roles en la cuenta de destino. Esta configuración permite implementar pilas de CDK en diferentes Cuentas de AWS. Al permitir que el rol de OIDC de la cuenta central adopte los permisos necesarios de la cuenta de destino, se crea un puente seguro para las implementaciones de CDK entre cuentas. Este enfoque mantiene un control de	

Tarea	Descripción	Habilidades requeridas
	acceso adecuado y, al mismo tiempo, facilita una administración fluida de la infraestructura de varias cuentas. Para actualizar la política de permisos del rol de OIDC en la central Cuenta de AWS, usa el siguiente código: `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": ["arn:aws:iam::<Target_Account_ID>:role/cdk-deploy-role-<Target_Account_ID>-<Target_Region>", "arn:aws:iam::<Target_Account_ID>:role/cdk-file-publishing-role-<Target_Account_ID>-<Target_Region>", "arn:aws:iam::<Target_Account_ID>:role/cdk-image-publishing-`	

Tarea	Descripción	Habilidades requeridas

	<pre>role-<Target_Account_ID>-<Target_Region>",
	
	"arn:aws:iam::<Target_Account_ID>:role/cdk-lookup-role-<Target_Account_ID>-<Target_Region>"
	]
	}
	]
	}</pre>	

Compilación de la imagen de Docker

Tarea	Descripción	Habilidades requeridas
Clone el repositorio del proyecto.	Para clonar el GitHub repositorio de este patrón, ejecute el siguiente comando: <pre>git clone https://github.com/aws-samples/aws-cdk-golang-serverless-cicd-github-actions.git</pre>	AWS DevOps
Vaya a la ruta de Dockerfile.	Para ir a la ruta de Dockerfile, ejecute el siguiente comando: <pre>cd lambda</pre>	AWS DevOps
Autentique Docker con Amazon ECR.	Amazon ECR requiere un acceso seguro a sus repositorios de contenedores privados. Al iniciar sesión de esta	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	manera, permite que Docker interactúe de forma segura con Amazon ECR en su máquina o CI/CD entorno local. Para autenticar Docker con Amazon ECR, ejecute el siguiente comando: `aws ecr get-login -password --region <AWS_REGION> | docker login --username AWS --password-stdin <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com` Revise los marcadores de posición `AWS_REGION` y `AWS_Account_ID` con su información.	
Cree la imagen de Docker.	Para compilar la imagen de Docker, ejecute el siguiente comando: `docker build --platform linux/arm64 -t sample-app .`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

Etiquete y envíe la imagen de Docker.	Para etiquetar y enviar la imagen de Docker en el repositorio de Amazon ECR, ejecute los siguientes comandos:
	`docker tag sample-ap p:latest <AWS_ACCO UNT_ID>.dkr.ecr.<A WS_REGION>.amazona ws.com/<ECR_REPOSI TORY>:<DOCKER_TAG>`
	`docker push <AWS_ACCO UNT_ID>.dkr.ecr.<A WS_REGION>.amazona ws.com/<ECR_REPOSI TORY>:<DOCKER_TAG>`
	Revise los marcadores de posición `AWS_Account_ID` , `AWS_REGION` , `ECR_REPOS ITORY` y `DOCKER_TAG` con su información.
		AWS DevOps

Implemente la AWS CDK aplicación

Tarea	Descripción	Habilidades requeridas
Sintetice la pila de CDK con variables específicas del entorno.	Para generar la CloudForm ation plantilla para su infraestr uctura tal como se define en el código CDK, ejecute el siguiente comando:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`ENV=<environment> IMAGETAG=<image_tag> ECR_ARN=<ecr_repo_arn> cdk synth` Revise los siguientes marcadores de posición con su información: • `environment` : se sustituye por un nombre de entorno específico, como `dev`. `staging` o `prod`. • `image_tag` : sustitúyalo por una etiqueta específica para una imagen de Docker, como `v1.0.0` o `latest`. • `ecr_repo_arn` : sustitúya lo por el nombre de recurso de Amazon (ARN) de un repositorio de Amazon ECR.	

Tarea	Descripción	Habilidades requeridas
Implemente la pila de CDK.	Para implementar la pila de CDK en su servidor Cuenta de AWS, ejecute el siguiente comando. El indicador `--require-approval never` significa que el CDK aprobará y ejecutará todos los cambios automáticamente. Esto incluye los cambios que CDK normalmente considera ría que necesitan una revisión manual (como los cambios en la política de IAM o la eliminación de recursos). Asegúrese de que el código y la CI/CD canalización de su CDK estén bien probados y sean seguros antes de usar la `--require-approval never` bandera en entornos de producción. `ENV=<environment> IMAGETAG=<image_tag> ECR_ARN=<ecr_repo_arn> cdk deploy --require-approval never`	AWS DevOps

Automatice CI/CD el uso de GitHub flujos de trabajo

Tarea	Descripción	Habilidades requeridas
Cree una rama de caracterí sticas y agregue los cambios.	Utilice el repositorio clonado que creó anteriormente, cree	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	una rama de características y, a continuación, agregue los cambios al código de la aplicación. Utilice los siguiente s comandos:
	
	`git checkout -b <feature_branch>`
	`git add .`
	`git commit -m "add your changes"`
	`git push origin <feature_branch>`
	
	A continuación, se muestran algunos ejemplos de cambios:
	
	• Cambios en la lógica de la función de Lambda
	• Adición de nuevas caracterí sticas o funcionalidades al código de Lambda
	• Corrección de errores u optimización del código existente en la función de Lambda
	
	GitHub Las acciones utilizará n los flujos de trabajo reutiliza bles y activarán las CI/CD canalizaciones.	

Combine los cambios.	Cree una solicitud de extracció n y fusione los cambios con la rama principal.	AWS DevOps

Resolución de problemas

Problema	Solución
`AccessDenied` errores al implement ar recursos en Cuentas de AWS, por ejemplo,`AccessDenied: User not authorized to perform: "sts:Assu meRole"` .	Para ayudar a resolver este problema, siga estos pasos para verificar los permisos entre cuentas: • Asegúrese de que existan los roles y políticas de IAM necesarios para las implementaciones entre cuentas. • Compruebe que los permisos `assume` de los roles estén configurados correctamente.
Problemas de compatibilidad debido a discordancias entre versiones; por ejemplo, un error `undefined: awscdkStack` con una versión de CDK desactualizada.	Para ayudar a resolver este problema, haga lo siguiente para comprobar que está utilizando las versiones necesarias de AWS CDK and Go: • Asegúrate de usar versiones compatibles del AWS CDK and Go. • Compruebe si hay problemas conocidos o cambios importantes en las versiones recientes.
Errores en las canalizaciones de CI/CD; por ejemplo, `Error: No such file or directory` debido a una configuración incorrecta de YAML o `Permission denied` para ramas protegidas.	Para ayudar a resolver los problemas relaciona dos con la configuración de GitHub Actions, comprueba que los flujos de trabajo reutiliza bles estén correctamente referenciados y configurados.

Recursos relacionados

Recursos de AWS

- AWS Prácticas recomendadas para seguridad, identidad y conformidad
- AWS CDK Taller
- AWS Biblioteca de kits de Cloud Development

- Creación de una función de Lambda con una imagen de contenedor
- Identity and Access Management para Amazon Elastic Container Registry
- Working with the AWS CDK in Go

Otros recursos

- Configuración de OpenID Connect en Amazon Web Services (documentación) GitHub
- Documentación de Golang
- Guía de inicio rápido para GitHub realizar acciones (documentación) GitHub
- Reutilización de flujos de trabajo (documentación) GitHub

AWS Service Catalog Aprovisione productos en función de AWS CloudFormation plantillas mediante GitHub acciones

Ashish Bhatt y Ruchika Modi, Amazon Web Services

Resumen

Este patrón proporciona a las organizaciones un enfoque simplificado que utiliza AWS Service Catalogproductos y carteras para aprovisionar de forma estandarizada y compatible con Servicios de AWS todos los equipos. AWS CloudFormationayuda a combinar los componentes esenciales de los productos y carteras de Service Catalog para aprovisionar la infraestructura de red base. Nube de AWSEste patrón también promueve DevOps prácticas al integrar la infraestructura como código (IaC) en los flujos de trabajo de desarrollo automatizados mediante Actions. GitHub

AWS Service Catalog permite a las organizaciones crear y gestionar servicios de TI aprobados AWS, lo que ofrece ventajas como la estandarización, el control centralizado, el aprovisionamiento de autoservicio y la gestión de costes. Al automatizar la implementación de las carteras y productos de Service Catalog mediante GitHub Actions, las empresas pueden hacer lo siguiente:

- Lograr implementaciones consistentes y repetibles.
- Usar el control de versiones para la IaC.
- Integrar la administración de recursos en la nube con los flujos de trabajo de desarrollo existentes.

Esta combinación optimiza las operaciones en la nube, refuerza la conformidad y acelera la prestación de los servicios aprobados a la par que reduce los errores manuales y mejora la eficiencia general.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Acceso al GitHub repositorio
- Comprensión básica de AWS CloudFormation y AWS Service Catalog
- Un depósito de Amazon Simple Storage Service (Amazon S3) para alojar plantillas CloudFormation

- Un nombre de rol AWS Identity and Access Management (IAM) `github-actions` que se utiliza para la conectividad entre y GitHub AWS

Limitaciones

- El código reutilizable de este patrón solo se ha probado con GitHub Actions.
- Algunos Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

La solución de este patrón se creó mediante las siguientes acciones de GitHub Marketplace y sus versiones respectivas:

- `actions/checkout@v4`
- `aws-actions/configure-aws-credentials@v2`
- `aws-actions/aws-cloudformation-github-deploy@v1.2.0`

Arquitectura

En el siguiente diagrama se muestra la arquitectura para esta solución.

1. Los administradores o los ingenieros de plataformas CloudFormation envían las plantillas estandarizadas a un GitHub repositorio, donde se guardan. El GitHub repositorio también contiene flujos de trabajo que automatizan el aprovisionamiento o el AWS Service Catalog uso GitHub de Actions.
2. GitHub Las acciones activan un flujo de trabajo que se conecta al Nube de AWS uso de un proveedor de OpenID Connect (OIDC) para aprovisionar Service Catalog.
3. Service Catalog contiene la cartera y los productos que los desarrolladores pueden utilizar directamente para aprovisionar AWS recursos estandarizados. Este patrón agrupa AWS recursos como nubes privadas virtuales (VPCs), subredes, pasarelas de Internet y NAT y tablas de enrutamiento.

4. Una vez que el desarrollador crea un producto de Service Catalog, Service Catalog lo convierte en AWS recursos estandarizados y preconfigurados. Como resultado, los desarrolladores ahorran tiempo porque no tienen que aprovisionar recursos individuales ni configurarlos manualmente.

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todo el mundo Cuentas de AWS . Regiones de AWS Se trata de un servicio de infraestructura como código (IaC) que se puede utilizar fácilmente como uno de los tipos de productos con AWS Service Catalog los que cuenta.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Service Catalogle ayuda a gestionar de forma centralizada el catálogo de servicios de TI aprobados. AWS Los usuarios finales pueden implementar rápidamente solo los servicios de TI aprobados que necesitan, de acuerdo con las limitaciones establecidas por su organización.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otros

- GitHub Actions es una plataforma de integración y entrega continuas (CI/CD) que está estrechamente integrada con GitHub los repositorios. Puedes usar GitHub Actions para automatizar tu proceso de creación, prueba e implementación.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub service-catalog-with-github-actions. El repositorio contiene los siguientes archivos de interés:

- `github/workflows`:
  - `e2e-test.yaml`: este archivo llama a `workflow.yaml`, que es el flujo de trabajo reutilizable. Este flujo de trabajo se activa en cuanto hay una confirmación y una inserción en una rama.

  - `workflow.yaml`: este archivo contiene el flujo de trabajo reutilizable de esta solución; está configurado con `workflow_call` como desencadenador. Al tratarse de un flujo de trabajo reutilizable, `workflow.yaml` se puede invocar desde cualquier otro flujo de trabajo.
- `templates`:
  - `servicecatalog-portfolio.yaml`— Esta CloudFormation plantilla incluye recursos que aprovisionan la cartera de Service Catalog y el producto Service Catalog. La plantilla contiene un conjunto de parámetros que se utilizan al aprovisionar la cartera y los productos de Service Catalog. Un parámetro acepta la URL de un archivo de Amazon S3 en la que se carga la plantilla `vpc.yaml`. Si bien este patrón incluye el `vpc.yaml` archivo para aprovisionar AWS los recursos, también puede utilizar la URL del archivo S3 del parámetro para la configuración.
  - `vpc.yaml`— Esta CloudFormation plantilla contiene AWS los recursos que se van a añadir al producto Service Catalog. AWS los recursos incluyen subredes VPCs, puertas de enlace de Internet, puertas de enlace NAT y tablas de enrutamiento. La `vpc.yaml` plantilla es un ejemplo de cómo puede utilizar cualquier CloudFormation plantilla con una plantilla de productos y portafolios de Service Catalog.

Prácticas recomendadas

- Consulte las prácticas recomendadas de seguridad AWS Service Catalog en la AWS Service Catalog documentación.
- Consulte Refuerzo de la seguridad para GitHub las acciones en la GitHub documentación.

Epics

Configuración de la estación de trabajo local

Tarea	Descripción	Habilidades requeridas
Configure Git en su estación de trabajo.	Para instalar y configurar Git en su estación de trabajo local, siga las instrucciones de Getting Started – Installing Git en la documentación de Git.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Clona el repositorio GitHub del proyecto.	Para clonar el repositorio GitHub del proyecto, haga lo siguiente: 1. Abre el GitHub repositorio de este patrón 2. Elija Código para ver las opciones de clonación y copie la URL proporcionada en la pestaña HTTPS. 3. Cree una carpeta para el proyecto en su estación de trabajo. 4. Abra una terminal y vaya a esta carpeta. 5. Para clonar el GitHub repositorio, ejecuta el siguiente comando con la URL que copiaste en el paso 2: `git clone https://github.com/aws-samples/service-catalog-with-github-actions.git` 6. Cuando se complete la clonación, use el siguiente comando para cambiar al repositorio clonado de la carpeta de su proyecto:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`cd <folder-name>/service-catalog-with-github-actions` 7. Abra el proyecto en un entorno de desarrollo integrado (IDE) de su elección.	

Configuración del proveedor de OIDC

Tarea	Descripción	Habilidades requeridas
Configure un proveedor de OIDC.	Cree un proveedor de OpenID Connect (OIDC) que permita a los flujos de trabajo de GitHub Actions acceder a los recursos sin necesidad de almacenar las AWS credencia les como secretos de larga duración. AWS GitHub Para obtener instrucciones, consulte Configuración de OpenID Connect en Amazon Web Services en la GitHub documentación. Una vez configurado un proveedor de OIDC, se actualizará la política de confianza del rol de IAM `github-actions` , mencionada anteriormente en Requisitos previos.	Administrador de AWS DevOps, AWS general

Proceso de activación de GitHub Actions para implementar la cartera y los productos de Service Catalog

Tarea	Descripción	Habilidades requeridas

Actualizar `e2e-test.yaml` .	El archivo `e2e-test.yaml` desencadena el flujo de trabajo reutilizable en `workflow.yaml` . Actualice y valide los valores de los siguientes parámetros de entrada en `e2e-test.yaml` :
	• `aws_account_id` — Especifique la correcta Cuenta de AWS.
	• `aws_region` — Especifiq ue la correcta Región de AWS.
	• `s3BucketName` — Especifique el bucket de Amazon S3 en el que se guardarán las CloudForm ation plantillas.
	• El archivo del flujo de trabajo requiere dos roles de IAM como entrada:
	  • `LaunchConstraintRo le` - La función de IAM que AWS Service Catalog asume cuando un usuario final lanza, actualiza o cancela un producto.
	  • `PrincipalArn` : el nombre de recurso de
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Amazon (ARN) de la entidad principal (usuario, rol o grupo de IAM) que se asociará a la cartera de Service Catalog. Si el `PrincipalType` es `IAM`, el valor admitido es un nombre de recurso de Amazon (ARN) de IAM completamente definido. Si el `PrincipalType` es `IAM_PATTERN`, el valor admitido es un ARN de IAM sin un `AccountID` en el siguiente formato: `arn:partition:iam::resource-type/resource-id`	

Validación de la implementación

Tarea	Descripción	Habilidades requeridas
Valide los recursos de Service Catalog.	Para validar los recursos de Service Catalog, haga lo siguiente: 1. Inicie sesión en Consola de administración de AWS el Cuenta de AWS y compruebe que Región de AWS es correcto.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	2. Vaya a AWS Service Catalog y compruebe que haya una cartera en Administración, Carteras. 3. Elija la cartera y compruebe la información en las pestañas Productos, Restricciones y Acceso.	

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Elimine la CloudFormation pila.	Para eliminar la CloudFormation pila, haga lo siguiente: 1. Abre la AWS CloudFormation consola en https://console.aws.amazon.com/cloudformation. 2. En la barra de navegación de la parte superior de la pantalla, selecciona la Región de AWS ubicación de la pila. 3. En la página Pilas, seleccione la pila que desea eliminar. La pila se debe estar ejecutando en este momento. 4. En el panel de detalles de la pila, seleccione Eliminar. 5. Seleccione Eliminar pila cuando se le indique.	DevOps ingeniero, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte Eliminar una pila de la CloudFormation consola en la CloudFormation documentación	

Resolución de problemas

Problema	Solución

`e2e-test`
 	
`Can't find 'action.yml', 'action.yaml' or 'Dockerfile' under '*/home/runner/work/service-catalog-with-github-actions/service-catalog-with-github-actions`
 	
`Did you forget to run actions/checkout before running your local action?`
	Para asegurarse de que ha activado la configuración de repositorio correcta, haga lo siguiente:
	
	1. Vaya hasta el repositorio de Github y abra la pestaña Settings.
	2. Seleccione Actions y, luego, General en el menú izquierdo.
	3. Vaya a la sección Access y seleccione la opción Accessible from repositories in the 'XXX' organization.

Recursos relacionados

AWS documentación

- Descripción general de Service Catalog

Otros recursos

- Acerca de los eventos que desencadenan los flujos de trabajo (GitHub documentación)
- Reutilización de flujos de trabajo (GitHub documentación)

Información adicional

Para ver capturas de pantalla relacionadas con las epopeyas, ve a la carpeta Imágenes del repositorio de este patrón. GitHub Están disponibles las siguientes capturas de pantalla:

- AWS Service Catalog portafolio, sección de administración
- AWS Service Catalog producto, sección de administración
- AWS Service Catalog producto, User/Provisioning sección

Aprovisionamiento de roles de IAM con privilegio mínimo mediante la implementación de una solución de máquina expendedora de roles

Benjamin Morris, Nima Fotouhi, Aman Kaur Gandhi y Chad Moon, Amazon Web Services

Resumen

Los permisos excesivos en los roles de AWS Identity and Access Management (IAM) para las canalizaciones pueden suponer un riesgo innecesario para la organización. A veces, los desarrolladores conceden permisos amplios durante el desarrollo, pero se olvidan de limitarlos después de solucionar problemas con el código. Esto provoca un problema, pues puede que haya roles importantes sin necesidad empresarial y que posiblemente no haya revisado un ingeniero de seguridad.

Este patrón ofrece una solución a este problema: la máquina expendedora de roles (RVM). Mediante un modelo de implementación seguro y centralizado, el RVM demuestra cómo aprovisionar las funciones de IAM con menos privilegios para las canalizaciones de los repositorios individuales con un esfuerzo mínimo por parte de los desarrolladores. GitHub Como la RVM es una solución central, puede configurar sus equipos de seguridad como revisores necesarios para aprobar los cambios. Este enfoque permite al personal de seguridad rechazar las solicitudes de roles de canalizaciones con un exceso de permisos.

La RVM obtiene el código de Terraform como entrada y genera roles de IAM listos para su uso como salida. Las entradas obligatorias son el Cuenta de AWS ID, el nombre del repositorio y la política de permisos. GitHub La RVM usa estas entradas para crear la política de confianza y la política de permisos del rol. La política de confianza resultante permite que el GitHub repositorio especificado asuma la función y la utilice para las operaciones de canalización.

La RVM usa un rol de IAM (configurado durante el arranque). Este rol tiene permisos para asumir un rol role-provisioning-role en cada cuenta de la organización. El rol se configura mediante AWS Control Tower Account Factory for Terraform (AFT) o AWS CloudFormation StackSets. Estas role-provisioning-roles son las funciones que realmente crean las funciones de canalización para los desarrolladores.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.

- Una GitHub organización que se utiliza para implementar la infraestructura como código (IaC) mediante GitHub acciones. (no GitHub Enterprise/Premium/Ultimate son obligatorios).
- Un AWS entorno con varias cuentas. No es necesario que este entorno forme parte de AWS Organizations.
- Un mecanismo para implementar una función de IAM en todos Cuentas de AWS (por ejemplo, AFT o CloudFormation StackSets).
- La versión 1.3 o posterior de Terraform instalada y configurada.
- Instalación y configuración de Terraform AWS Provider, versión 4 o posterior.

Limitaciones

- El código de este patrón es específico de GitHub Actions y Terraform. Sin embargo, los conceptos generales del patrón se pueden reutilizar en otros marcos de integración y entrega continuas (CI/CD).
- Algunos Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

En el siguiente diagrama, se ilustra el flujo de trabajo de este patrón.

El flujo de trabajo para el uso típico de la máquina expendedora de roles consta de los siguientes pasos:

1. Un desarrollador envía el código que contiene el código de Terraform para un rol de IAM recién solicitado al repositorio de RVM. GitHub Esta acción activa la canalización de acciones de RVM. GitHub
2. La canalización utiliza una política de confianza de OpenID Connect (OIDC) para asumir el rol de la RVM.
3. Conforme se pone en marcha la canalización de la RVM, esta asume el rol de flujo de trabajo de la RVM en la cuenta en la que se aprovisiona el nuevo rol de IAM del desarrollador. (La función de flujo de trabajo de RVM se aprovisionó mediante AFT o.) CloudFormation StackSets

4. La RVM crea el rol de IAM del desarrollador con la confianza y los permisos adecuados, de modo que otras canalizaciones de la aplicación puedan asumir el rol.
5. Los desarrolladores de la aplicación pueden configurar las canalizaciones de la aplicación para que asuman este rol aprovisionado por RVM.

El rol creado incluye los permisos solicitados por el desarrollador y una política `ReadOnlyAccess`. El rol solo lo pueden asumir las canalizaciones que se ponen en marcha en la rama `main` del repositorio especificado por el desarrollador. Este enfoque permite garantizar que sea necesaria la protección y las revisiones de las ramas para poder utilizar el rol.

Automatización y escala

Los permisos con privilegio mínimo requieren prestar atención a los detalles de cada rol que se aprovisione. Este modelo reduce la complejidad necesaria para crear estos roles, lo que permite a los desarrolladores crear los roles que necesitan sin mucho aprendizaje o esfuerzo adicionales.

Tools (Herramientas)

Servicios de AWS

- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar múltiples cuentas Cuentas de AWS en una organización que usted crea y administra de forma centralizada.

Otras herramientas

- Git es un sistema de control de versiones distribuido y de código abierto. Incluye la posibilidad de crear una cuenta de organización.
- GitHub Actions es una plataforma de integración y entrega continuas (CI/CD) que está estrechamente integrada con GitHub los repositorios. Puedes usar GitHub Actions para automatizar tu proceso de creación, prueba e implementación.
- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que te ayuda a crear y administrar recursos locales y en la nube.

Repositorio de código

El código de este patrón está disponible en el repositorio. GitHub role-vending-machine

Prácticas recomendadas

- Haga que lo correcto sea fácil y que lo incorrecto sea difícil: procure que hacer lo correcto sea sencillo. Si los desarrolladores tienen dificultades con el proceso de aprovisionamiento de la RVM, podrían intentar crear roles por otros medios, lo que socavaría la naturaleza central de la RVM. Asegúrese de que su equipo de seguridad proporcione una guía clara sobre cómo utilizar la RVM de forma segura y eficaz.

  También debería impedir que los desarrolladores hagan cosas incorrectas. Usa las políticas de control de servicios (SCPs) o los límites de permisos para restringir qué roles pueden crear otros roles. Este enfoque puede ser útil para que solo la RVM y otros orígenes fiables puedan crear roles.
- Brinde buenos ejemplos: es inevitable que algunos desarrolladores usen los roles existentes en el repositorio de la RVM como plantillas informales para conceder permisos a sus nuevos roles. Si tiene ejemplos de privilegio mínimo para los desarrolladores, puede reducir el riesgo de que soliciten permisos amplios y con muchos caracteres comodín. Si empieza con roles con muchos permisos y muchos comodines, el problema puede multiplicarse con el paso del tiempo.
- Use condiciones y convenciones de nomenclatura: aunque un desarrollador no conozca todos los nombres de los recursos que va a crear su aplicación, debería limitar los permisos de los roles mediante una convención de nomenclatura. Por ejemplo, si el desarrollador está creando buckets de Amazon S3, el valor de la clave deñ recurso puede ser parecido a `arn:aws:s3:::myorg-myapp-dev-*` para que el rol no tenga permisos más allá de los buckets que coincidan con ese nombre. Implementar una convención de nomenclatura mediante una política de IAM tiene la ventaja adicional de mejorar el cumplimiento de la convención de nomenclatura. Esta mejora se debe a que no se permitirá la creación de recursos que no coincidan con dicha convención.
- Exija revisiones mediante solicitudes de extracción (PR): el valor de la solución de RVM es que crea una ubicación central donde se pueden revisar los nuevos roles de canalización. Sin embargo, este diseño solo es útil si hay barreras de protección que permitan garantizar que la RVM reciba código seguro y de alta calidad. Proteja las ramas que se utilizan para implementar código (por ejemplo, `main`) de las inserciones directas y solicite la aprobación de cualquier solicitud para fusionarlas.
- Configure los roles de solo lectura: de forma predeterminada, la RVM aprovisiona una versión `readonly` de cada rol solicitado. Esta función se puede usar en CI/CD canalizaciones que no escriben datos, como un flujo de trabajo de `terraform plan` canalización. Este enfoque ayuda a evitar cambios no deseados si un flujo de trabajo de solo lectura no funciona correctamente.

De forma predeterminada, la `ReadOnlyAccess` política AWS administrada está asociada tanto a las funciones de solo lectura como a las funciones de lectura y escritura. Esta política reduce la necesidad de iteración a la hora de determinar los permisos necesarios, pero puede resultar demasiado permisiva para algunas organizaciones. Si lo desea, puede eliminar la política del código de Terraform.

- Otorgue permisos mínimos: siga el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Preparación del entorno

Tarea	Descripción	Habilidades requeridas
Copie el repositorio de muestras en su organización. GitHub	Clona el repositorio de este patrón o bifurca este repositorio a tu GitHub organización para que puedas adaptarlo a tus necesidades. • Si elige clonar este repositorio, puede usar el siguiente comando: `git clone https://github.com/aws-samples/role-vending-machine` • Si decides bifurcar el repositorio a tu GitHub organización, puedes usar el siguiente comando: `gh repo fork aws-samples/role-vending-machine`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`--org YOUR_ORGANIZATION_NAME`	
Determine el Cuenta de AWS para el RVM.	Determine qué implementación de infraestructura usar Cuenta de AWS para la RVM. No utilice la cuenta de administración ni la cuenta raíz.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
(Opcional) Permita que se creen las canalizaciones de la organización. PRs	**Note** Este paso solo es necesario si quieres permitir la creación PRs del `generate_providers_and_account_vars` flujo de trabajo. Para permitir la creación de las canalizaciones de tu organización PRs, sigue estos pasos: 1. Vaya a `https://github.com/organizations/YOUR_ORG/settings/actions` . 2. Selecciona Permitir GitHub acciones para crear y aprobar solicitudes de extracción. Para obtener más información, consulte Administrar la configuración de GitHub las acciones de un repositorio en la GitHub documentación.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Otorgue permisos de solo lectura a la cuenta de la RVM.	Cree una política de delegación en su cuenta de administración que conceda permisos de solo lectura a la cuenta de la RVM. Esto permite que los GitHub flujos de trabajo de RVM obtengan dinámicamente una lista de las cuentas de su AWS organización cuando se ejecute el `generate_providers_and_account_vars.py` script. Utilice el siguiente código y `<YOUR RVM Account ID>` sustitúyalo por el Cuenta de AWS ID que seleccionó en el paso 2: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "Statement", "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::<YOUR RVM Account ID>:root" }, "Action": [ "organizations:ListAccounts",`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	"organizations:DescribeOrganization", "organizations:DescribeOrganizationalUnit", "organizations:ListRoots", "organizations:ListAWSServiceAccessForOrganization", "organizations:ListDelegatedAdministrators"], "Resource": "*" }] }	

Tarea	Descripción	Habilidades requeridas
Actualice los valores predeterminados del repositorio de ejemplo.	Para configurar el RVM para que funcione en su entorno específico Región de AWS, haga lo siguiente: 1. Actualice `scripts/generate_providers_and_account_vars.py` y otros archivos (como la carpeta `bootstrap`) con la región correspondiente en la que opera. 2. Actualice el `.github/workflows/.env` archivo con el Cuenta de AWS ID, la región y cualquier otra variable que desee especificar.	DevOps ingeniero

Inicialización de la infraestructura

Tarea	Descripción	Habilidades requeridas
Inicie el repositorio de la RVM.	Este paso es necesario para crear los roles de IAM y la política de confianza de OIDC que utiliza la propia canalización de la RVM, de modo que pueda empezar a operar y ofrecer otros roles. En la cuenta de la RVM, ponga en marcha manualmente un comando `terraform`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`apply` desde el directorio `scripts/bootstrap` . Proporcione los valores necesarios en función de la documentación de las variables.	

Configuración de operaciones

Tarea	Descripción	Habilidades requeridas
Implemente los roles `github-workflow-rvm` y `github-workflow-rvm-readonly` en todas las cuentas.	Elija un método de implementación que se adapte a las prácticas de su organización, como AFT o StackSets . Utilice ese método para implementar las dos roles de IAM del archivo `scripts/assumed_role/main.tf` (nombres predeterminados `github-workflow-rvm` y `github-workflow-rvm-readonly`) en cada cuenta en la que desee que la RVM pueda crear roles de canalización. Estos roles de IAM tienen políticas de confianza que permiten que el rol de asunción de roles de la cuenta de la RVM (o su `readonly` equivalente) los asuma. Los roles también tienen políticas de permisos de IAM que les	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	permiten leer roles y escribir (a menos que usen el rol `readonly`) en ellos, siempre que coincidan con `github-workflow-role-*` .	
Ponga en marcha el flujo de trabajo `generate_providers_and_account_vars` .	Para configurar su RVM de forma que esté lista para crear roles de canalización, haga lo siguiente: 1. Ponga en marcha el flujo de trabajo `generate_providers_and_account_vars` mediante workflow_dispatch. 2. Fusione la solicitud de extracción que crea el flujo de trabajo. Una vez finalizado el flujo de trabajo, la RVM está listo para hacer lo siguiente: • Aceptar solicitudes de nuevos roles de canalización. • Crear roles de solo lectura o de lectura y escritura según se solicite. • Despliegue las funciones según lo especificado Cuentas de AWS.	DevOps ingeniero

Resolución de problemas

Problema	Solución
He creado un rol mediante el RVM, pero GitHub no puedo asumirlo.	Compruebe que el nombre del GitHub repositorio coincide con el nombre proporcionado al `github_workflow_roles` módulo. El alcance de los roles solo permite que un único repositorio pueda asumirlos. Del mismo modo, compruebe que la rama utilizada en la GitHub canalización coincida con el nombre de la rama proporcionada al `github_workflow_roles` módulo. Por lo general, los roles creados por la RVM con permisos de escritura solo los pueden usar los flujos de trabajo relacionados con la rama `main` (es decir, las implementaciones provenientes de `main`).
Mi rol de solo lectura no puede poner en marcha su canalización porque carece de permisos para leer un recurso específico.	Si bien la `ReadOnlyAccess` política proporciona amplios permisos de solo lectura, no incluye algunas acciones de lectura (por ejemplo, determinadas AWS Security Hub CSPM acciones). Puede agregar permisos de acciones específicas mediante el parámetro `inline_policy_readonly` del módulo `github-workflow-roles` .

Recursos relacionados

- Prácticas recomendadas de uso AWS CloudFormation StackSets
- Organizar su AWS entorno mediante varias cuentas
- Descripción general de AWS Control Tower Account Factory para Terraform (AFT)

- Mejores prácticas en materia de políticas

Información adicional

Uso de GitHub entornos

GitHub Los entornos son un enfoque alternativo a las restricciones basadas en las sucursales para el acceso a los roles. Si prefiere utilizar un GitHub entorno, a continuación se muestra un ejemplo de la sintaxis de una condición adicional de la política de confianza de IAM. Esta sintaxis especifica que el rol solo se puede usar cuando la GitHub acción se ejecuta en el `Production` entorno.

```
"StringLike": {
    "token.actions.githubusercontent.com:sub": "repo:octo-org/octo-
repo:environment:Production"
}
```

La sintaxis de ejemplo usa los siguientes valores de marcador de posición:

- `octo-org`es el nombre GitHub de la organización.
- `octo-repo` es el nombre del repositorio.
- `Production`es el nombre del GitHub entorno específico.

Publica CloudWatch las métricas de Amazon en un archivo CSV

Abdullahi Olaoye, Amazon Web Services

Resumen

Este patrón utiliza un script de Python para recuperar CloudWatch las métricas de Amazon y convertir la información de las métricas en un archivo de valores separados por comas (CSV) para mejorar la legibilidad. El script toma como argumento obligatorio el servicio de AWS cuyas métricas deben recuperarse. Puede especificar la región de AWS y el perfil de credenciales de AWS como argumentos opcionales. Si no especifica esos argumentos, el script utilizará la región y el perfil predeterminados configurados para la estación de trabajo en la que se ejecuta el script. Una vez ejecutado, el script genera y almacena un archivo CSV en el mismo directorio.

Consulte la sección Adjuntos para ver el script y los archivos asociados que se proporcionan con este patrón.

Requisitos previos y limitaciones

Requisitos previos

- Python 3.x
- Interfaz de la línea de comandos de AWS (AWS CLI)

Limitaciones

El script en estos momentos admite los siguientes servicios de AWS:

- AWS Lambda
- Amazon Elastic Compute Cloud (Amazon EC2)
  - De forma predeterminada, el script no recopila métricas de volúmenes de Amazon Elastic Block Store (Amazon EBS). Para recopilar las métricas de Amazon EBS, debe modificar el archivo adjunto `metrics.yaml`.
- Amazon Relational Database Service (Amazon RDS)
  - Sin embargo, el script no es compatible con Amazon Aurora.
- Equilibrador de carga de aplicación
- Equilibrador de carga de red
- Amazon API Gateway

Tools (Herramientas)

- Amazon CloudWatch es un servicio de supervisión creado para DevOps ingenieros, desarrolladores, ingenieros de confiabilidad de sitios (SREs) y administradores de TI. CloudWatch proporciona datos e información procesable para ayudarlo a monitorear sus aplicaciones, responder a los cambios de rendimiento en todo el sistema, optimizar la utilización de los recursos y obtener una visión unificada del estado operativo. CloudWatch recopila datos operativos y de supervisión en forma de registros, métricas y eventos, y proporciona una vista unificada de los recursos, las aplicaciones y los servicios de AWS que se ejecutan en AWS y en servidores locales.

Epics

Instalar y configurar los requisitos previos

Tarea	Descripción	Habilidades requeridas
Instalar los requisitos previos.	Use el siguiente comando: `$ pip3 install -r requirements.txt`	Desarrollador
Configure la CLI de AWS.	Use el siguiente comando: `$ aws configure`	Desarrollador

Configuración del script de Python

Tarea	Descripción	Habilidades requeridas
Abra el script.	Para cambiar la configuración predeterminada del script, abra `metrics.yaml` .	Desarrollador
Defina el período del script.	Este es el período de tiempo para realizar la búsqueda. El período predeterminado es	Desarrollador

Tarea	Descripción	Habilidades requeridas
	de 5 minutos (300 segundos) . Puede cambiar el período de tiempo, pero tenga en cuenta las siguientes limitaciones: • Si el valor de horas que especificó es de entre 3 horas y 15 días atrás, utilice un múltiplo de 60 segundos (1 minuto) para el período. • Si el valor de horas que especificó es de entre 15 horas y 63 días atrás, utilice un múltiplo de 300 segundos (5 minutos) para el período. • Si el valor de horas que especificó es mayor que 63 días atrás, utilice un múltiplo de 3.600 segundos (1 hora) para el período. De lo contrario, la operación de la API no devolverá ningún punto de datos.	
Defina las horas del script.	Este valor especifica cuántas horas de métricas desea obtener. El valor predeterm inado es una hora. Para recuperar métricas de varios días, proporcione el valor en horas. Por ejemplo, para 2 días, especifique 48.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Cambie los valores de las estadísticas del script.	(Opcional) El valor de las estadísticas globales es `Average`, que se utiliza al buscar métricas que no tienen asignado un valor estadístico específico. El script admite los valores estadísticos `Maximum`, `SampleCount` y `Sum`.	Desarrollador

Ejecute el script de Python

Tarea	Descripción	Habilidades requeridas

Ejecute el script.	Utilice el siguiente comando:
	`$ python3 cwreport.py <service>`
	Para ver una lista de los valores del servicio y los `region` opcionales y parámetros `profile`, ejecute el siguiente comando:
	`$ python3 cwreport.py -h`
	Para más información sobre los parámetros opcionales, consulte la sección Informaci ón adicional.
		Desarrollador

Recursos relacionados

- Configuración de la CLI de AWS
- Uso de CloudWatch las métricas de Amazon
- CloudWatch Documentación de Amazon
- EC2 CloudWatch Métricas
- Métricas de AWS Lambda
- Métricas de Amazon RDS
- Métricas del Equilibrador de carga de aplicación
- Métricas del Equilibrador de carga de red
- Métricas de Amazon API Gateway

Información adicional

Uso de scripts

```
$ python3 cwreport.py -h
```

Ejemplo de sintaxis

```
python3 cwreport.py <service> <--region=Optional Region> <--profile=Optional credential
 profile>
```

Parámetros

- servicio (obligatorio): el servicio en el que desea ejecutar el script. Actualmente, el script es compatible con los siguientes servicios: AWS Lambda, Amazon, EC2 Amazon RDS, Application Load Balancer, Network Load Balancer y API Gateway.
- región (opcional): la región de AWS de la que se van a obtener las métricas. La región predeterminada es `ap-southeast-1`.
- perfil (opcional): el perfil con nombre de la CLI de AWS que se va a utilizar. Si no se especifica este parámetro, se utiliza el perfil de credenciales configurado por defecto.

Ejemplos

- Para usar la región predeterminada `ap-southeast-1` y las credenciales configuradas por defecto para obtener las EC2 métricas de Amazon: `$ python3 cwreport.py ec2`
- Para especificar una región y obtener las métricas de API Gateway: `$ python3 cwreport.py apigateway --region us-east-1`
- Para especificar un perfil de AWS y obtener las EC2 métricas de Amazon: `$ python3 cwreport.py ec2 --profile testprofile`
- Para especificar la región y el perfil para obtener las EC2 métricas de Amazon: `$ python3 cwreport.py ec2 --region us-east-1 --profile testprofile`

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Elimine EC2 las entradas de Amazon Cuentas de AWS de un lado a otro AWS Managed Microsoft AD mediante AWS Lambda la automatización

Dr. Rahul Sharad Gaikwad y Tamilselvan P, Amazon Web Services

Resumen

Active Directory (AD) es una herramienta de secuencias de comandos de Microsoft que administra la información de dominio y las interacciones de los usuarios con los servicios de red. Los proveedores de servicios gestionados (MSPs) lo utilizan ampliamente para gestionar las credenciales de los empleados y los permisos de acceso. Como los atacantes de AD pueden usar cuentas inactivas para intentar hackear una organización, es importante encontrar las cuentas inactivas y desactivarlas siguiendo un programa de mantenimiento rutinario. Con AWS Directory Service for Microsoft Active Directory, puede ejecutar Microsoft Active Directory como un servicio gestionado. Este patrón puede ayudarle a configurar la AWS Lambda automatización para encontrar y eliminar rápidamente las cuentas inactivas.

Si los siguientes escenarios se aplican a su organización, este patrón puede ser útil para lo siguiente:

- Administración centralizada de AD: si su organización tiene varias Cuentas de AWS, cada una con su propia implementación de AD, puede resultar difícil administrar las cuentas de usuario y los permisos de acceso de manera uniforme en todas las cuentas. Con una solución de limpieza de AD multicuenta, puede desactivar o eliminar las cuentas inactivas de todas las instancias de AD de forma centralizada.
- Reestructuración o migración de AD: si su organización planea reestructurar o migrar su implementación de AD, una solución de limpieza de AD multicuenta puede ser útil para preparar el entorno. Con esta solución, podrá eliminar cuentas innecesarias o inactivas, simplificar el proceso de migración y reducir los posibles conflictos o problemas.

Cuando utiliza este patrón, puede obtener los siguientes beneficios:

- Mejore el rendimiento de las bases de datos y los servidores, y corrija también de las vulnerabilidades de seguridad causadas por cuentas inactivas.
- Si su servidor de AD está alojado en la nube, eliminar las cuentas inactivas también puede reducir los costes de almacenamiento y, al mismo tiempo, mejorar el rendimiento. Es posible que sus facturas mensuales disminuyan porque los cargos asociados al uso de ancho de banda y los recursos de computación pueden disminuir.

- Mantenga a raya a los posibles atacantes con un Active Directory limpio.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta principal activa Cuenta de AWS y una o varias cuentas secundarias. En este patrón, una cuenta principal es donde se crea Active Directory. Las cuentas secundarias alojan servidores Windows y se unen a través de la cuenta principal de Active Directory.
- Git instalado y configurado en una estación de trabajo local.
- Terraform instalado y configurado en una estación de trabajo local.
- AWS Managed Microsoft AD directorio configurado en la cuenta principal y compartido con todas las cuentas secundarias. Para obtener más información, consulta el tutorial: Cómo compartir tu AWS Managed Microsoft AD directorio para EC2 unirte a un dominio sin problemas en la Guía de AWS Directory Service administración.
- Una conexión de emparejamiento de nube privada virtual (VPC) o una AWS Transit Gateway conexión disponible entre la VPC de AWS Directory Service (cuenta principal) y la VPC de las instancias de Amazon Elastic Compute Cloud (EC2Amazon) (cuentas secundarias). Para obtener más información, consulte Configure a VPC peering connection between the directory owner and the directory consumer account en la Guía de administración de AWS Directory Service .
- Una máquina Windows configurada con el script `EC2WindowsUserdata` en la cuenta principal y en todas las cuentas secundarias. El archivo de script está disponible en la raíz del repositorio de códigos de este patrón.
- Un rol multicuenta AWS Identity and Access Management (IAM) disponible en cada cuenta secundaria que está configurado con una política de confianza que permite el uso de una AWS Lambda función de la cuenta principal. Para obtener más información, consulta Enviar y recibir eventos entre Amazon Cuentas de AWS EventBridge en la Guía del EventBridge usuario de Amazon.
- Los siguientes valores secretos están disponibles en el almacén de AWS Systems Manager parámetros de la cuenta principal:
  - `domainJoinUser`: nombre de usuario del servicio de directorio
  - `domainJoinPassword`: contraseña del servicio de directorio

  Para obtener más información sobre los secretos, consulte Crear un AWS Secrets Manager secreto en la Guía del AWS Secrets Manager usuario.

Limitaciones

- La creación de un recurso en una cuenta secundaria no está automatizada con Terraform. Debe crear los siguientes recursos manualmente mediante Consola de administración de AWS:
  - EventBridge Regla de Amazon para enviar los eventos de EC2 rescisión de Amazon a la cuenta principal
  - Creación de roles EC2 multicuentas de Amazon en la cuenta secundaria con política de confianza
  - conexión de emparejamiento de VPC o Transit Gateway
- Algunas Servicios de AWS no están disponibles en todas las Regiones de AWS versiones. Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- Terraform, versión 1.1.9 o posterior
- Terraform AWS Provider versión 3.0 o superior

Arquitectura

El siguiente diagrama muestra la arquitectura de alto nivel de la solución.

El diagrama de arquitectura ilustra el proceso siguiente:

1. En las cuentas infantiles, la EventBridge regla recopila todos los eventos de EC2 rescisión de Amazon. La regla envía los eventos EventBridge que están presentes en la cuenta principal.
2. De la cuenta principal, EventBridge recopila todos los eventos y contiene la regla para activar la función Lambda. `ADcleanup-Lambda`
3. La cuenta principal recibe cualquier evento de terminación de la cuenta principal o secundaria y activa la función de Lambda.
4. La función Lambda realiza la llamada a los grupos de Amazon EC2 Auto Scaling mediante el módulo boto de Python y obtiene el ID de instancia aleatorio. El ID de instancia se utiliza para poner en marcha los comandos de Systems Manager.

5. La función Lambda realiza otra llamada a Amazon EC2 mediante el módulo boto. La función de Lambda obtiene las direcciones IP privadas de los servidores Windows en marcha y las almacena en una variable temporal. En los pasos 5.1 y 5.2, las EC2 instancias de Windows en ejecución se recopilan de las cuentas secundarias.
6. La función de Lambda hace otra llamada a Systems Manager para obtener la información del equipo conectado a AWS Directory Service.
7. Un AWS Systems Manager documento ayuda a ejecutar el PowerShell comando en los servidores de Amazon EC2 Windows para obtener las direcciones IP privadas de las computadoras que están conectadas a AD. (El documento de Systems Manager usa el ID de instancia que se obtuvo en el paso 4).
8. El nombre de usuario y las contraseñas del dominio AD se almacenan en el almacén de AWS Systems Manager parámetros. AWS Lambda y Systems Manager hacen una llamada a Parameter Store y obtienen los valores de nombre de usuario y contraseña que se utilizarán para conectarse a AD.
9. Con el documento Systems Manager, el PowerShell script se ejecuta en el servidor Amazon EC2 Windows utilizando el identificador de instancia obtenido anteriormente en el paso 4.
10. Amazon EC2 se conecta AWS Directory Service mediante PowerShell comandos y elimina los ordenadores que no están en uso o inactivos.

Tools (Herramientas)

AWS servicios

- AWS Directory Serviceproporciona varias formas de utilizar Microsoft Active Directory (AD) con otras, Servicios de AWS como Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS) para SQL Server y FSx Amazon para Windows File Server.
- AWS Directory Service for Microsoft Active Directorypermite que sus cargas de trabajo y AWS recursos compatibles con directorios utilicen Microsoft Active Directory en. Nube de AWS
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática escalable en el Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, AWS Lambda funciones, puntos de enlace de invocación HTTP que utilizan destinos de API o buses de eventos en otros. Cuentas de AWS

- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos. Con IAM, puede especificar quién o qué puede acceder a los servicios y recursos AWS, gestionar de forma centralizada los permisos detallados y analizar el acceso para restringir todos los permisos. AWS
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Systems Manager lo ayuda a administrar las aplicaciones y la infraestructura que se ejecutan en la Nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo necesario para detectar y resolver problemas operativos y le ayuda a gestionar sus recursos de forma segura y a escala. AWS
- AWS Systems Manager los documentos definen las acciones que Systems Manager realiza en las instancias gestionadas. Systems Manager incluye más de 100 documentos preconfigurados que puede utilizar especificando los parámetros en tiempo de ejecución.
- AWS Systems Manager El almacén de parámetros es una capacidad AWS Systems Manager y proporciona un almacenamiento jerárquico seguro para la administración de los datos de configuración y la administración de secretos.

Otras herramientas

- HashiCorp Terraform es una herramienta de infraestructura como código (IaC) que facilita usar el código para aprovisionar y administrar los recursos y la infraestructura en la nube.
- PowerShelles un programa de administración de automatización y configuración de Microsoft que se ejecuta en Windows, Linux y macOS.
- Python es un lenguaje de programación informático de uso general.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub aws-lambda-ad-cleanup-terraform-samples.

Prácticas recomendadas

- Unirse a dominios de manera automática.Cuando lances una instancia de Windows que vaya a formar parte de un Directory Service dominio, únete al dominio durante el proceso de creación de

la instancia en lugar de añadirla manualmente más adelante. Para unirse automáticamente a un dominio, seleccione el directorio correcto de la lista desplegable Directorio de unión al dominio al lanzar una nueva instancia. Para obtener más información, consulte Cómo unir sin problemas una instancia de Amazon EC2 Windows a AWS Managed Microsoft AD Active Directory en la Guía de Directory Service administración.

- Elimine las cuentas que no se usen.Es habitual encontrar cuentas en AD que nunca se han utilizado. Al igual que las cuentas desactivadas o inactivas que permanecen en el sistema, las cuentas no utilizadas y desatendidas pueden ralentizar el sistema de AD o hacer que la organización sea vulnerable a las filtraciones de datos.
- Automatice las limpiezas de Active Directory.Para mitigar los riesgos de seguridad y evitar que las cuentas obsoletas afecten al rendimiento de AD, las limpiezas de AD deberían realizarse con una frecuencia periódica. Puede realizar la mayoría de las tareas de administración y limpieza de AD escribiendo scripts. Algunos ejemplos de tareas son eliminar cuentas desactivadas e inactivas, eliminar grupos vacíos e inactivos y localizar cuentas de usuario y contraseñas caducadas.

Epics

Configuración de cuentas secundarias

Tarea	Descripción	Habilidades requeridas
Cree un rol multicuenta en la cuenta secundaria.	Para crear un rol multicuenta en una cuenta secundaria, haga lo siguiente: 1. En cada cuenta secundaria, cree un rol con el nombre `ec2crossaccountrole` usando la política administrada `AmazonEC2ReadOnlyAccess`. (Para obtener más información, consulte Crear un rol mediante políticas de confianza personalizadas	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	en la documentación de IAM). 2. En la sección Política de confianza personalizada, agregue el siguiente código: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "ec2.amazonaws.com" }, "Action": "sts:AssumeRole" }, { "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::${Parentaccountid}:role/ADcleanuprole" }, "Action": "sts:AssumeRole" } ] }`	

Tarea	Descripción	Habilidades requeridas
Cree una regla de eventos en la cuenta secundaria.	Para crear una EventBridge regla para cada cuenta secundaria, haga lo siguiente: 1. Inicia sesión con el niño y Cuenta de AWS, a continuación, abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/. 2. En el panel de navegación, seleccione Reglas. 3. Seleccione Crear regla. 4. Indique un nombre para la regla y, opcionalmente, una descripción. 5. En Bus de eventos, elija Bus de eventos predeterminado de AWS. 6. En Tipo de regla, elija Regla con un patrón de eventos. 7. Elija Siguiente. 8. En Patrón de eventos, pegue el siguiente código: `{ "source": ["aws.ec2"], "detail-type": ["EC2 Instance State-change Notification"], "detail": {`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	<pre>"state": ["terminated"]
	}
	}</pre>
	9. Elija Siguiente.
	10. En Tipo de destino, seleccione Bus de eventos en una cuenta o región diferente.En Bus de eventos como destino, ingrese el nombre de recurso de Amazon (ARN) del bus de eventos para la cuenta principal.
	11. En Rol de ejecución, elija Crear un nuevo rol para el recurso especificado.
	12. Seleccione Siguiente para revisar los detalles de la nueva regla y, a continuación, elija Crear.
	
	Para obtener más información, consulta Cómo crear reglas que reaccionen a los eventos en Amazon EventBridge en la Guía del EventBridge usuario de Amazon.	

Tarea	Descripción	Habilidades requeridas
Crea una EC2 instancia y únete a AD.	Para crear una EC2 instancia para Windows, haz lo siguiente: 1. Utilice el script `EC2WindowsUserdata` que está disponible en el repositorio de código de este patrón. 2. En el script de datos de usuario, revise el siguiente código para usar los valores de `Directory service addresses` de la cuenta principal: `set-DnsClientServerAddress -InterfaceIndex 6 -ServerAddresses $(Directory service addresses)`	DevOps ingeniero

Configuración de la estación de trabajo local

Tarea	Descripción	Habilidades requeridas
Cree una carpeta de proyecto y agregue los archivos.	Para clonar el repositorio y crear una carpeta de proyecto, haga lo siguiente: 1. Abre el GitHub repositorio de este patrón. 2. Seleccione el botón Code para ver las opciones	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	de clonación en el menú desplegable Clone.
	3. En la pestaña HTTPS, copie la URL proporcionada en Clone using the web URL.
	4. Cree una carpeta en su máquina y asígnele el nombre de su proyecto.
	5. Abra una terminal en su máquina local y navegue hasta esa carpeta.
	6. Para clonar el repositor io de git, use el siguiente comando.
	`git clone <reposito ry-URL>.git`
	7. Una vez clonado el repositorio, utilice el siguiente comando para ir al directorio clonado.
	`cd <directory name>/terraform-aw s-lambda-ad-cleanu p/multiple-account -cleanup`
	8. En el repositorio clonado, abra este proyecto en un entorno de desarroll o integrado (IDE) de su elección.	

Tarea	Descripción	Habilidades requeridas
Compile el archivo `adcleanup.zip` .	Para comprimir el archivo `lambda_function.py` , use el siguiente comando: `zip -r adcleanup.zip lambda_function.py`	DevOps ingeniero

Aprovisionamiento de la arquitectura de destino mediante la configuración de Terraform

Tarea	Descripción	Habilidades requeridas
Proporcione valores para las variables de Terraform.	En la cuenta secundaria, proporcione valores para las siguientes variables `arn` como tipos de cadenas en el archivo `terraform.tfvars` : • `lambda_env_cross_role_arn` • `child_account_cross_role_arn`	DevOps ingeniero
Inicialice la configuración de Terraform.	Para inicializar el directorio de trabajo que contiene los archivos de Terraform, use el siguiente comando: `terraform init`	DevOps ingeniero
Previsualice los cambios.	Puede obtener una vista previa de los cambios que Terraform realizará en la infraestructura antes de implementarla. Para comprobar que Terraform	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	realizará los cambios necesarios, use el siguiente comando: `terraform plan –– var-file=examples/ terraform.tfvars`	
Realice las acciones propuestas.	Para comprobar que los resultados del comando `terraform plan` sean los esperados, haga lo siguiente: 1. Ejecute el comando siguiente: `terraform apply` 2. Inicie sesión en Consola de administración de AWS y compruebe que los recursos estén presentes.	DevOps ingeniero

Verifique la implementación

Tarea	Descripción	Habilidades requeridas
Ponga en marcha y pruebe la función de Lambda.	Para verificar que la implementación se realizó correctamente, haga lo siguiente: 1. Inicie sesión en la Consola de administración de AWS consola Lambda y ábrala. Abra la página Funciones y seleccione el nombre de la	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	función que comience por ADcleanup-Lambda-*. 2. En la página de descripci ón general de la función, seleccione Probar en la pestaña Código de la sección Código fuente. 3. Para guardar el evento de prueba, proporcione un nombre para el evento y seleccione Guardar. Elija Probar de nuevo para probar el evento. Los resultados de la puesta en marcha muestran el resultado de la función.	

Tarea	Descripción	Habilidades requeridas
Vea los resultados de la ejecución de la EventBridge regla desde la cuenta principal .	Para ver los resultados de la EventBridge regla que se basa en los eventos de EC2 rescisión de Amazon desde la cuenta principal, haz lo siguiente: 1. EC2 Termina las instancias de la cuenta principal. 2. Abra la consola de Lambda de la cuenta principal. Abra la página Funciones y seleccione el nombre de la función que comience por ADcleanup-Lambda-*. 3. Seleccione la pestaña Supervisar y, a continuac ión, seleccione Ver registros. CloudWatch En la CloudWatch consola, la página Grupos de registros muestra los resultados de la función Lambda.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Vea los resultados de la ejecución de la EventBrid ge regla desde la cuenta secundaria.	Para ver los resultados de la EventBridge regla que se basa en los eventos de EC2 rescisión de Amazon desde la cuenta secundaria, haz lo siguiente: 1. EC2 Finaliza las instancias de la cuenta secundaria. 2. Abra la consola de Lambda de la cuenta principal. Abra la página Funciones y seleccione el nombre de la función que comience por ADcleanup-Lambda-*. 3. Seleccione la pestaña Supervisar y, a continuac ión, seleccione Ver registros. CloudWatch En la CloudWatch consola, la página Grupos de registros muestra los resultados de la función Lambda.	DevOps ingeniero

Limpieza de la infraestructura después de utilizarla

Tarea	Descripción	Habilidades requeridas
Limpie la infraestructura.	Para limpiar la infraestructura que ha creado, utilice el siguiente comando: `terraform destroy`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Para confirmar el comando `destroy`, escriba `yes`.	
Verifique después de limpiar.	Compruebe que los recursos se hayan eliminado correctam ente.	DevOps ingeniero

Resolución de problemas

Problema	Solución
Problema de conexión entre AWS Directory Service (cuenta principal) e EC2 instancia de Amazon (cuenta secundaria): no puedes unir los ordenadores de la cuenta secundaria a AD aunque la interconexión de VPC esté disponibl e.	Agregue el enrutamiento en. VPCs Para obtener instrucciones, consulte Configurar una conexión de emparejamiento de VPC entre el propietario del directorio y la cuenta del consumidor del directorio en la documentación. AWS Directory Service

Recursos relacionados

AWS documentación

- Amazon EventBridge y AWS Identity and Access Management
- Configuración de permisos de instancia requeridos para Systems Manager
- Gestión de identidad y acceso para Directory Service
- Políticas de IAM basadas en identidad para Lambda
- Unir manualmente una instancia de Amazon EC2 Windows a AWS Managed Microsoft AD Active Directory
- Elimine EC2 las entradas de Amazon en el mismo Cuenta de AWSAWS Managed Microsoft AD formulario mediante AWS Lambda la automatización

Otros recursos

- AWS Proveedor (documentación de Terraform)
- Backend Configuration (documentación de Terraform)
- Install Terraform (documentación de Terraform)
- Python boto module (repositorio Python Package Index)
- Terraform binary download (documentación de Terraform)

Elimine EC2 las entradas de Amazon en el mismo Cuenta de AWS AWS Managed Microsoft AD formulario mediante AWS Lambda la automatización

Dr. Rahul Sharad Gaikwad y Tamilselvan P, Amazon Web Services

Resumen

Active Directory (AD) es una herramienta de secuencias de comandos de Microsoft que administra la información de dominio y las interacciones de los usuarios con los servicios de red. Los proveedores de servicios gestionados (MSPs) la utilizan ampliamente para gestionar las credenciales de los empleados y los permisos de acceso. Como los atacantes de AD pueden usar cuentas inactivas para intentar hackear una organización, es importante encontrar las cuentas inactivas y desactivarlas siguiendo un programa de mantenimiento rutinario. Con AWS Directory Service for Microsoft Active Directory, puede ejecutar Microsoft Active Directory como un servicio gestionado.

Este patrón puede ayudarle a configurar la AWS Lambda automatización para encontrar y eliminar rápidamente las cuentas inactivas. Cuando utiliza este patrón, puede obtener los siguientes beneficios:

- Mejore el rendimiento de las bases de datos y los servidores, y corrija también de las vulnerabilidades de seguridad causadas por cuentas inactivas.
- Si su servidor de AD está alojado en la nube, eliminar las cuentas inactivas también puede reducir los costes de almacenamiento y, al mismo tiempo, mejorar el rendimiento. Es posible que sus facturas mensuales disminuyan porque los cargos asociados al uso de ancho de banda y los recursos de computación pueden disminuir.
- Mantenga a raya a los posibles atacantes con un Active Directory limpio.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.
- Git instalado y configurado en una estación de trabajo local.
- Terraform instalado y configurado en una estación de trabajo local.
- Equipo Windows con módulos de Active Directory (`ActiveDirectory`).

- Un directorio AWS Managed Microsoft AD y credenciales almacenadas en un parámetro del almacén de AWS Systems Manager parámetros.
- AWS Identity and Access Management (IAM) con permisos para los que Servicios de AWS aparecen en Herramientas. Para obtener más información sobre IAM, consulte Recursos relacionados.

Limitaciones

- Este patrón no admite la configuración multicuenta.
- Algunos Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- Terraform, versión 1.1.9 o posterior
- La versión 3.0 o posterior del Proveedor de AWS para Terraform

Arquitectura

En el siguiente diagrama se muestran los componentes de la arquitectura y el flujo de trabajo de esta aplicación.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Amazon EventBridge activa la AWS Lambda función basándose en una expresión cron. (En este patrón, las expresiones cron están programadas una vez al día).
2. La función y la política de IAM requeridas se crean y se adjuntan a AWS Lambda través de Terraform.
3. La AWS Lambda función se ejecuta y llama a los grupos de Auto Scaling de Amazon Elastic Compute Cloud (Amazon EC2) mediante el módulo boto de Python. La función de Lambda obtiene el ID de instancia aleatorio. El identificador de instancia se usa para ejecutar AWS Systems Manager comandos.

4. AWS Lambda realiza otra llamada a Amazon EC2 mediante el módulo boto y obtiene las direcciones IP privadas de los servidores Windows en ejecución y las almacena en una variable temporal.
5. AWS Lambda realiza otra llamada a Systems Manager para obtener la información del equipo al que está conectado Directory Service.
6. Un AWS Systems Manager documento ayuda a ejecutar el PowerShell script en los servidores de Amazon EC2 Windows para obtener las direcciones IP privadas de los ordenadores que están conectados a AD.
7. El nombre de usuario y las contraseñas del dominio AD se almacenan en el almacén de AWS Systems Manager parámetros. AWS Lambda y Systems Manager hacen una llamada a Parameter Store y obtienen los valores de nombre de usuario y contraseña que se utilizarán para conectar AD.
8. Con el documento Systems Manager, el PowerShell script se ejecuta en el servidor Amazon EC2 Windows utilizando el identificador de instancia obtenido anteriormente en el paso 3.
9. Amazon EC2 se conecta Directory Service mediante PowerShell comandos y elimina los ordenadores que no están en uso o inactivos.

Tools (Herramientas)

Servicios de AWS

- AWS Directory Serviceproporciona varias formas de utilizar Microsoft Active Directory (AD) con otras, Servicios de AWS como Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS) para SQL Server y FSx Amazon para Windows File Server.
- AWS Directory Service for Microsoft Active Directorypermite que sus cargas de trabajo y AWS recursos compatibles con directorios utilicen Microsoft Active Directory en. Nube de AWS
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática escalable en el Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, AWS Lambda funciones, puntos de enlace de invocación HTTP que utilizan destinos de API o buses de eventos en otros. Cuentas de AWS
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos. Con IAM, puede

especificar quién o qué puede acceder a los servicios y recursos AWS, gestionar de forma centralizada los permisos detallados y analizar el acceso para restringir todos los permisos. AWS

- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Systems Manager lo ayuda a administrar las aplicaciones y la infraestructura que se ejecutan en la Nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo necesario para detectar y resolver problemas operativos y le ayuda a gestionar sus recursos de forma segura y a escala. AWS
- AWS Systems Manager los documentos definen las acciones que Systems Manager realiza en las instancias gestionadas. Systems Manager incluye más de 100 documentos preconfigurados que puede utilizar especificando los parámetros en tiempo de ejecución.
- AWS Systems Manager El almacén de parámetros es una capacidad AWS Systems Manager y proporciona un almacenamiento jerárquico seguro para la administración de datos de configuración y la administración de secretos.

Otras herramientas

- HashiCorp Terraform es una herramienta de código abierto de infraestructura como código (IaC) que le ayuda a usar el código para aprovisionar y administrar la infraestructura y los recursos de la nube.
- PowerShelles un programa de administración de automatización y configuración de Microsoft que se ejecuta en Windows, Linux y macOS.
- Python es un lenguaje de programación informático de uso general.

Repositorio de código

El código de este patrón está disponible en el repositorio de soluciones GitHub personalizadas de AD Cleanup Automation.

Prácticas recomendadas

- Unirse a dominios de manera automática.Cuando lances una instancia de Windows que vaya a formar parte de un Directory Service dominio, únete al dominio durante el proceso de creación de la instancia en lugar de añadirla manualmente más adelante. Para unirse automáticamente a un

dominio, seleccione el directorio correcto de la lista desplegable Directorio de unión al dominio al lanzar una nueva instancia. Para obtener más información, consulte Cómo unir sin problemas una instancia de Amazon EC2 Windows a AWS Managed Microsoft AD Active Directory en la Guía de Directory Service administración.

- Elimine las cuentas que no se usen.Es habitual encontrar cuentas en AD que nunca se han utilizado. Al igual que las cuentas desactivadas o inactivas que permanecen en el sistema, las cuentas no utilizadas y desatendidas pueden ralentizar el sistema de AD o hacer que la organización sea vulnerable a las filtraciones de datos.
- Automatice las limpiezas de Active Directory.Para mitigar los riesgos de seguridad y evitar que las cuentas obsoletas afecten al rendimiento de AD, las limpiezas de AD deberían realizarse con una frecuencia periódica. Puede realizar la mayoría de las tareas de administración y limpieza de AD escribiendo scripts. Algunos ejemplos de tareas son eliminar cuentas desactivadas e inactivas, eliminar grupos vacíos e inactivos y localizar cuentas de usuario y contraseñas caducadas.

Epics

Configure su entorno

Tarea	Descripción	Habilidades requeridas
Cree una carpeta de proyecto y agregue los archivos.	Para clonar el repositorio y crear una carpeta de proyecto, haga lo siguiente: 1. Abra el GitHub repositorio de este patrón. 2. Seleccione el botón Code para ver las opciones de clonación en el menú desplegable Clone. 3. En la pestaña HTTPS, copie la URL proporcionada en Clone using the web URL.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	4. Cree una carpeta en su máquina y asígnele el nombre de su proyecto.
	5. Abra una terminal en su máquina local y navegue hasta esa carpeta.
	6. Para clonar el repositorio de git, use el siguiente comando.
	`git clone <repository-URL>.git`
	7. Una vez clonado el repositorio, utilice el siguiente comando para ir al directorio clonado.
	`cd <directory name>`
	8. En el repositorio clonado, abra este proyecto en un entorno de desarrollo integrado (IDE) de su elección.	

Aprovisionamiento de la arquitectura de destino mediante la configuración de Terraform

Tarea	Descripción	Habilidades requeridas
Inicialice la configuración de Terraform.	Para inicializar el directorio de trabajo que contiene los archivos de Terraform, use el siguiente comando. `terraform init`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Previsualice los cambios.	Puede obtener una vista previa de los cambios que Terraform realizará en la infraestructura antes de implementarla. Para comprobar que Terraform realizará los cambios necesarios, use el siguiente comando. `terraform plan`	DevOps ingeniero
Realice las acciones propuestas.	Para comprobar que los resultados del comando `terraform plan` sean los esperados, haga lo siguiente: 1. Ejecute el comando siguiente. `terraform apply` 2. Inicie sesión en Consola de administración de AWS y compruebe que los recursos estén presentes.	DevOps ingeniero
Limpie la infraestructura.	Para limpiar la infraestructura que ha creado, utilice el siguiente comando. `terraform destroy` Para confirmar el comando de eliminación, ingrese `yes`.	DevOps ingeniero

Verifique la implementación

Tarea	Descripción	Habilidades requeridas
Ponga en marcha y pruebe la función de Lambda.	Para verificar que la implementación se realizó correctamente, haga lo siguiente: 1. Inicie sesión en la consola Consola de administración de AWS y ábrala. Abra la página Funciones y seleccione el nombre de la función que comience por ADcleanup-Lambda-*. 2. En la página de descripci ón general de la función, seleccione Probar en la pestaña Código de la sección Código fuente. 3. Para guardar el evento de prueba, proporcione un nombre para el evento y seleccione Guardar. A continuación, elija Probar de nuevo para probar el evento. Los resultados de la puesta en marcha muestran el resultado de la función.	DevOps ingeniero
Vea los resultados de la función de Lambda.	En este patrón, una EventBrid ge regla ejecuta la función Lambda una vez al día. Para ver los resultados de la	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	función de Lambda, haga lo siguiente: 1. Inicie sesión en la consola Consola de administración de AWS y ábrala. AWS Lambda Abra la página Funciones y seleccione el nombre de la función que comience por ADcleanup-Lambda-*. 2. Seleccione la pestaña Supervisar y, a continuac ión, seleccione Ver registros. CloudWatch En la CloudWatch consola, la página Grupos de registros muestra los resultados de la función Lambda.	

Limpieza de la infraestructura después de utilizarla

Tarea	Descripción	Habilidades requeridas
Limpie la infraestructura.	Para limpiar la infraestructura que ha creado, utilice el siguiente comando. `terraform destroy` Para confirmar el comando de eliminación, ingrese `yes`.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Verifique después de limpiar.	Compruebe que los recursos se hayan eliminado correctam ente.	DevOps ingeniero

Resolución de problemas

Problema	Solución
Si intenta eliminar el equipo de AD, aparecerá un mensaje de “Acceso denegado”. No se puede eliminar el equipo de AD porque, de forma predeterminada, la acción intenta eliminar dos direcciones IP privadas que están conectadas como parte de los servicios de AD.	Para evitar este error, utilice la siguiente operación de Python para ignorar los dos primeros equipos al enumerar las diferencias entre la salida de un equipo de AD y la salida de un equipo que usa Windows. `Difference = Difference[2:]`
Cuando Lambda ejecuta un PowerShell script en un servidor Windows, espera que los módulos de Active Directory estén disponibles de forma predeterminada. Si los módulos no están disponibles, una función Lambda crea un error que indica que «Get- no AdComputer está instalado en la instancia».	Para evitar este error, instala los módulos necesarios utilizando los datos de usuario de las EC2 instancias. Usa el EC2Window sUserdatascript que se encuentra en el GitHub repositorio de este patrón.

Recursos relacionados

AWS documentación

- Amazon EventBridge y AWS Identity and Access Management
- Configuración de permisos de instancia requeridos para Systems Manager
- Gestión de identidad y acceso para Directory Service
- Unir manualmente una instancia de Amazon EC2 Windows a AWS Managed Microsoft AD Active Directory

- Trabaje con políticas de IAM basadas en la identidad en AWS Lambda

Otros recursos

- AWS Proveedor (documentación de Terraform)
- Backend Configuration (documentación de Terraform)
- Install Terraform (documentación de Terraform)
- Python boto module (repositorio Python Package Index)
- Terraform binary download (documentación de Terraform)

Ejecute pruebas unitarias para trabajos ETL de Python AWS Glue utilizando el marco pytest

Praveen Kumar Jeyarajan y Vaidy Sankaran, Amazon Web Services

Resumen

Puede ejecutar pruebas unitarias para trabajos de extracción, transformación y carga (ETL) de Python AWS Glue en un entorno de desarrollo local, pero replicar esas pruebas en una DevOps canalización puede resultar difícil y llevar mucho tiempo. Las pruebas unitarias pueden resultar especialmente complicadas cuando se moderniza el proceso de ETL de un mainframe basándolo en AWS tecnologías. Este patrón le muestra cómo simplificar las pruebas unitarias y, al mismo tiempo, mantener intacta la funcionalidad existente, evitar interrupciones de funcionalidad de la aplicaciones clave cuando se lanzan nuevas características y mantener un software de alta calidad. Puede usar los pasos y los ejemplos de código de este patrón para ejecutar pruebas unitarias para trabajos ETL de Python AWS Glue utilizando el marco pytest en AWS CodePipeline. También puedes usar este patrón para probar e implementar varios AWS Glue trabajos.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Un URI de imagen de Amazon Elastic Container Registry (Amazon ECR) para AWS Glue su biblioteca, descargado de la galería pública de Amazon ECR
- Un terminal Bash (en cualquier sistema operativo) con un perfil para el destino y Cuenta de AWS Región de AWS
- Python 3.10 o posterior
- Pytest
- Biblioteca Moto Python para pruebas Servicios de AWS

Arquitectura

El siguiente diagrama describe cómo incorporar las pruebas unitarias para los procesos de AWS Glue ETL basados en Python en una canalización típica de escala empresarial AWS DevOps .

En el diagrama, se muestra el siguiente flujo de trabajo:

1. En la fase de código fuente, AWS CodePipeline utiliza un bucket versionado de Amazon Simple Storage Service (Amazon S3) para almacenar y gestionar los activos del código fuente. Estos activos incluyen un ejemplo de trabajo ETL de Python (`sample.py`), un archivo de prueba unitaria (`test_sample.py`) y una AWS CloudFormation plantilla. A continuación, CodePipeline transfiere el código más reciente de la rama principal al AWS CodeBuild proyecto para su posterior procesamiento.
2. En la fase de creación y publicación, el código más reciente de la fase fuente anterior se somete a pruebas unitarias con la ayuda de una imagen AWS Glue pública de Amazon ECR. A continuación, el informe de la prueba se publica en los grupos de CodeBuild informes. La imagen del contenedor del repositorio público de Amazon ECR para AWS Glue bibliotecas incluye todos los binarios necesarios para ejecutar tareas ETL PySparkbasadas en AWS Glue pruebas unitarias de forma local. El repositorio de contenedores público tiene tres etiquetas de imagen, una para cada versión compatible con AWS Glue. Con fines de demostración, este patrón usa la etiqueta de imagen `glue_libs_4.0.0_image_01`. Para usar esta imagen de contenedor como imagen en tiempo de ejecución CodeBuild, copie el URI de la imagen que corresponda a la etiqueta de imagen que pretende usar y, a continuación, actualice el `pipeline.yml` archivo en el GitHub repositorio del recurso. `TestBuild`
3. En la fase de despliegue, el CodeBuild proyecto se lanza y publica el código en un bucket de Amazon S3 si se aprueban todas las pruebas.
4. El usuario implementa la AWS Glue tarea mediante la CloudFormation plantilla de la `deploy` carpeta.

Tools (Herramientas)

Servicios de AWS

- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- AWS CodePipeline permite diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software y automatizar los pasos necesarios para lanzar los cambios en el software de manera continua.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- AWS Glue es un servicio de ETL completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento líderes del sector.

Otras herramientas

- Python es un lenguaje de programación de uso general interpretado de alto nivel.
- Moto es una biblioteca de Python para realizar pruebas Servicios de AWS.
- Pytest es un marco para escribir pruebas unitarias pequeñas que se escalan para permitir pruebas funcionales complejas para aplicaciones y bibliotecas.
- La biblioteca ETL de Python para AWS Glue es un repositorio de bibliotecas de Python que se utilizan en el desarrollo local de trabajos PySpark por lotes para AWS Glue.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub aws-glue-jobs-unit-testing. El repositorio incluye los siguientes recursos:

- Un ejemplo de AWS Glue trabajo basado en Python en la carpeta `src`
- Los casos de pruebas unitarias asociados (creados con el marco pytest) están en la carpeta `tests`
- Una CloudFormation plantilla (escrita en YAML) en la carpeta `deploy`

Prácticas recomendadas

Seguridad de los recursos CodePipeline

Se recomienda utilizar el cifrado y la autenticación en los repositorios de origen que se conectan a tus canalizaciones. CodePipeline Para obtener más información, consulta las prácticas recomendadas de seguridad en la CodePipeline documentación.

Supervisión y registro de los CodePipeline recursos

Se recomienda utilizar las funciones de AWS registro para determinar qué acciones realizan los usuarios en tu cuenta y qué recursos utilizan. Los archivos de registro muestran lo siguiente:

- La fecha y la hora de las acciones
- Dirección IP de origen de las acciones

- Las acciones que han fallado debido a permisos inadecuados

Las funciones de registro están disponibles en AWS CloudTrail Amazon CloudWatch Events. Puede utilizarlas CloudTrail para registrar las llamadas a la AWS API y los eventos relacionados realizados por usted o en su nombre Cuenta de AWS. Para obtener más información, consulta Cómo registrar las llamadas a la CodePipeline API AWS CloudTrail en la CodePipeline documentación.

Puede usar CloudWatch Events para supervisar Nube de AWS los recursos y las aplicaciones que se estén ejecutando AWS. También puede crear alertas en CloudWatch Eventos. Para obtener más información, consulte Supervisión de CodePipeline eventos en la CodePipeline documentación.

Epics

Implementar el código fuente

Tarea	Descripción	Habilidades requeridas
Prepare el archivo de códigos para su implementación.	1. Descárguelo `code.zip` del repositorio GitHub aws-glue-jobs-unit-testing o cree el archivo.zip usted mismo mediante una herramien ta de línea de comandos. Por ejemplo, puede crear el archivo .zip en Linux o Mac ejecutando los siguientes comandos en la terminal: `git clone https://g ithub.com/aws-samp les/aws-glue-jobs- unit-testing.git cd aws-glue-jobs- unit-testing git checkout master zip -r code.zip src/ tests/ deploy/`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	2. Inicie sesión en Consola de administración de AWSy elija el que prefiera. Región de AWS 3. Cree un bucket de S3 y, a continuación, cargue el paquete .zip y el archivo `code.zip` (descargados anteriormente) en el bucket de Amazon S3 creado.	

Tarea	Descripción	Habilidades requeridas
Crea la CloudFormation pila.	1. Inicie sesión en la CloudFormation consola Consola de administración de AWS y, a continuación, ábrala. 2. Elija Create stack (Crear pila) y, a continuación, seleccione With existing resources (import resources) (Con recursos existentes (importar recursos)). 3. En la sección Especificar la plantilla de la página Crear pila, selecciona Cargar un archivo de plantilla y, a continuación, elige la plantilla pipeline.yml (descargada del repositor io). GitHub A continuación, elija Siguiente. 4. En Nombre de pila glue-unit -testing-pipeline, introduce o elige el nombre de pila que prefieras. 5. Para ApplicationStackNa me, usa el glue-code pipeline-appnombre rellenado previamente. Este es el nombre de la CloudFormation pila que crea la canalización. 6. Para ello BucketName, usa el nombre del bucket	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	aws-glue-artifacts-us-east-1 rellenado previamente. Este es el nombre del bucket de Amazon S3 que contiene el archivo .zip y que la canalización utiliza para almacenar artefactos de código. 7. Para CodeZipFile, utilice el valor code.zip rellenado previamente. Este es el nombre de la clave del objeto de Amazon S3 del código de ejemplo. El objeto debe ser un archivo .zip. 8. Para TestReportGroupName, utilice el nombre rellenado previamente glue-unittest-report. Es el nombre del grupo de informes de CodeBuild pruebas que se creó para almacenar los informes de las pruebas unitarias. 9. Seleccione Next (Siguiente) y, a continuación, vuelva a seleccionar Next (Siguiente) en la página Configure stack options (Configurar opciones de pila). 10. En la página de revisión, en Capacidades, elija la opción Reconozco que	

Tarea	Descripción	Habilidades requeridas
	CloudFormation podría crear recursos de IAM con nombres personalizados. 11. Elija Submit (Enviar). Una vez finalizada la creación de la pila, podrá ver los recursos creados en la pestaña Resources (Recursos). Las pilas tardan aproximadamente entre 5 y 7 minutos en crearse. La pila crea una CodePipeline vista con Amazon S3 como fuente. En los pasos anteriores, la canalización es aws-glue-unit-test-pipeline.	

Ejecute las pruebas unitarias

Tarea	Descripción	Habilidades requeridas
Ejecute las pruebas unitarias en la canalización.	1. Para probar la canalización implementada, inicie sesión en la CodePipeline consola y Consola de administración de AWS, a continuación, ábrala. 2. Selecciona la canalización creada por la CloudFormation pila y, a continuación, selecciona Release change. La canalización comienza a ponerse en marcha (utilizan	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	do el código más reciente del bucket de Amazon S3). 3. Una vez finalizada la etapa de Test_and_build, seleccione la pestaña Details (Detalles) y, a continuación, examine los registros. 4. Seleccione la pestaña Reports (Informes) y, a continuación, elija el informe de prueba en el Report history (Historial de informes) para ver los resultados de las pruebas unitarias. 5. Una vez finalizada la fase de despliegue, ejecute y supervise el AWS Glue trabajo desplegado en la AWS Glue consola. Para obtener más informaci ón, consulte Supervisión AWS Glue en la AWS Glue documentación.	

Limpia todos los AWS recursos

Tarea	Descripción	Habilidades requeridas
Limpie los recursos del entorno.	Para evitar costos de infraestr uctura adicionales, asegúrese de eliminar la pila después de experimentar con los ejemplos	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	que se proporcionan en este patrón. 1. Abre la CloudFormation consola y, a continuación, selecciona la pila que has creado. 2. Elija Eliminar. De este modo, se eliminan todos los recursos que creó tu pila, incluidos los roles AWS Identity and Access Management (de IAM), las políticas de IAM y los proyectos. CodeBuild	

Resolución de problemas

Problema	Solución
El rol CodePipeline de servicio no puede acceder al bucket de Amazon S3.	• Para la política asociada a su función de CodePipeline servicio, `s3:ListBucket` añádala a la lista de acciones de su política. Para obtener instrucciones sobre cómo ver la política de roles de servicio, consulte View the pipeline ARN and service role ARN (console). Edita la declaración de política de tu función de servicio tal y como se detalla en Añadir permisos a la función CodePipeline de servicio. • En el caso de la política basada en recursos que se adjunta al depósito de artefactos de Amazon S3 de su canalización, también denominada política de cubos de artefacto

Problema	Solución
	s, añada una declaración que permita al rol de CodePipeline servicio utilizar el permiso. `s3:ListBucket`
CodePipeline devuelve un error que indica que el bucket de Amazon S3 no está versionado.	CodePipeline requiere que el bucket Amazon S3 de origen esté versionado. Habilite el control de versiones en el bucket de origen de Amazon S3 Para obtener instrucciones, consulte Habilitar el control de versiones en buckets.

Recursos relacionados

- AWS Glue
- Desarrollar y probar AWS Glue trabajos a nivel local
- AWS CloudFormation para AWS Glue

Información adicional

Además, puede implementar las AWS CloudFormation plantillas mediante AWS Command Line Interface (AWS CLI). Para obtener más información, consulte Implementación rápida de plantillas con transformaciones en la CloudFormation documentación.

Configure una CI/CD canalización mediante AWS CodePipeline y AWS CDK

Konstantin Zarudaev, Yasha Dabas, Lars Kinder y Cizer Pereira en Amazon Web Services

Inicio

Automatizar el proceso de creación y lanzamiento de software mediante una integración y una entrega continuas (CI/CD) supports repeatable builds and rapid delivery of new features to your users. You can quickly and easily test each code change, and you can catch and fix bugs before releasing your software. By running each change through your staging and release process, you can verify the quality of your application or infrastructure code. CI/CDimplica una cultura, un conjunto de principios operativos y un conjunto de prácticas que ayudan a los equipos de desarrollo de aplicaciones a realizar cambios de código con mayor frecuencia y fiabilidad). Esta implementación también se conoce como proceso de CI/CD.

Este patrón define una canalización reutilizable de integración continua y entrega continua (CI/CD) en Amazon Web Services (AWS) con un repositorio de AWS CodeCommit . La CodePipeline canalización de AWS se ha escrito con el AWS Cloud Development Kit (AWS CDK) v2.

Con CodePipeline él, puede modelar las diferentes etapas del proceso de lanzamiento de software a través de la interfaz de la consola de administración de AWS, la interfaz de línea de comandos de AWS (AWS CLI), CloudFormation AWS o AWS SDKs. Este patrón demuestra la implementación CodePipeline y sus componentes mediante AWS CDK. Además de crear bibliotecas, AWS CDK incluye un kit de herramientas (el comando de CLI `cdk`). Es la herramienta principal para interactuar con la aplicación de AWS CDK. Entre otras funciones, el kit de herramientas ofrece la posibilidad de convertir una o más pilas en CloudFormation plantillas e implementarlas en una cuenta de AWS.

El proceso incluye pruebas para validar la seguridad de sus bibliotecas de terceros, y ayuda a garantizar una publicación rápida y automatizada en los entornos especificados. Puede aumentar la seguridad general de sus aplicaciones sometiéndolas a un proceso de validación.

El objetivo de este patrón es acelerar el uso de las CI/CD canalizaciones para implementar el código y, al mismo tiempo, garantizar que los recursos que se implementen se ajusten a DevOps las mejores prácticas. Tras implementar el código de ejemplo, dispondrá de un AWS CodePipeline con procesos de linting, pruebas, controles de seguridad y procesos de implementación y posteriores a la implementación. Este patrón también incluye pasos para Makefile. Con un Makefile, los desarrolladores pueden reproducir los CI/CD pasos de forma local y aumentar la velocidad del proceso de desarrollo.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una comprensión básica de lo siguiente:
  - AWS CDK
  - AWS CloudFormation
  - AWS CodePipeline
  - TypeScript

Limitaciones

Este patrón utiliza AWS CDK TypeScript únicamente para. No abarca otros lenguajes compatibles con AWS CDK.

Versiones de producto

Utilice las últimas versiones de las herramientas siguientes:

- Interfaz de la línea de comandos de AWS (AWS CLI)
- cfn_nag
- git-remote-codecommit
- Node.js

Arquitectura

Pila de tecnología de destino

- AWS CDK
- AWS CloudFormation
- AWS CodeCommit
- AWS CodePipeline

Arquitectura de destino

La canalización se desencadena por un cambio en el CodeCommit repositorio de AWS (`SampleRepository`). Al principio, CodePipeline crea artefactos, se actualiza automáticamente e inicia el proceso de implementación. El proceso resultante implementa una solución en tres entornos independientes:

- Desarrollo: verificación del código en tres pasos en el entorno de desarrollo activo
- Prueba: entorno de pruebas de integración y regresión
- Prod: entorno de producción

Los tres pasos incluidos en la etapa de desarrollo son el linting, la seguridad y las pruebas unitarias. Estos pasos se ejecutan en paralelo para acelerar el proceso. Para garantizar que el proceso solo proporcione artefactos funcionales, dejará de funcionar cada vez que falle un paso del proceso. Tras la implementación en la fase de desarrollo, el proceso ejecuta pruebas de validación para verificar los resultados. En caso de éxito, el proceso implementará los artefactos en el entorno de prueba, que contiene la validación posterior a la implementación. El paso final consiste en implementar los artefactos en el entorno de producción.

El siguiente diagrama muestra el flujo de trabajo desde el CodeCommit repositorio hasta los procesos de creación y actualización que se llevan a cabo en el entorno de desarrollo, así como el despliegue y la validación posteriores en cada uno de los tres entornos. CodePipeline

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS. En este patrón, CloudFormation las plantillas se pueden utilizar para crear un CodeCommit repositorio y una canalización de CodePipeline CI/CD.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.

- AWS CodePipeline es un CI/CD servicio que le ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.
- La Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de la línea de comandos.

Otras herramientas

- cfn_nag es una herramienta de código abierto que busca patrones en las CloudFormation plantillas para identificar posibles problemas de seguridad.
- git-remote-codecommites una utilidad para insertar y extraer código de los CodeCommit repositorios mediante la extensión de Git.
- Node.js es un entorno de JavaScript ejecución basado en eventos diseñado para crear aplicaciones de red escalables.

Código

El código de este patrón está disponible en el repositorio GitHub AWS CodePipeline CI/CD with practices.

Prácticas recomendadas

Revise los recursos, como las políticas de AWS Identity and Access Management (IAM), para asegurarse de que se ajusten a las prácticas recomendadas de su organización.

Epics

Instalar herramientas

Tarea	Descripción	Habilidades requeridas
Instalar herramientas en macOS o Linux.	Si usa macOS o Linux, puede instalar las herramien tas ejecutando el siguiente comando en su terminal preferido o usando Homebrew para Linux.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	`brew install`
	`brew install git-remote-codecommit`
	`brew install ruby brew-gem`
	`brew-gem install cfn-nag`	

Configure AWS CLI.	Para configurar la CLI de AWS, consulte las instrucciones del sistema operativo: • Windows: pasos de configuración para las conexiones HTTPS a los CodeCommit repositorios de AWS en Windows con el asistente de credenciales de la CLI de AWS • Linux, macOS y Unix: pasos de configuración para las conexiones HTTPS a los CodeCommit repositorios de AWS en Linux, macOS o Unix con el asistente de credenciales de la CLI de AWS	DevOps ingeniero

Configurar la implementación inicial

Tarea	Descripción	Habilidades requeridas
Descargue o clone el código.	Para obtener el código que utiliza este patrón, realice una de las siguientes acciones:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	• Descarga el código fuente más reciente de las versiones del GitHub repositorio y descomprime el archivo descargado en una carpeta.
	• Clone el proyecto ejecutando el siguiente comando.
	
	`git clone --depth 1 https://github.com/aws-samples/aws-codepipeline-cicd.git`
	
	Elimine el directorio `.git` del repositorio clonado.
	
	`cd ./aws-codepipeline-cicd`
	`rm -rf ./.git`
	
	Más adelante, utilizará un CodeCommit repositorio de AWS recién creado como origen remoto.	

Tarea	Descripción	Habilidades requeridas

Conéctese a la cuenta de AWS.	Puede conectarse mediante un token de seguridad temporal o una autentica ción de zona de aterrizaj e. Para confirmar que está utilizando la cuenta y región de AWS correctas, ejecute los siguientes comandos.
	`AWS_REGION="eu-west-1"`
	`ACCOUNT_NUMBER=$(aws sts get-caller-identit y --query Account -- output text)`
	`echo "${ACCOUN T_NUMBER}"`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Arranque el entorno de .	Para arrancar un entorno AWS CDK, ejecute los siguientes comandos.
	`npm install`
	`npm run cdk bootstrap "aws://${ACCOUNT_NUMBER}/${AWS_REGION}"`
	Tras arrancar correctamente el entorno, debería aparecer el siguiente resultado.
	`# Bootstrapping environment aws://{account}/{region}...`
	`# Environment aws://{account}/{region} bootstrapped`
	Para más información sobre el proceso de arranque de AWS CDK, consulte la documentación de AWS CDK.
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Sintetice una plantilla.	Para sintetizar una aplicación de AWS CDK, ejecute el comando `cdk synth`.
	`npm run cdk synth`
	Debería ver la siguiente salida.
	`Successfully synthesized to <path-to-directory>/aws-codepipeline-cicd/cdk.out`
	`Supply a stack id (CodePipeline, Dev-MainStack) to display its template.`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Despliega la CodePipeline pila.	Ahora que ha iniciado y sintetizado la CloudFormation plantilla, puede desplegarla. La implementación creará la CodePipeline canalización y un CodeCommit repositor io, que serán la fuente y el desencadenante de la canalización.
	`npm run cdk -- deploy CodePipeline --require-approval never`
	Tras ejecutar el comando, debería ver una implement ación correcta de la CodePipel ine pila y la información de salida. `CodePipel ine.RepositoryName` Le da el nombre del CodeCommit repositorio de la cuenta de AWS.
	`CodePipeline: deploying ... CodePipeline: creating CloudFormation changeset... # CodePipeline Outputs: CodePipeline.R epositoryName = SampleRepository Stack ARN: arn:aws:cloudformation :REGION:ACCOUNT-ID`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`:stack/CodePipeline/STACK-ID`	

Tarea	Descripción	Habilidades requeridas

Configure el CodeCommit repositorio y la sucursal remotos.	Tras una implementación correcta, CodePipeline iniciará la primera ejecución de la canalización, que puede encontrar en la CodePipeline consola de AWS. Como AWS CDK y CodeCommit no inician una rama predeterminada, esta canalización inicial fallará y devolverá el siguiente mensaje de error.
	`The action failed because no branch named main was found in the selected AWS CodeCommit repository SampleRepository. Make sure you are using the correct branch name, and then try again. Error: null`
	Para corregir este error, configure un origen remoto como `SampleRepository` y cree la ramificación `main` requerida.
	`RepoName=$(aws cloudformation describe-stacks --stack-name CodePipeline --query "Stacks[0].Outputs[?OutputKey=='RepositoryName'].OutputValue" --output text)`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	`echo "${RepoName}"`
	`#`
	`git init`
	`git branch -m master main`
	`git remote add origin codecommit://${RepoName}`
	`git add .`
	`git commit -m "Initial commit"`
	`git push -u origin main`	

Pruebe la CodePipeline canalización desplegada

Tarea	Descripción	Habilidades requeridas
Realice un cambio para activar el proceso.	Tras una implementación inicial satisfactoria, deberías disponer de una CI/CD canalización completa con una `main` rama `SampleRepository` como rama de origen. En cuanto realice los cambios en la ramificación `main`, se iniciará el proceso y se ejecutará la siguiente secuencia de acciones: 1. Obtén tu código del CodeCommit repositorio. 2. Compila el código. 3. Actualiza el proceso (`UpdatePipeline`).	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	4. Ejecuta tres trabajos paralelos para comprobar el linting, la seguridad y las pruebas unitarias. 5. En caso de éxito, el proceso implementará la pila `Main` de `./lib/main-stack.ts` en el entorno de desarrollo. 6. Realice una comprobación de los recursos tras la implementación. Puedes seguir todos los CodePipeline pasos y resultados en la CodePipeline consola. 7. En caso de éxito, el proceso repetirá la implementación y la validación en los entornos de prueba y producción.	

Realice pruebas locales mediante Makefile

Tarea	Descripción	Habilidades requeridas
Ejecute el proceso de desarrollo mediante Makefile.	Puede ejecutar todo el proceso de forma local mediante el comando `make`, o bien ejecutar un paso individual (por ejemplo, `make linting`).	Desarrollador de aplicaciones, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Para probar el uso de `make`, realice las siguientes acciones: • Implemente el proceso local: `make` • Ejecute solo pruebas unitarias: `make unittest` • Implemente en la cuenta actual: `make deploy` • Limpie el entorno: `make clean`	

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Elimine los recursos de la aplicación AWS CDK.	Para limpiar su aplicación AWS CDK, ejecute el siguiente comando. `cdk destroy --all` Tenga en cuenta que los buckets de Amazon Simple Storage Service (Amazon S3) creados durante el arranque no se eliminan automáticamente. Necesitará una política de retención que permita su eliminación, o bien tendrá que eliminarlos manualmente en su cuenta de AWS.	DevOps ingeniero

Resolución de problemas

Problema	Solución
La plantilla no funciona como se esperaba.	Si algo sale mal y la plantilla no funciona, asegúrese de que dispone de lo siguiente: • Las versiones adecuadas de las herramien tas. • Acceso a la cuenta de AWS de destino (conectividad de red). • Permisos suficientes para la cuenta de AWS de destino.

Recursos relacionados

- Introducción a las tareas habituales en IAM Identity Center
- CodePipeline Documentación de AWS
- AWS CDK

Configuración del registro centralizado a escala empresarial mediante Terraform

Aarti Rajput, Yashwant Patel y Nishtha Yadav, Amazon Web Services

Resumen

El registro centralizado es vital para la infraestructura en la nube de una organización porque proporciona visibilidad de sus operaciones, seguridad y cumplimiento normativo. A medida que su organización amplía su AWS entorno a varias cuentas, una estrategia estructurada de administración de registros se vuelve fundamental para ejecutar las operaciones de seguridad, cumplir con los requisitos de auditoría y lograr la excelencia operativa.

Este patrón proporciona un marco seguro y escalable para centralizar los registros de múltiples servicios Cuentas de AWS y, de este modo, posibilitar la administración de registros a escala empresarial en despliegues complejos. AWS La solución se automatiza mediante Terraform, que es una herramienta de infraestructura como código (IaC) HashiCorp que garantiza despliegues consistentes y repetibles, y minimiza la configuración manual. Al combinar Amazon CloudWatch Logs, Amazon Data Firehose y Amazon Simple Storage Service (Amazon S3), puede implementar un proceso sólido de agregación y análisis de registros que ofrece:

- Administración centralizada de registros en toda su organización en AWS Organizations
- Recopilación de registros automatizada con controles de seguridad integrados
- Procesamiento de registros escalable y almacenamiento duradero
- Generación de informes de cumplimiento y registros de auditoría simplificados
- Supervisión e información operativa en tiempo real

La solución recopila registros de los AWS Lambda contenedores de Amazon Elastic Kubernetes Service (Amazon EKS), las funciones y las instancias de bases de datos de Amazon Relational Database Service (Amazon RDS) mediante Logs. CloudWatch Reenvía automáticamente estos registros a una cuenta de registro dedicada mediante filtros de suscripción. CloudWatch Firehose administra el flujo de registro de alto rendimiento a Amazon S3 para un almacenamiento a largo plazo. Amazon Simple Queue Service (Amazon SQS) está configurado para recibir notificaciones de eventos de Amazon S3 al crear el objeto. Esto permite la integración con los servicios de análisis, tales como:

- Amazon OpenSearch Service para búsqueda de registros, visualización y análisis en tiempo real

- Amazon Athena para consultas basadas en SQL
- Amazon EMR para procesamiento a gran escala
- Lambda para una transformación personalizada
- Amazon Quick Sight para paneles

Todos los datos se cifran mediante AWS Key Management Service (AWS KMS) y toda la infraestructura se implementa mediante Terraform para lograr una configuración uniforme en todos los entornos.

Este enfoque de registro centralizado permite a las organizaciones mejorar su postura de seguridad, mantener los requisitos de cumplimiento y optimizar la eficiencia operativa en toda su AWS infraestructura.

Requisitos previos y limitaciones

Requisitos previos

- Una zona de aterrizaje para su organización que se crea mediante AWS Control Tower
- Generador de cuentas para Terraform (AFT), implementado y configurado con las cuentas requeridas
- Terraform para aprovisionar la infraestructura
- AWS Identity and Access Management Funciones y políticas (IAM) para el acceso entre cuentas

Para obtener instrucciones sobre cómo configurar AWS Control Tower las cuentas AFT y de aplicación, consulta la sección Epics.

Cuentas obligatorias

Su organización AWS Organizations debe incluir estas cuentas:

- Cuenta de aplicación: una o más cuentas de origen en las que Servicios de AWS (Amazon EKS, Lambda y Amazon RDS) ejecutan y generan registros
- Cuenta de archivo de registro: una cuenta dedicada para el almacenamiento y la administración centralizados de registros

Versiones de producto

- AWS Control Tower versión 3.1 o posterior
- La versión 0.15.0 o posterior de Terraform

Arquitectura

El siguiente diagrama ilustra una arquitectura de registro AWS centralizada que proporciona una solución escalable para recopilar, procesar y almacenar los registros de varias cuentas de aplicaciones en una cuenta dedicada de Log Archive. Esta arquitectura gestiona de forma eficiente los registros de Servicios de AWS Amazon RDS, Amazon EKS y Lambda, y los enruta mediante un proceso simplificado a los buckets regionales de S3 de la cuenta de Log Archive.

El flujo de trabajo incluye cinco procesos:

1. Proceso del flujo de registros
   - El proceso de flujo de registros comienza en las cuentas de la aplicación, donde se Servicios de AWS generan varios tipos de registros, como registros generales, de errores, de auditoría, registros de consultas lentas de Amazon RDS, registros del plano de control de Amazon EKS y registros de ejecución de funciones y errores de Lambda.
   - CloudWatch sirve como punto de recopilación inicial. Recopila estos registros por grupo de registros dentro de cada cuenta de aplicación.
   - En CloudWatch, los filtros de suscripción determinan qué registros deben reenviarse a la cuenta central. Estos filtros le proporcionan un control pormenorizado del reenvío de los registros, de modo que puede especificar los patrones de registro exactos o flujos de registro completos para centralizarlos.
2. Transferencia de registros entre cuentas
   - Los registros se mueven a la cuenta de Log Archive. CloudWatch Los filtros de suscripción facilitan la transferencia entre cuentas y preservan el contexto regional.
   - La arquitectura establece varios flujos paralelos para gestionar diferentes orígenes de registro de manera eficiente, a fin de garantizar un rendimiento y una escalabilidad óptimos.
3. Procesamiento de registros en la cuenta de archivo de registros
   - En la cuenta de archivo de registros, Firehose procesa los flujos de registro entrantes.
   - Cada región mantiene flujos de entrega de Firehose dedicados que pueden transformar, convertir o enriquecer los registros según sea necesario.

- Estos flujos de Firehose envían los registros procesados a los buckets de S3 de la cuenta de archivo de registros, que se encuentra en la misma región que las cuentas de la aplicación de origen (región A en el diagrama) para mantener los requisitos de soberanía de datos.

4. Notificaciones y flujos de trabajo adicionales
   - Cuando los registros llegan a sus buckets de S3 de destino, la arquitectura implementa un sistema de notificaciones mediante Amazon SQS.
   - Las colas de SQS regionales permiten el procesamiento asíncrono y pueden activar flujos de trabajo, análisis o sistemas de alertas adicionales según los registros almacenados.
5. AWS KMS por seguridad

   La arquitectura incorpora medidas AWS KMS de seguridad. AWS KMS proporciona claves de cifrado para los cubos S3. Esto garantiza que todos los registros almacenados mantengan el cifrado en reposo y, al mismo tiempo, que el cifrado sea regional para cumplir con los requisitos de residencia de datos.

Tools (Herramientas)

Servicios de AWS

- Amazon CloudWatch es un servicio de monitoreo y observabilidad que recopila datos operativos y de monitoreo en forma de registros, métricas y eventos. Proporciona una vista unificada de AWS los recursos, las aplicaciones y los servicios que se ejecutan en AWS y en los servidores locales.
- CloudWatch Los filtros de suscripción a los registros son expresiones que coinciden con un patrón en los eventos de registro entrantes y envían los eventos de registro coincidentes al AWS recurso especificado para su posterior procesamiento o análisis.
- AWS Control Tower Account Factory For Terraform (AFT) establece una canalización de Terraform para ayudarlo a aprovisionar y personalizar las cuentas. AWS Control Tower AFT proporciona un aprovisionamiento de cuentas basado en Terraform y, al mismo tiempo, le permite administrar sus cuentas con. AWS Control Tower
- Amazon Data Firehose ofrece datos de streaming en tiempo real a destinos como Amazon S3, Amazon Redshift y Amazon Service. OpenSearch Se escala automáticamente para adaptarse al rendimiento de los datos y no es necesaria ninguna administración continua.
- Amazon Elastic Kubernetes Service (Amazon EKS) es un servicio administrado de orquestación de contenedores que facilita la implementación, administración y escalado de aplicaciones

en contenedores con Kubernetes. Administra de manera automática la disponibilidad y la escalabilidad de los nodos del plano de control de Kubernetes.

- AWS Key Management Service (AWS KMS) crea y controla las claves de cifrado para cifrar sus datos. AWS KMS se integra con otros Servicios de AWS para ayudarle a proteger los datos que almacena con estos servicios.
- AWS Lambda es un servicio informático sin servidor que permite ejecutar código sin aprovisionar ni administrar servidores. Escala de manera automática las aplicaciones mediante la ejecución de código en respuesta a cada desencadenador y solo cobra por el tiempo de procesamiento que se utilice.
- Amazon Relational Database Service (Amazon RDS) es un servicio administrado de base de datos relaciona que facilita la configuración, la operación y la escala de una base de datos relacional en la nube. Proporciona una capacidad rentable y redimensionable, además de que automatiza las tareas de administración que consumen mucho tiempo.
- Amazon Simple Queue Service (Amazon SQS) es un servicio de colas de mensajes que le permite desacoplar y escalar microservicios, sistemas distribuidos y aplicaciones sin servidor. Elimina la complejidad de administrar y operar el middleware orientado a los mensajes.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento. Puede almacenar y recuperar cualquier cantidad de datos desde cualquier parte de la web.

Otras herramientas

- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.

Código

El código de este patrón está disponible en el repositorio de registro GitHub centralizado.

Prácticas recomendadas

- Utilice varios Cuentas de AWS en una sola organización en AWS Organizations. Esta práctica permite una administración centralizada y un registro estandarizado en las cuentas.
- Configure los buckets de S3 con el control de versiones, las políticas de ciclo de vida y la replicación entre regiones. Implemente el cifrado y el registro de acceso para garantizar la seguridad y el cumplimiento.

- Implemente estándares de registro comunes mediante el formato JSON con marcas de tiempo y campos estándares. Utilice una estructura de prefijos y una correlación coherentes IDs para facilitar el seguimiento y el análisis.
- Habilite los controles de seguridad con AWS KMS cifrado y acceso con privilegios mínimos. Mantenga la AWS CloudTrail supervisión y la rotación regular de las claves para mejorar la seguridad.
- Configure CloudWatch métricas y alertas para el seguimiento de las entregas. Supervise los costos y el rendimiento con notificaciones automáticas.
- Configure las políticas de retención de Amazon S3 para satisfacer los requisitos de cumplimiento y habilite el registro de acceso al servidor de Amazon S3 para hacer un seguimiento de las solicitudes hechas a los buckets de S3. Conserve la documentación sobre las políticas de los buckets de S3 y las reglas del ciclo de vida. Haga revisiones periódicas de los registros de acceso, los permisos de los buckets y las configuraciones de almacenamiento para garantizar el cumplimiento y las prácticas recomendadas de seguridad.

Epics

Configure cuentas AWS Control Tower de AFT y de aplicación

Tarea	Descripción	Habilidades requeridas
Configure un AWS Control Tower entorno con AFT.	1. Implemente AWS Control Tower siguiendo las instrucciones de la AWS Control Tower documentación. 2. Implemente AFT y siga las instrucciones de la documentación de AWS Control Tower.	Administrador de AWS
Habilite el uso compartido de recursos para la organización.	1. Configure AWS Command Line Interface (AWS CLI) con las credenciales de la cuenta de administr ación, que proporcionan	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	permisos administrativos para administrar AWS Control Tower. 2. Ejecute el siguiente AWS CLI comando en cualquier lugar Región de AWS: `aws ram enable-sharing-with-aws-organization` Esto permite compartir recursos dentro de su organización en AWS Organizations todas las regiones que admiten AWS Resource Access Manager (AWS RAM).	
Verifique o aprovisione las cuentas de la aplicación.	Para aprovisionar cuentas nuevas de aplicación para su caso de uso, créelas mediante AFT. Para obtener más información, consulte Aprovisionar una nueva cuenta con AFT en la AWS Control Tower documentación.	Administrador de AWS

Configuración de archivos de configuración para cuentas de la aplicación

Tarea	Descripción	Habilidades requeridas
Copie el contenido de la carpeta `Application_account` al repositor	1. Cree una carpeta con el nombre `Application_account` en la	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
io `aft-account-customizations` .	ruta raíz del repositorio `aft-account-customizations` . Este repositorio se crea de manera automática al configurar AFT (consulte el apartado anterior). 2. Navegue hasta el directorio raíz del scale-using-terraform repositorio, copie el contenido del `aft/account` directorio y péguelo en el `Application_account` directorio que creó en el paso 1 del `aft-account-customizations` repositorio. centralised-logging-at-enterprise 3. Desde el directorio raíz del repositorio `centralised-logging-at-enterprise-scale-using-terraform` , copie el contenido del directorio `Application_account` en el directorio `Application_account/terraform` del repositorio `aft-account-customizations` . 4. En el archivo `aft-account-customizations/Application_accoun`	

Tarea	Descripción	Habilidades requeridas
	`t/terraform.tfvars`, confirme que todos los parámetros se pasan como argumentos en los archivos de configuración de Terraform correspon dientes.	

Tarea	Descripción	Habilidades requeridas
Revise y edite los parámetros de entrada para configurar la cuenta de la aplicación.	En este paso, debe configurar el archivo de configuración para crear recursos en las cuentas de la aplicación, incluidos los grupos de CloudWatch registros, los filtros de CloudWatch suscripción, las funciones y políticas de IAM y los detalles de configuración de las funciones de Amazon RDS, Amazon EKS y Lambda. En el repositorio `aft-account-customizations`, en la carpeta `Application_account`, configure los parámetros de entrada del archivo `terraform.tfvars` según los requisitos de su organización: • `environment`: nombre del entorno (por ejemplo, `prod`, `dev`, `staging`) en el que se implementarán los recursos. • `account_name`: el nombre del Cuenta de AWS lugar donde se crearán los recursos. • `log_archive_account_id`: el Cuenta de AWS ID en el que se archivarán los registros.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• `admin_role_name` : nombre del rol administrativo que se utilizará para administrar los recursos. • `tags`: mapa de pares clave-valor que representan etiquetas comunes que se aplican a todos los recursos. • `rds_config` : objeto que contiene los detalles de configuración de las instancias de Amazon RDS. • `allowed_cidr_blocks` : lista de bloques de CIDR a los que se les permite acceder a los recursos. • `destination_name:` Variable que se utiliza para crear el nombre de recurso de Amazon (ARN) del CloudWatch destino al que se van a transmitir los registros. • `rds_parameters:` : objeto que contiene la configuración del grupo de parámetros de Amazon RDS. • `vpc_config` : objeto que contiene los detalles de configuración de VPC.	

Tarea	Descripción	Habilidades requeridas
	• `eks_config` : objeto que contiene los detalles de configuración de los clústeres de Amazon RDS. • `lambda_config` : objeto que contiene los detalles de configuración de las funciones de Lambda. • `restrictive_cidr_range` : lista de rangos de CIDR restrictivos para las reglas de los grupos de seguridad. • `target_account_id` : el Cuenta de AWS ID de la cuenta de Log Archive de destino en la que se desplegarán los recursos.	

Definición de los archivos de configuración para la cuenta de archivo de registros

Tarea	Descripción	Habilidades requeridas
Copie el contenido de la carpeta `Log_archive_account` al repositorio `aft-account-customizations` .	1. Cree una carpeta nombrada `Log_archive_account` en la ruta raíz del repositorio `aft-account-customizations` . Este repositorio se crea automáticamente al configurar AFT. 2. Vaya al directorio raíz del repositorio `centralis`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`ed-logging-at-ente rprise-scale-using -terraform`, copie el contenido del directorio `aft/account` y péguelo en el directorio `Log_archi ve_account` que creó en el paso anterior del repositorio `aft-accou nt-customizations`. 3. Desde el directorio raíz del repositorio `centralis ed-logging-at- enterprise-scale- using-terraform`, copie el contenido del directorio `Log_archi ve_account` en el directorio `Log_archi ve_account/terrafo rm` del repositorio `aft- account-custom izations`. 4. En el archivo `aft-accou nt-customizations/ Log_archive_accoun t/terraform.tfvars`, confirme que todos los parámetros se pasan como argumentos en los archivos de configuración de Terraform correspon dientes.	

Tarea	Descripción	Habilidades requeridas
Revise y edite los parámetros de entrada para configurar la cuenta de archivo de registros.	En este paso, definirá el archivo de configuración para crear recursos en la cuenta de archivo de registros, tales como los flujos de entrega de Firehose, los buckets de S3, las colas de SQS y los roles y políticas de IAM. En la carpeta `Log_archive_account` del repositorio `aft-account-customizations`, configure los parámetros de entrada del archivo `terraform.tfvars` según los requisitos de su organización: • `environment`: nombre del entorno (por ejemplo, `prod`, `dev`, `staging`) en el que se implementarán los recursos. • `destination_name`: variable que se utiliza para crear el ARN del CloudWatch destino al que se transmitirán los registros. • `source_account_ids`: una lista de las Cuenta de AWS IDs que pueden colocar filtros de suscripción en el destino del registro. Puede introducir tantas cuentas IDs como desee	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	para habilitar el registro centralizado.	

Ejecución de los comandos de Terraform para aprovisionar recursos

Tarea	Descripción	Habilidades requeridas

Opción 1: implemente los archivos de configuración de Terraform desde AFT.	En AFT, la canalización de AFT se activa después de introducir el código con los cambios de configuración en el GitHub `aft-account-customizations` repositorio. AFT detecta de manera automática los cambios e inicia el proceso de personalización de la cuenta.
	
	Después de hacer cambios en los archivos de Terraform (`terraform.tfvars`), confirme y envíe los cambios al repositorio `aft-account-customizations` :
	
	`$ git add *`
	`$ git commit -m "update message"`
	`$ git push origin main`
	
	Note
	Si utiliza una rama distinta (por ejemplo `dev`), sustituya `main`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	por el nombre de la rama.	

Tarea	Descripción	Habilidades requeridas

Opción 2: implemente el archivo de configuración de Terraform de manera manual.	Si no utiliza AFT o quiere implementar la solución de manera manual, puede utilizar los comandos siguientes de Terraform de las carpetas `Application_account` y `Log_archive_account`:
	1. Clone el GitHub repositorio y configure los parámetros de entrada en el `terraform.tfvars` archivo.
	2. Use el siguiente comando:
	`$ terraform init`
	3. Previsualice los cambios:
	`$ terraform plan`
	Este comando evalúa la configuración de Terraform para determinar el estado deseado de los recursos y lo compara con el estado actual de la infraestructura.
	4. Aplicación de cambios:
	`$ terraform apply`
	5. Revise los cambios planificados y escriba sí cuando se le solicite para continuar con la aplicación.
		DevOps ingeniero

Valide los recursos

Tarea	Descripción	Habilidades requeridas
Verifique los filtros de suscripción.	Para verificar que los filtros de suscripción reenvían correctamente los registros de los grupos de registros de cuentas de la aplicación a la cuenta de archivo de registros, haga lo siguiente: 1. En la cuenta de la aplicación, abra la CloudWatch consola. 2. En el panel de navegación izquierdo, elija Registros, Grupos de registros. 3. Seleccione cada grupo de registros (`/aws/rds`, `/aws/eks`, `/aws/lambda`) y elija la pestaña Filtros de suscripción. Debe ver los filtros de suscripción activos que apuntan al ARN de destino, según el nombre que especificó en el archivo de configuración de Terraform. 4. Elija cualquier filtro de suscripción para verificar su configuración y estado.	DevOps ingeniero
Verifique los flujos de Firehose.	Para verificar que los flujos de Firehose en la cuenta de archivo de registros procesan	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	los registros de la aplicación correctamente, haga lo siguiente: 1. En la cuenta de archivo de registros, abra la consola de Firehose. 2. En el panel de navegación izquierdo, elija Flujos de Firehose. 3. Elija cualquier flujo de Firehose y verifique lo siguiente: • El destino muestra el bucket de S3 correcto. • La pestaña Supervisión muestra las métricas de entrega correcta. • La marca de tiempo de entrega reciente es actual.	

Tarea	Descripción	Habilidades requeridas
Valide los buckets de S3 centralizados.	Para verificar que los buckets de S3 centralizados reciben y organizan los registros correctamente, haga lo siguiente: 1. En la cuenta de archivo de registros, abra la consola de Amazon S3. 2. Seleccione cada bucket de registro central. 3. Navegue por la estructura de carpetas: AWSLogs/AccountID/Region/Service. Deberías ver los archivos de registro organizados por timestamp () YYYY/MM/DD/HH. 4. Elija cualquier archivo de registro reciente y verifique su formato y la integridad de los datos.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Valide las colas de SQS.	Para verificar que las colas de SQS reciben notificaciones de archivos de registro nuevos, haga lo siguiente: 1. En la cuenta de archivo de registros, abra la consola de Amazon SQS. 2. En el panel de navegació n izquierdo, elija Queues (Colas). 3. Seleccione cada cola configurada y elija Enviar y recibir mensajes. Debe ver los mensajes que contienen notificaciones de eventos de S3 de los nuevos archivos de registro. 4. Elija cualquier mensaje para verificar que contiene la información correcta del objeto de S3.	DevOps ingeniero

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Opción 1: retire los archivos de configuración de Terraform desde AFT.	Al eliminar los archivos de configuración de Terraform e introducir los cambios, AFT inicia de manera automática el proceso de eliminación de recursos.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	1. Vaya al repositorio de `aft-account-customizations` .
	2. Vaya al directorio `terraform` .
	3. Elimine los archivos siguientes:
	• Directorio `modules`
	• `iam.tf`
	• `versions.tf`
	• `variables.tf`
	• `outputs.tf`
	• `terraform.tfvars`
	4. Borre el contenido del archivo `main.tf`.
	5. Envíe los cambios al repositorio:
	`# Stage all changes`
	`$ git add *`
	`# Commit cleanup changes`
	`$ git commit -m "Remove AFT customizations"`
	`# Push to repository`
	`$ git push origin main`
	Note
	Si utiliza una rama distinta (por ejemplo	

Tarea	Descripción	Habilidades requeridas
	dev), sustituya `main` por el nombre de la rama.	

Opción 2: limpie los recursos de Terraform de manera manual.	Si no utiliza AFT o quiere limpiar los recursos de manera manual, utilice los comandos siguientes de Terraform de las carpetas `Application_account` y `Log_archive_account`:
	1. Inicialice la configuración de Terraform:
	`$ terraform init`
	Este comando inicializa Terraform y garantiza el acceso al estado actual.
	2. Vista previa de los cambios de limpieza:
	`$ terraform destroy`
	Este comando evalúa qué recursos se destruirán y compara el estado deseado con el estado actual de la infraestructura.
	3. Ejecute la limpieza. Cuando se le solicite, escriba sí para confirmar y ejecutar el plan de destrucción.
		DevOps ingeniero

Resolución de problemas

Problema	Solución
El destino CloudWatch de los registros no se creó o está inactivo.	Valide lo siguiente: 1. En la cuenta de archivo de registros, verifique que la política de destino incluya lo siguiente: • La entidad principal correcta de la cuenta de origen. • La acción correcta (`logs:PutSubscriptionFilter`). • Un ARN de destino válido. 2. Confirme que el flujo de Firehose existe y está activo. 3. Verifique que el rol de IAM asociado al destino tenga permisos para Firehose.
Se produjo un error en el filtro de suscripción o está bloqueado en estado pendiente.	Comprueba lo siguiente: 1. En la cuenta de aplicación, verifique que el rol de IAM tenga lo siguiente: • Permisos para llamar a `PutSubscriptionFilter`. • Una relación de confianza con CloudWatch Logs. 2. Confirme que el ARN de destino es correcto. 3. Compruebe CloudWatch los registros para ver si hay mensajes de error específicos.
El flujo de entrega de Firehose no muestra registros de entrada.	Compruebe lo siguiente: 1. Confirme que el rol de IAM de Firehose tiene lo siguiente: • Permisos para escribir en Amazon S3.

Problema	Solución
	• Acceso a la AWS KMS clave si el cifrado está activado. 2. Revise CloudWatch las métricas de: • `IncomingRecords` • `DeliveryToS3.Records` 3. Verifique la configuración del búfer y la configuración de entrega.

Recursos relacionados

- Terraform infrastructure setup (documentación de Terraform)
- Implemente AWS Control Tower Account Factory para Terraform (AFT) (AWS Control Tower documentación)
- Tutorial de IAM: delegue el acceso mediante el Cuentas de AWS uso de funciones de IAM () IAMdocumentation

Configure el end-to-end cifrado para aplicaciones en Amazon EKS mediante cert-manager y Let's Encrypt

Mahendra Revanasiddappa y Vasanth Jeyaraj, Amazon Web Services

Resumen

La implementación del end-to-end cifrado puede resultar compleja y necesita administrar los certificados de cada activo de su arquitectura de microservicios. Si bien puede finalizar la conexión de Transport Layer Security (TLS) en el extremo de la red de Amazon Web Services (AWS) con un Network Load Balancer o Amazon API Gateway, algunas organizaciones end-to-end requieren el cifrado.

Este patrón utiliza el controlador de entrada NGINX para la entrada. Esto se debe a que cuando se crea una entrada de Kubernetes, el recurso de entrada utiliza un equilibrador de carga de red. El equilibrador de carga de red no permite cargar certificados de cliente. Por lo tanto, no puede lograr el TLS mutuo con el ingreso de Kubernetes.

Este patrón está pensado para las organizaciones que requieren la autenticación mutua entre todos los microservicios de sus aplicaciones. El TLS mutuo reduce la carga que supone mantener los nombres de usuario o las contraseñas y, además, puede utilizar un marco de seguridad listo para usar. El enfoque de este patrón es compatible si su organización tiene una gran cantidad de dispositivos conectados o si debe cumplir con estrictas pautas de seguridad.

Este patrón ayuda a aumentar la postura de seguridad de su organización al implementar el end-to-end cifrado para las aplicaciones que se ejecutan en Amazon Elastic Kubernetes Service (Amazon EKS). Este patrón proporciona una aplicación y un código de muestra en el repositorio de GitHub End-to-end cifrado de Amazon EKS para mostrar cómo se ejecuta un microservicio con el end-to-end cifrado en Amazon EKS. El enfoque del patrón utiliza cert-manager, un complemento de Kubernetes, con Let's Encrypt como autoridad de certificación (CA). Let's Encrypt es una solución rentable para administrar certificados y proporciona certificados gratuitos con una validez de 90 días. Cert-Manager automatiza el aprovisionamiento bajo demanda y la rotación de los certificados cuando se implementa un nuevo microservicio en Amazon EKS.

Destinatarios previstos

Este patrón se recomienda para los usuarios que tengan experiencia con Kubernetes, TLS, Amazon Route 53 y el Sistema de nombres de dominio (DNS).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un clúster existente de Amazon EKS.
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 1.7, instalada y configurada en macOS, Linux o Windows
- La utilidad de línea de comandos `kubectl`, instalada y configurada para acceder al clúster de Amazon EKS. Para obtener más información, consulte Installing kubectl (Instalación de kubectl) en la documentación de Amazon EKS.
- Un nombre DNS existente para probar una aplicación. Para obtener más información, consulte Registrar nombres de dominio mediante Amazon Route 53 en la documentación de Amazon Route 53.
- La última versión de Helm, instalada en su máquina local. Para obtener más información al respecto, consulte Uso de Helm con Amazon EKS en la documentación de Amazon EKS y en el repositorio de GitHub Helm.
- El GitHub End-to-end cifrado del repositorio EKS de Amazon, clonado en su máquina local.
- Sustituya los siguientes valores en los `trustpolicy.json` archivos `policy.json` y del repositorio de GitHub End-to-end cifrado clonado en Amazon EKS:
  - `<account number>`: sustitúyalo por el ID de cuenta de AWS de la cuenta en la que desea implementar la solución.
  - `<zone id>`: sustitúyalo por el ID de zona de Route 53 del nombre de dominio.
  - `<node_group_role>`: sustitúyalo por el nombre de la función de AWS Identity and Access Management del rol de IAM asociada a los nodos de Amazon EKS.
  - `<namespace>`: sustitúyalo por el espacio de nombres de Kubernetes en el que se despliega el controlador de entrada NGINX y la aplicación de ejemplo.
  - `<application-domain-name>`: sustitúyalo por el nombre de dominio DNS de Route 53

Limitaciones

- Este patrón no describe cómo rotar los certificados y solo muestra cómo usar los certificados con microservicios en Amazon EKS.

Arquitectura

En el siguiente diagrama se muestran los componentes de la arquitectura y el flujo de trabajo de esta aplicación.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un cliente envía una solicitud de acceso a la aplicación al nombre DNS.
2. El registro de Route 53 es un CNAME para el equilibrador de carga de red.
3. El equilibrador de carga de red reenvía la solicitud al controlador de entrada NGINX que está configurado con un agente oyente TLS. La comunicación entre el controlador de entrada NGINX y el equilibrador de carga de red sigue el protocolo HTTPS.
4. El controlador de entrada NGINX realiza un enrutamiento basado en rutas en función de la solicitud del cliente al servicio de la aplicación.
5. El servicio de aplicaciones reenvía la solicitud al pod de la aplicación. La aplicación está diseñada para utilizar el mismo certificado al llamar a secretos.
6. Los pods ejecutan la aplicación de ejemplo con los certificados del administrador de certificados. La comunicación entre el controlador de entrada de NGINX y los pods utiliza HTTPS.

Nota: Cert-Manager se ejecuta en su propio espacio de nombres. Utiliza un rol de clúster de Kubernetes para aprovisionar certificados como secretos en espacios de nombres específic os. Puede adjuntar esos espacios de nombres a los pods de aplicaciones y al NGINX Ingress Controller.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Kubernetes Service (Amazon EKS) es un servicio administrado que puede utilizar para ejecutar Kubernetes en AWS sin necesidad de instalar, operar ni mantener su propio plano de control o nodos de Kubernetes.
- Elastic Load Balancing distribuye automáticamente el tráfico entrante entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en una o varias zonas de disponibilidad.

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.

Otras herramientas

- cert-manager es un complemento de Kubernetes que solicita certificados, los distribuye a los contenedores de Kubernetes y automatiza la renovación de los certificados.
- NGINX Ingress Controller es una solución de gestión del tráfico para aplicaciones nativas en la nube en Kubernetes y entornos contenerizados.

Epics

Cree y configure una zona alojada pública con Route 53

Tarea	Descripción	Habilidades requeridas
Cree una zona alojada pública para Route 53.	Inicie sesión en la consola de administración de AWS, abra la consola Amazon Route 53, elija Zonas alojadas y, a continuación, elija Crear zona alojada. Cree una zona alojada pública y registre el ID de la zona. Para obtener más información, consulte Crear una zona alojada pública en la documentación de Amazon Route 53. **Note** ACME DNS01 utiliza el proveedor de DNS para solicitar al administrador	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	de certificados que emita el certifica do. Este desafío le pide que demuestre que controla el DNS de su nombre de dominio poniendo un valor específico en un registro TXT situado debajo de ese nombre de dominio. Cuando Let's Encrypt proporciona un token a su cliente ACME, este crea un registro TXT derivado de ese token y de su clave de cuenta, y coloca ese registro en `_acme-challenge.<YOURDOMAIN>` . Luego, Let's Encrypt consulta el DNS de ese registro. Si encuentra una coincidencia, puede proceder a emitir un certificado.	

Configure un rol de IAM para permitir que el administrador de certificados acceda a la zona alojada pública

Tarea	Descripción	Habilidades requeridas
Cree la política de IAM para cert-manager.	Se requiere una política de IAM para proporcionar a cert-manager permiso para validar que usted es propietario del dominio de Route 53. El `policy.json` ejemplo de política de IAM se proporciona en el `1-IAMRole` directorio del repositorio de GitHub End-to-end cifrado clonado de Amazon EKS. Escriba el siguiente comando en la CLI de AWS para crear la política de IAM: `aws iam create-policy \ --policy-name PolicyForCertManager \ --policy-document file://policy.json`	AWS DevOps
Cree el rol de IAM para cert-manager.	Después de crear la política de IAM, debe crear un rol de IAM. El ejemplo del rol de IAM `trustpolicy.json` se proporciona en el directorio `1-IAMRole` . Escriba el siguiente comando en la CLI de AWS para crear el rol de IAM:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`aws iam create-role \ --role-name RoleForCertManager \ --assume-role-policy-document file://trustpolicy.json`	
Asocie la política de al rol.	Escriba el siguiente comando en la CLI de AWS para adjuntar la política de IAM al rol de IAM: Sustituya `AWS_ACCOUNT_ID` por el ID de la cuenta de AWS. `aws iam attach-role-policy \ --policy-arn arn:aws:iam::AWS_ACCOUNT_ID:policy/PolicyForCertManager \ --role-name RoleForCertManager`	AWS DevOps

Configure el controlador de entrada NGINX en Amazon EKS

Tarea	Descripción	Habilidades requeridas
Implemente el controlador de entrada NGINX.	Instale la versión más reciente de `nginx-ingress` mediante Helm. Puede modificar la configuración `nginx-ingress` según sus requisitos antes de implementarla. Este patrón utiliza un equilibrador de carga de red	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	anotado e interno que está disponible en el directorio `5-Nginx-Ingress-Controller` . Instale el controlador de entrada NGINX ejecutando el siguiente comando Helm desde el directorio `5-Nginx-Ingress-Controller` . `helm install test-nginx nginx-stable/nginx-ingress -f 5-Nginx-Ingress-Controller/values_internal_nlb.yaml`	
Verifique que el controlador de entrada NGINX se encuentre instalado.	Escriba el comando `helm list`. El resultado debería mostrar que el controlador de entrada NGINX está instalado.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Cree un registro A de Route 53.	El registro A apunta al equilibrador de carga de red creado por el controlador de entrada de NGINX. 1. Obtener el nombre del DNS del equilibrador de carga de red. Para más instrucciones, consulte Obtener el nombre del DNS para un equilibrador de carga ELB. 2. En la consola de Amazon Route 53, elija Hosted Zones (Zonas alojadas). 3. Seleccione la zona alojada pública en la que desee crear el registro y, a continuación, elija Crear registro. 4. Ingrese un nombre para el registro. 5. En Tipo de registro, elija A: Dirige el tráfico hacia IPv4 y algunos recursos de AWS. 6. Habilite el Alias. 7. En Enrutar el tráfico a, haga lo siguiente: a. Elija Alias para el equilibrador de carga de red. b. Elija la región de AWS en la que se implementa	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	el equilibrador de carga de red. c. Introduzca el nombre DNS del equilibrador de carga de red. 8. Elija Crear registros.	

Configurar NGINX en VirtualServer Amazon EKS

Tarea	Descripción	Habilidades requeridas
Implemente NGINX. VirtualServer	El VirtualServer recurso NGINX es una configuración de equilibrio de carga que es una alternativa al recurso de entrada. La configuración para crear el VirtualServer recurso NGINX está disponible en el archivo del `nginx_virtualserver.yaml` directorio. `6-Nginx-Virtual-Server` Introduzca el siguiente comando `kubectl` para crear el recurso VirtualServer NGINX. `kubectl apply -f nginx_virtualserver.yaml`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Important Asegúrese de actualizar el nombre de dominio de la aplicación, el secreto del certificado y el nombre del servicio de la aplicación en el archivo `nginx_virtualserver.yaml` .	
Compruebe que se ha creado NGINX VirtualServer .	Introduzca el siguiente comando `kubectl` para comprobar que el VirtualServer recurso NGINX se creó correctamente. `kubectl get virtualserver` **Note** Compruebe que la columna `Host` coincida con el nombre de dominio de su aplicación.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Implemente el servidor web NGINX con TLS habilitado.	Este patrón utiliza un servidor web NGINX con TLS habilitado como aplicación para probar el cifrado. end-to-end Los archivos de configuración necesarios para implementar la aplicación de prueba están disponibles en el directorio `demo-webserver` . Para implementar la aplicación de prueba, ejecute el siguiente comando en `kubectl`: `kubectl apply -f nginx-tls-ap.yaml`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Compruebe que se hayan creado los recursos de la aplicación de prueba.	Introduzca los siguientes comandos en `kubectl` para comprobar que se han creado los recursos necesarios para la aplicación de prueba: • `kubectl get deployments` **Note** Valide la columna `Ready` y la columna `Available` . • `kubectl get pods | grep -i example-deploy` **Note** Los pods deben estar en un estado `running`. • `kubectl get configmap` • `kubectl get svc`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Validación de la solicitud.	1. Introduzca el siguiente comando sustituyendo `<application-domain-name>` por el nombre DNS de Route53 que creó anteriormente. `curl --verbose https://<application-domain-name>` 2. Compruebe que puede acceder a la aplicación.	AWS DevOps

Recursos relacionados

Recursos de AWS

- Creación de registros con la consola de Amazon Route 53 (documentación de Amazon Route 53)
- Uso de un equilibrador de carga de red con el controlador de entrada de NGINX en Amazon EKS en el blog de AWS

Otros recursos

- Route 53 (documentación del administrador de certificados)
- Configuración del proveedor de desafíos DNS01 (documentación sobre el administrador de certificados)
- El desafío Let's Encrypt DNS (documentación de Let's Encrypt)

Simplificación de la implementación de aplicaciones multiusuario de Amazon EKS mediante Flux

Nadeem Rahaman, Aditya Ambati, Aniket Dekate y Shrikant Patil, Amazon Web Services

Resumen

Muchas empresas que ofrecen productos y servicios son sectores regulados por los datos que deben mantener las barreras de datos entre sus funciones empresariales internas. Este patrón describe cómo puede utilizar la característica de varias tenencias de Amazon Elastic Kubernetes Service (Amazon EKS) para crear una plataforma de datos que logre el aislamiento lógico y físico entre los inquilinos o usuarios que comparten un clúster único de Amazon EKS. El patrón proporciona aislamiento a través de los enfoques siguientes:

- Aislamiento del espacio de nombres de Kubernetes
- Control de acceso basado en roles (RBAC)
- Políticas de red
- Cuotas de recursos
- AWS Identity and Access Management Funciones (IAM) para cuentas de servicio (IRSA)

Además, esta solución utiliza Flux para mantener inmutable la configuración del inquilino al implementar aplicaciones. Puede implementar las aplicaciones del inquilino y especificar el repositorio del inquilino que contiene el archivo `kustomization.yaml` de Flux en la configuración.

Este patrón implementa lo siguiente:

- Un AWS CodeCommit repositorio, AWS CodeBuild proyectos y una AWS CodePipeline canalización, que se crean mediante la implementación manual de los scripts de Terraform.
- Componentes de red y cómputo obligatorios para alojar a los inquilinos. Se crean a través de Terraform CodePipeline y CodeBuild utilizando Terraform.
- Espacios de nombres de inquilinos, políticas de red y cuotas de recursos, que se configuran a través de un gráfico de Helm.
- Aplicaciones que pertenecen a diferentes inquilinos, implementadas con Flux.

Le recomendamos que planifique y cree con detenimiento su propia arquitectura para varios inquilinos según sus requisitos únicos y sus consideraciones de seguridad. Este patrón proporciona un punto de partida para la implementación.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- AWS Command Line Interface (AWS CLI) versión 2.11.4 o posterior, instalada y configurada
- La versión 0.12 o posterior de Terraform instalada en su máquina local
- La versión 3.0.0 o posterior del Proveedor de AWS para Terraform
- Versión 2.10 o posterior de Kubernetes Provider
- Versión 2.8.0 o posterior de Helm Provider
- Versión 1.14 o posterior de Kubectl Provider

Limitaciones

- Dependencia de las implementaciones manuales de Terraform: la configuración inicial del flujo de trabajo, que incluye la creación de CodeCommit repositorios, CodeBuild proyectos y CodePipeline canalizaciones, se basa en las implementaciones manuales de Terraform. Esto introduce una posible limitación respecto de automatización y escalabilidad, ya que requiere una intervención manual para hacer cambios en la infraestructura.
- CodeCommit dependencia de los repositorios: el flujo de trabajo se basa en CodeCommit los repositorios como solución de gestión del código fuente y está estrechamente vinculado a ellos. Servicios de AWS

Arquitectura

Arquitecturas de destino

Este patrón implementa tres módulos para crear la infraestructura de canalización, red y computación de una plataforma de datos, como se ilustra en los diagramas siguientes.

Arquitectura de canalización:

Arquitectura de redes:

Arquitectura de computación:

Tools (Herramientas)

Servicios de AWS

- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- AWS CodeCommit es un servicio de control de versiones que permite almacenar y administrar repositorios de Git de forma privada, sin necesidad de administrar su propio sistema de control de origen.
- AWS CodePipeline permite diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software y automatizar los pasos necesarios para lanzar los cambios en el software de manera continua.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar AWS Kubernetes sin necesidad de instalar o mantener su propio plano de control o nodos de Kubernetes.
- AWS Transit Gatewayes un centro central que conecta nubes privadas virtuales () y redes locales. VPCs
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Otras herramientas

- Las políticas de red de Cilium son compatibles con las políticas de red de L3 y L4 de Kubernetes. Se pueden ampliar con políticas de L7 para proporcionar seguridad de las API para HTTP, Kafka y gRPC, y otros protocolos similares.
- Flux es una herramienta de entrega continua (CD) basada en Git que automatiza las implementaciones de aplicaciones en Kubernetes.
- Helm: es un administrador de paquetes de código abierto para Kubernetes que le permite instalar y administrar aplicaciones en el clúster de Kubernetes.

- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.

Repositorio de código

El código de este patrón está disponible en el repositorio de soluciones Terraform Multi-Tenancy de GitHub EKS.

Prácticas recomendadas

Para directrices y prácticas recomendadas para utilizar esta implementación, consulte lo siguiente:

- Amazon EKS multi-tenancy best practices
- Documentación de Flux

Epics

Creación de canalizaciones para las etapas de compilación, prueba e implementación de Terraform

Tarea	Descripción	Habilidades requeridas
Clone el repositorio del proyecto.	Clone el repositorio de la solución GitHub EKS Multi-Tenancy Terraform ejecutando el siguiente comando en una ventana de terminal: `git clone https://github.com/aws-samples/aws-eks-multitenancy-deployment.git`	AWS DevOps
Inicie el bucket de S3 de Terraform y Amazon DynamoDB.	1. En la carpeta `bootstrap`, abra el archivo `bootstrap.sh` y actualice los valores de las variables para el nombre del bucket de S3, el nombre de la tabla de	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	DynamoDB y la Región de AWS:
	
	`S3_BUCKET_NAME="<S3_BUCKET_NAME>" DYNAMODB_TABLE_NAME="<DYNAMODB_NAME>" REGION="<AWS_REGION>"`
	
	2. Ejecute el script `bootstrap.sh` . El script requiere el AWS CLI, que usted instaló como parte de los requisitos previos.
	
	`cd bootstrap ./bootstrap.sh`	

Tarea	Descripción	Habilidades requeridas

Actualice los archivos `run.sh` y `locals.tf` .	1. Cuando el proceso de arranque se complete correctamente, copie el bucket de S3 y el nombre de la tabla de DynamoDB de la sección `variables` del script `bootstrap.sh` :
	`# Variables S3_BUCKET_NAME="< S3_BUCKET_NAME>" DYNAMODB_TABLE_NAME ="<DYNAMODB_NAME"`
	2. Pegue esos valores en el script `run.sh`, que se encuentra en el directorio raíz del proyecto:
	`BACKEND_BUCKET_ID= "<SAME_NAME_AS_S3_ BUCKET_NAME>" DYNAMODB_ID=" <SAME_NAME_AS_DYNA MODB_NAME>"`
	3. Cargue el código del proyecto en un CodeCommit repositorio. Puede crear este repositorio automáticamente a través de Terraform. Para ello, establezca la variable siguiente en `true` en el archivo `demo/pipeline/ locals.tf` :
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`create_new_repo = true` 4. Actualice el archivo `locals.tf` de acuerdo con sus requisitos para crear recursos de canalización.	

Implemente el módulo de canalización.	Para crear recursos de canalización, ejecute los comandos siguientes de Terraform de manera manual. No hay ninguna orquestación para ejecutar estos comandos automáticamente.
	`./run.sh -m pipeline -e demo -r <AWS_REGION> -t init`
	`./run.sh -m pipeline -e demo -r <AWS_REGION> -t plan`
	`./run.sh -m pipeline -e demo -r <AWS_REGION> -t apply`
		AWS DevOps

Creación de la infraestructura de red

Tarea	Descripción	Habilidades requeridas
Iniciar la canalización.	1. En la carpeta `templates`, asegúrese de que los archivos `buildspec`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	tengan la siguiente variable establecida en `network`: `TF_MODULE_TO_BUILD: "network"` 2. En la CodePipeline consola, en la página de detalles de la canalización, inicia la canalización seleccionando Release change. Tras esta primera ejecución , la canalización se iniciará automáticamente cada vez que realices un cambio en la rama principal del CodeCommit repositorio. La canalización incluye las siguientes etapas: • `validate` inicializa Terraform, ejecuta los análisis de seguridad de Terraform mediante las herramientas checkov y tfsec y carga los informes de análisis en el bucket de S3. • `plan` muestra el plan de Terraform y lo carga en el bucket de S3.	

Tarea	Descripción	Habilidades requeridas
	• `apply`aplica el resultado del plan Terraform del depósito de S3 y crea AWS recursos. • `destroy`elimina los AWS recursos creados durante la `apply` etapa. Para habilitar esta etapa opcional, establezca la variable siguiente en `true` en el archivo `demo/pipeline/locals.tf` : `enable_destroy_stage = true`	

Tarea	Descripción	Habilidades requeridas
Valide los recursos creados a través del módulo de red.	Confirme que los siguiente s AWS recursos se crearon después de que la canalizac ión se implementara correctamente: • Una VPC de salida con tres subredes públicas y tres privadas, una puerta de enlace de Internet y una puerta de enlace NAT. • Una VPC de Amazon EKS con tres subredes privadas. • El arrendatario 1 y el arrendatario 2 VPCs tienen tres subredes privadas cada uno. • Una puerta de enlace de tránsito con todas las conexiones de la VPC y las rutas a cada subred privada. • Una ruta de puerta de enlace de tránsito estática para la VPC de salida de Amazon EKS con un bloque de CIDR de destino de `0.0.0.0/0` . Esto es necesario para permitir que todos tengan acceso saliente VPCs a Internet a través de la VPC de salida de Amazon EKS.	AWS DevOps

Creación de la infraestructura de computación

Tarea	Descripción	Habilidades requeridas

Actualice `locals.tf` para permitir el acceso del CodeBuild proyecto a la VPC.	Para implementar los complementos para el clúster privado de Amazon EKS, el CodeBuild proyecto debe estar adjunto a la VPC de Amazon EKS.
	1. En la carpeta `demo/pipeline` , abra el archivo `locals.tf` y establezca la variable `vpc_enabled` en `true`.
	2. Ejecute el script `run.sh` para aplicar los cambios al módulo de canalización:
	`demo/pipeline/locals.tf`
	`./run.sh -m pipeline -env demo -region <AWS_REGION> -tfcmd init`
	`./run.sh -m pipeline -env demo -region <AWS_REGION> -tfcmd plan`
	`./run.sh -m pipeline -env demo -region <AWS_REGION> -tfcmd apply`
		AWS DevOps

Actualice los archivos `buildspec` para crear el módulo de computación.	En la carpeta `templates` , en todos los archivos de YAML `buildspec` , establezca el valor de	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	la variable `TF_MODULE_TO_BUILD` de `network` a `compute`: `TF_MODULE_TO_BUILD: "compute"`	

Tarea	Descripción	Habilidades requeridas

Actualice el archivo `values` para el gráfico de Helm de administración de inquilinos.	1. Abra el archivo `values.yaml` en la ubicación siguiente:
	`cd cfg-terraform/demo/compute/cfg-tenant-mgmt`
	El archivo tiene este aspecto:
	`---`
	`global:`
	`  clusterRoles:`
	`  operator:`
	`  platform-tenant`
	`  flux: flux-tenant-applier`
	`  flux:`
	`  tenantCloneBaseUrl: ${TEANT_BASE_URL}`
	`  repoSecret:`
	`  ${TENANT_REPO_SECRET}`
	`tenants:`
	`  tenant-1:`
	`  quotas:`
	`  limits:`
	`  cpu: 1`
	`  memory: 1Gi`
	`  flux:`
	`  path: overlays/tenant-1`
	`  tenant-2:`
	`  quotas:`
	`  limits:`
	`  cpu: 1`
	`  memory: 2Gi`
	`  flux:`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`path: overlays/tenant-2` 2. En las secciones `global` y `tenants`, actualice la configuración según sus requisitos: • `tenantCloneBaseUrl` : ruta al repositorio que aloja el código para todos los inquilinos (utilizamos el mismo repositorio de Git para todos los inquilinos) • `repoSecret` : el secreto de Kubernetes que contiene las claves SSH y los hosts conocidos para autenticarse en el repositorio Git de inquilinos global • `quotas`: cuotas de recursos de Kubernetes que quiere aplicar a cada inquilino • `flux path`: ruta a los archivos de YAML de la aplicación de inquilinos en el repositorio global de inquilinos	

Tarea	Descripción	Habilidades requeridas
Valide los recursos de computación.	Tras actualizar los archivos en los pasos anteriores, se CodePipeline inicia automáticamente. Confirme que creó los siguientes AWS recursos para la infraestructura informática: • Clúster de Amazon EKS con punto de conexión privado • Nodos de trabajo de Amazon EKS • Complementos de Amazon EKS: secretos externos, `aws-loadbalancer-controller` y `metrics-server` • GitOps módulo, gráfico de Flux Helm, gráfico de Cilium Helm y gráfico de Helm de gestión de inquilinos	AWS DevOps

Comprobación de la administración de inquilinos y otros recursos

Tarea	Descripción	Habilidades requeridas
Valide los recursos de administración de inquilinos en Kubernetes.	Ejecute los comandos siguientes para comprobar que los recursos de administración de inquilinos se hayan creado correctamente con la ayuda de Helm. 1. Se crearon los espacios de nombres de inquilinos,	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	tal y como se especifica en `values.yaml` :
	`kubectl get ns -A`
	2. Las cuotas se asignan a cada espacio de nombres de inquilinos, tal y como se especifica en `values.yaml` :
	`kubectl get quota --namespace=<tenant_namespace>`
	3. Los detalles de las cuotas son correctos para cada espacio de nombres de inquilinos:
	`kubectl describe quota cpu-memory-resource-quota-limit -n <tenant_namespace>`
	4. Las políticas de red de Cilium se aplicaron a cada espacio de nombres de inquilinos:
	`kubectl get CiliumNetworkPolicy -A`	

Tarea	Descripción	Habilidades requeridas

Verifique las implement aciones de aplicaciones de inquilinos.	Para comprobar que se implementaron las aplicacio nes de inquilinos, ejecute los comandos siguientes.
	
	1. Flux puede conectarse al CodeCommit repositorio especificado en el GitOps módulo:
	
	`kubectl get gitreposi tories -A`
	
	2. El controlador de personali zación de Flux ha desplegado los archivos YAML en el repositorio: CodeCommit
	
	`kubectl get kustomiza tions -A`
	
	3. Todos los recursos de la aplicación se implement an en sus espacios de nombres de inquilinos:
	
	`kubectl get all -n <tenant_namespace>`
	
	4. Se creó una entrada para cada inquilino:
	
	`kubectl get ingress -n <tenant_namespace>`	

Resolución de problemas

Problema	Solución

Aparece un mensaje de error similar al siguiente:
 	
`Failed to checkout and determine revision: unable to clone unknown error: You have successfully authenticated over SSH. You can use Git to interact with AWS CodeCommit.`
	Para solucionar el problema, haga lo siguiente:
	
	1. Verifique el repositorio de aplicaciones de inquilinos: es posible que el error se deba a un repositorio vacío o mal configura do. Asegúrese de que el repositorio de aplicaciones de inquilinos contenga el código necesario.
	2. Vuelva a implementar el módulo `tenant_mgmt` : en el archivo de configuración del módulo `tenant_mgmt` , encuentre el bloque `app` y, a continuación establezca el parámetro `deploy` en `0`:
	
	`deploy = 0`
	
	Tras ejecutar el comando `apply` de Terraform, vuelva a cambiar el valor del parámetro `deploy` a `1`:
	
	`deploy = 1`
	
	3. Vuelva a comprobar el estado: tras ejecutar los pasos anteriores, utilice el comando siguiente para comprobar si persiste el problema:
	
	`kubectl get gitrepositories -A`
	
	Si persiste, considere la posibilidad de profundizar en los registros de Flux para obtener más detalles o consulte la guía general de solución de problemas de Flux.

Recursos relacionados

- Amazon EKS Blueprints for Terraform
- Amazon EKS Best Practices Guides, Multi-tenancy section
- Sitio web de Flux
- Sitio web de Helm

Información adicional

A continuación, se muestra un ejemplo de estructura de repositorios para implementar aplicaciones de inquilinos:

```
applications
sample_tenant_app
### README.md
### base
#   ### configmap.yaml
#   ### deployment.yaml
#   ### ingress.yaml
#   ### kustomization.yaml
#   ### service.yaml
### overlays
    ### tenant-1
    #   ### configmap.yaml
    #   ### deployment.yaml
    #   ### kustomization.yaml
    ### tenant-2
        ### configmap.yaml
        ### kustomization.yaml
```

Simplificación del desarrollo y la implementación de los bots de Amazon Lex mediante un flujo de trabajo automatizado

Balaji Panneerselvam, Attila Dancso, Pavan Dusanapudi, Anand Junnani y James O'Hara, Amazon Web Services

Resumen

Desarrollar e implementar los bots conversacionales de Amazon Lex puede ser un desafío cuando se trata de administrar varias características, desarrolladores y entornos. Un flujo de trabajo automatizado que utilice los principios de la infraestructura como código (IaC) puede ayudar a agilizar el proceso. Este patrón puede ayudar a mejorar la productividad de los desarrolladores de Amazon Lex y permitir una administración eficiente del ciclo de vida de los bots de las maneras siguientes:

- Permita el desarrollo simultáneo de varias características: con un flujo de trabajo automatizado, los desarrolladores pueden trabajar en distintas características en paralelo en ramas independientes. Luego, los cambios se pueden combinar e implementar sin bloquear otros trabajos.
- Utilice la IU de la consola de Amazon Lex: los desarrolladores pueden utilizar la consola sencilla de Amazon Lex para crear y probar bots. A continuación, se describen los bots en el código de infraestructura para su implementación.
- Promocione los bots en los entornos: el flujo de trabajo automatiza la promoción de las versiones de los bots desde entornos más bajos, como el de desarrollo y las pruebas, hasta la producción. Este enfoque reduce el riesgo y la sobrecarga de las promociones manuales.
- Mantenga el control de versiones: la administración de las definiciones de bots en Git, en lugar de hacerlo únicamente a través del servicio Amazon Lex, le proporciona el control de versiones y un registro de auditoría. Los cambios se rastrean a los desarrolladores individuales, a diferencia de cuando solo se utilizan Consola de administración de AWS o APIs para modificar los bots almacenados en ellos AWS.

Al automatizar el proceso de lanzamiento de los bots de Amazon Lex, los equipos pueden ofrecer características más rápido, con menos riesgos y esfuerzos. Los bots permanecen bajo control de versiones en lugar de estar aislados en la consola de Amazon Lex.

Requisitos previos y limitaciones

Requisitos previos

- El flujo de trabajo incluye varios Cuentas de AWS para diferentes entornos (desarrollo, producción y DevOps), lo que requiere configuraciones de administración de cuentas y acceso entre cuentas.
- Python 3.9 está disponible en el entorno de implementación o canalización.
- Git se instaló y configuró en una estación de trabajo local para el control del código fuente.
- AWS Command Line Interface (AWS CLI) instalado y configurado para autenticarse mediante la línea de comandos o Python.

Limitaciones

- Acceso al repositorio: el flujo de trabajo presupone que la canalización de integración continua y entrega continua (CI/CD) tiene los permisos necesarios para llevar a cabo cambios en el repositorio de código fuente.
- Versión inicial del bot: las herramientas requieren que se implemente una versión inicial del bot mediante AWS CloudFormation plantillas. Debe crear la primera iteración del bot y enviarla al repositorio antes de que el flujo de trabajo automatizado pueda tomar el control.
- Conflictos de combinación: aunque el flujo de trabajo tiene como objetivo permitir el desarrollo simultáneo, aún existe la posibilidad de que se produzcan conflictos de combinación al integrar cambios de ramas distintas. La resolución de conflictos en las configuraciones de los bots puede requerir una intervención manual.

Versiones de producto

- Python 3.9 o superior
- AWS CDK v2 2.12.4.0 o superior
- AWS SDK para Python (Boto3)1,28 o superior

Arquitectura

En el diagrama siguiente se muestra la arquitectura de alto nivel y los componentes clave de la solución.

Entre los componentes clave se incluyen los siguientes:

- Repositorio de bots de Lex: un repositorio de Git que almacena las definiciones de IaC para los bots de Amazon Lex.

- DevOps— Una Cuenta de AWS dedicada a alojar los CI/CD oleoductos y los recursos relacionados para el proceso de desarrollo e implementación.
- Canalizaciones: AWS CodePipeline instancias que automatizan varias etapas del ciclo de vida de desarrollo e implementación de los bots, como la creación de un nuevo bot, la exportación de la definición de un bot, la importación de una definición de bot y la eliminación de un bot.
- Bots de tickets y bot principal: los recursos del bot de Amazon Lex, en los que los bots de tickets son bots con características específicas desarrollados por equipos o desarrolladores individuales, y el bot principal es el bot básico que integra todas las características.

El diagrama de arquitectura ilustra el flujo de trabajo siguiente:

1. Bot principal de referencia: el punto de partida del flujo de trabajo es basar el bot principal en el entorno de desarrollo (Dev). El bot principal sirve de base para desarrollos futuros y adiciones de características.
2. Cree un bot de tickets: cuando es necesaria una característica nueva o un cambio, se crea un bot de tickets. El bot de tickets es básicamente una copia o una rama del bot principal en la que los desarrolladores pueden trabajar sin que ello afecte a la versión principal.
3. Exporte el bot de tickets: una vez finalizado el trabajo en el bot de tickets, se exporta desde el servicio Amazon Lex. A continuación, se hace un cambio de base de la rama que contiene el bot de tickets desde la rama principal. Este paso garantiza que se incorporen todos los cambios hechos en el bot principal mientras el bot de tickets se encontraba en desarrollo, lo que reduce los conflictos posibles.
4. Importe el bot de tickets con cambio de base y valide: el bot de tickets con cambio de base se importa de nuevo al entorno de desarrollo y se valida para garantizar que funciona correctamente con los cambios más recientes de la rama principal. Si la validación se hace correctamente, se crea una solicitud de extracción (PR) para combinar los cambios del bot de tickets con la rama principal.
5. Elimine el bot de tickets: una vez que los cambios se hayan combinado correctamente en la rama principal, el bot de tickets ya no será necesario. El bot de tickets se puede eliminar para mantener el entorno limpio y manejable.
6. Implemente el bot principal en el entorno de desarrollo y pruébelo: el bot principal actualizado, que ahora incluye las nuevas características o cambios, se implementa en el entorno de desarrollo. Aquí se somete a pruebas exhaustivas para garantizar que todas las funcionalidades responden según lo previsto.

7. Implemente el bot principal en el entorno de producción: una vez finalizadas y satisfactorias las pruebas en el entorno de desarrollo, el bot principal se implementa en el entorno de producción. Este paso es la etapa final del flujo de trabajo, en la que las características nuevas están disponibles para los usuarios finales.

Automatización y escala

El flujo de trabajo automatizado permite a los desarrolladores trabajar en características distintas en paralelo, cada una en ramas independientes. Esto facilita el desarrollo simultáneo, lo que permite a los equipos colaborar de manera eficaz y ofrecer características con mayor rapidez. Al estar las ramas aisladas unas de otras, los cambios se pueden combinar e implementar sin bloquear ni interferir con otros trabajos en curso.

El flujo de trabajo automatiza la implementación y la promoción de versiones de bots en entornos distintos, por ejemplo, desarrollo, pruebas y producción.

El almacenamiento de las definiciones de bots en un sistema de control de versiones como Git proporciona un registro de auditoría completo y permite una colaboración eficiente. Los desarrolladores individuales controlan los cambios, lo que garantiza la transparencia y la responsabilidad durante todo el ciclo de vida del desarrollo. Este enfoque también facilita las revisiones del código, lo que permite a los equipos identificar y abordar los problemas antes de la implementación en la producción.

Al usar AWS CodePipeline y otros Servicios de AWS, el flujo de trabajo automatizado se puede escalar para adaptarse a cargas de trabajo y tamaños de equipos cada vez mayores.

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software de código abierto para definir la Nube de AWS infraestructura en el código mediante el uso de lenguajes de programación conocidos y aprovisionarla mediante el aprovisionamiento. CloudFormation La implementación de muestra de este patrón utiliza Python.
- AWS CDK Interfaz de línea de comandos (AWS CDK CLI): el AWS CDK kit de herramientas es la herramienta principal para interactuar con AWS CDK la aplicación. Ejecuta tu aplicación, consulta el modelo de aplicación que has definido y produce e implementa las CloudFormation plantillas generadas por la CDK.

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todo el país. Cuentas de AWS Regiones de AWS Este patrón se utiliza CloudFormation para implementar las configuraciones de bots de Amazon Lex y los recursos relacionados utilizando la infraestructura como código.
- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar. Este patrón se utiliza CodeBuild para crear y empaquetar los artefactos de implementación.
- AWS CodePipeline permite diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software y automatizar los pasos necesarios para lanzar los cambios en el software de manera continua. Este patrón se utiliza CodePipeline para organizar el proceso de entrega continua.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que te ayuda a interactuar Servicios de AWS mediante comandos en el shell de tu línea de comandos.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Lex V2 sirve Servicio de AWS para crear interfaces de conversación (bots) para aplicaciones que utilizan voz y texto.
- AWS SDK para Python (Boto3)es un kit de desarrollo de software que le ayuda a integrar su aplicación, biblioteca o script de Python con Servicios de AWS.

Otras herramientas

- Git es un sistema de control de versiones distribuido de código abierto.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub management-framework-sample-for-amazon-lex. El repositorio de código contiene las carpetas y los archivos siguientes.

- `prerequisites`carpeta: contiene las definiciones de CloudFormation pila (utilizando la AWS CDK) para configurar los recursos y entornos necesarios.

- Carpeta `prerequisite/lexmgmtworkflow`: directorio principal del proyecto de Lex Management Workflow, que incluye las definiciones de pila y el código Python.
- `prerequisite/tests`: contiene pruebas unitarias.
- `src`: directorio de código fuente, que incluye el contenedor y las utilidades de administración de bots de Amazon Lex.
- `src/dialogue_lambda`: directorio de códigos fuente de la función de Lambda del enlace de diálogo que intercepta y procesa las entradas de los usuarios durante una conversación con un bot de Amazon Lex.

Prácticas recomendadas

- Separación de preocupaciones
  - Mantenga una clara separación de responsabilidades entre DevOps los entornos de desarrollo y producción.
  - Úselo Cuentas de AWS por separado para cada entorno a fin de reforzar los límites de aislamiento y seguridad adecuados.
  - Utilice roles entre cuentas y principios de acceso con privilegios mínimos para garantizar el acceso controlado entre entornos.
- La infraestructura como código
  - Revise y actualice de manera periódica el código de infraestructura para adaptarlo a las prácticas recomendadas y a los requisitos en evolución.
  - Establezca una estrategia clara de ramificación y combinación para el repositorio de código fuente
- Pruebas y validación
  - Implemente pruebas automatizadas en varias etapas del proceso para detectar los problemas al principio del ciclo de desarrollo.
  - Utilice la consola de Amazon Lex o los marcos de pruebas automatizadas para validar las configuraciones y la funcionalidad de los bots antes de pasarlo a entornos superiores.
  - Considere la posibilidad de implementar puertas de aprobación manuales para las implementaciones en entornos críticos o de producción.
- Supervisión y registro
  - Configure mecanismos de supervisión y registro para las canalizaciones, las implementaciones y las interacciones de bots.

  - Supervise los eventos de la canalización, los estados de la implementación y las métricas de rendimiento de los bots para identificar y abordar los problemas de inmediato.
  - Utilice los servicios de AWS, como Amazon CloudWatch AWS CloudTrail, y AWS X-Ray para el registro y la supervisión centralizados.
  - Revise y analice de manera periódica el rendimiento, la eficiencia y la eficacia del flujo de trabajo automatizado.
- Seguridad y conformidad
  - Implemente prácticas de codificación seguras y siga las prácticas recomendadas de AWS seguridad para el desarrollo e implementación de los bots Amazon Lex.
  - Revise y actualice de manera periódica los roles, las políticas y los permisos de IAM para ajustarlos al principio de privilegios mínimos.
  - Considere la posibilidad de integrar el análisis de seguridad y las comprobaciones de cumplimiento en los procesos.

Epics

Configuración de IaC para la administración de bots de Amazon Lex

Tarea	Descripción	Habilidades requeridas

Configure el entorno local de CDK.	1. Para clonar el repositorio de este patrón e ir al directorio `prerequisite` , ejecute el comando siguiente.
	`git clone https://github.com/aws-samples/management-framework-sample-for-amazon-lex.git`
	`cd management-framework-sample-for-amazon-lex`
	2. Para instalar y activar el entorno virtual de Python,
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	ejecute el comando siguiente que instala las dependencias de la CDK de manera local en la carpeta del proyecto, en lugar de hacerlo de manera global:
	`pip install virtualenv`
	`python<version> -m venv .venv`
	`source .venv/bin/activate`
	`python -m pip install -r requirements.txt`	

Cree un rol entre cuentas en el entorno de `devops`.	La `devops` cuenta es responsable del alojamiento y la administración de las CI/CD canalizaciones. Para permitir que las CI/CD canalizaciones interactúen con los `prod` entornos `dev` y, ejecuta los siguientes comandos para crear un rol multicuenta en la cuenta. `devops`
	`cdk bootstrap --profile=devops`
	`cdk deploy LexMgmtDevopsRoleStack -c dev-account-id=222222222222 -c prod-account-id=333333333333 --profile=devops`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

Cree un rol entre cuentas en el entorno de `dev`.	Cree un rol de IAM en la cuenta de `dev` con los permisos necesarios para permitir que la cuenta de `devops` asuma este rol. La CI/CD canalización utiliza esta función para realizar acciones en la `dev` cuenta, como implementar y administrar los recursos de los bots de Amazon Lex.
	
	Para crear el rol de IAM, ejecute los comandos siguientes:
	
	`cdk bootstrap --profile =dev`
	
	`cdk deploy LexMgmtCr ossaccountRoleStac k -c devops-account- id=1111111111111 -- profile=dev`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

Cree un rol entre cuentas en el entorno de `prod`.	Cree un rol de IAM en la cuenta de `prod` con los permisos necesarios para permitir que la cuenta de `devops` asuma este rol. La CI/CD canalización utiliza esta función para realizar acciones en la `prod` cuenta, como implementar y administrar los recursos de los bots de Amazon Lex.
	`cdk bootstrap --profile =prod`
	
	`cdk deploy LexMgmtCr ossaccountRoleStac k -c devops-account- id=1111111111111 -- profile=prod`
		AWS DevOps

Cree canalizaciones en el entorno de `devops`.	Para administrar el flujo de trabajo de desarrollo de los bots de Amazon Lex, ejecute el comando siguiente para configurar las canalizaciones en el entorno de `devops`. `cdk deploy LexMgmtWo rkflowStack -c devops- account-id=111111111 1111 -c dev-account- id=2222222222222 -c prod-account-id=33 3333333333 --profile =devops`	AWS DevOps

Establecimiento de la línea de base para el bot principal

Tarea	Descripción	Habilidades requeridas
Defina la versión inicial del bot principal.	Para definir la versión inicial del bot principal, desencadene la canalización de `BaselineBotPipeline` . La canalización implement a la definición básica del bot que se define en la CloudForm ation plantilla, exporta la definición principal del bot en forma de archivos.json y almacena el código del bot principal en un sistema de control de versiones.	AWS DevOps

Implemente el flujo de trabajo de desarrollo de características

Tarea	Descripción	Habilidades requeridas
Cree el bot de tickets para desarrollar y probar una característica.	`TicketBot` es una instancia de bot nueva que se importa de la definición de bot principal existente en la rama de características. Este enfoque garantiza que el bot nuevo tenga todas las funcionalidades y configura ciones actuales del bot principal. Para definir la versión inicial del bot de tickets, desencade	Desarrollador de bots de Lex

Tarea	Descripción	Habilidades requeridas
	ne la canalización `CreateTicketBotPipeline` . La canalización crea una rama nueva de características en el sistema de control de versiones y crea una instancia nueva de bot de tickets basada en el bot principal.	
Desarrolle y pruebe la característica del bot de tickets.	Para desarrollar y probar la función, inicie sesión en la consola Amazon Lex Consola de administración de AWS y ábrala en https://console.aws.amazon.com/lex/. Para más información, consulte Testing a bot using the console en la documentación de Amazon Lex. Con la instancia de `TicketBot` , ahora puede agregar, modificar o ampliar la funcionalidad del bot para implementar la característica nueva. Por ejemplo, puede crear o modificar intenciones, expresiones, espacios y flujos de diálogo. Para más información, consulte Adding intents en la documentación de Amazon Lex.	Desarrollador de bots de Lex

Tarea	Descripción	Habilidades requeridas
Exporte la definición de bot de tickets.	La definición de bot exportada es básicamente una representación de la configuración y la funcionalidad del bot en formato JSON. Para exportar la definición del bot de tickets, desencadene la canalización `ExportTicketBotPipeline` . La canalización exporta la definición del bot de tickets como archivos .json y almacena el código del bot de tickets en una rama de características del sistema de control de versiones.	Desarrollador de bots de Lex

Tarea	Descripción	Habilidades requeridas
Cambie la base de la rama de características desde la última rama principal.	Durante el desarrollo de una característica nueva, es posible que la rama principal haya recibido otros cambios por parte de desarrolladores o equipos distintos. Para incorporar estos cambios en la rama de características, haga una operación `rebase` de Git. Básicamente, esta operación reproduce las confirmaciones de la rama de características sobre las confirmaciones más recientes de la rama principal, lo que garantiza que la rama de características incluya todos los cambios más recientes	Desarrollador de bots de Lex

Tarea	Descripción	Habilidades requeridas
Importe y valide el bot de tickets que cambió de base.	Tras cambiar la base de la rama de características, debe importarla a la instancia del bot de tickets. Esta importación actualiza el bot de tickets existente con los cambios más recientes de la rama que cambió de base. Para importar el bot de tickets con nueva base, desencadene la canalización `ImportTicketBotPipeline` . La canalización importa a la instancia de `TicketBot` los archivos .json de la definición del bot de tickets que se encuentran en la rama de características del sistema de control de versiones.	Desarrollador de bots de Lex

Tarea	Descripción	Habilidades requeridas
Valide la definición de bot que cambió de base.	Tras importar la definición de bot con cambio de base, es fundamental validar su funcionalidad. Debe asegurarse de que la característica nueva funcione según lo esperado y no entre en conflicto con la funcionalidad existente. Por lo general, esta validación implica probar el bot con varios escenarios de entrada, comprobar las respuestas y comprobar que el bot se comporta según lo previsto. Puede llevar a cabo la validación de cualquiera de las siguientes maneras: • Pruebe el bot manualmente mediante la consola de Amazon Lex. • Utilice un enfoque automatizado mediante marcos y herramientas de prueba que puedan simular las interacciones de los usuarios y afirmar las respuestas esperadas.	Desarrollador de bots de Lex

Tarea	Descripción	Habilidades requeridas
Combine la rama de caracterí sticas con la rama principal.	Tras desarrollar y probar la característica nueva en la instancia de `TicketBot` aislada, haga lo siguiente: 1. Haga los cambios en la rama de características correspondiente del sistema de control de versiones. 2. Para combinar la rama de características con la rama principal, cree una solicitud de extracción (PR). Esta PR sirve como una solicitud para revisar e incorporar los cambios en el código base principal.	Desarrollador de bots de Lex, administrador de repositorios

Tarea	Descripción	Habilidades requeridas
Elimine la rama de caracterí sticas y el bot de tickets.	Cuando una rama de caracterí sticas se haya combinado correctamente con la rama principal, elimine la rama de características y el bot de tickets del repositorio de código fuente. Para eliminar la rama de características y el bot de tickets, desencadene la canalización `DeleteTic ketBotPipeline` . La canalización elimina los recursos de bots temporale s que se crearon durante el proceso de desarrollo (por ejemplo, el bot de tickets). Esta acción ayuda a mantener un repositorio limpio y a evitar confusiones o conflictos con las ramas de características futuras.	Desarrollador de bots de Lex

Mantén el bot principal

Tarea	Descripción	Habilidades requeridas
Importe la última definición de bot principal al entorno de `dev`.	Para importar al entorno de `dev` la última definición de bot principal de la rama principal, desencadene la canalización de `DeployBotDevPipeli ne` .	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	La canalización también crea una etiqueta de git tras su aprobación.	
Importe la última definición de bot principal al entorno de `prod`.	Para importar al entorno de `prod` la definición de bot más reciente de la rama principal , proporcione la referenci a de etiqueta de la tarea anterior como parámetro y desencadene la canalización de `DeployBotProdPipel ine` . La canalización importa al entorno de `prod` la definició n de bot más reciente de una etiqueta específica.	AWS DevOps

Resolución de problemas

Problema	Solución
Al implementar los bots de Amazon Lex en diferentes cuentas Cuentas de AWS, los servicios de herramientas deben tener los permisos necesarios para acceder a los recursos de esas cuentas.	Para conceder acceso entre cuentas, utilice roles y políticas de IAM. Cree roles de IAM en las cuentas de destino y adjunte políticas a los roles que concedan los permisos necesarios. A continuación, asuma estos roles desde la cuenta en la que está implementado el bot de Amazon Lex. Para más información, consulte IAM permissio ns required to import y IAM permissions required to export bots in Lex V2 en la documentación de Amazon Lex.

Recursos relacionados

- Importing bots in Amazon Lex V2
- Inicie una canalización en CodePipeline
- Trabajar con los bots de Amazon Lex V2

Coordine la dependencia de los recursos y la ejecución de tareas mediante la construcción AWS Fargate WaitCondition hook

Stan Fan, Amazon Web Services

Resumen

Este patrón describe el paquete npm WaitCondition hook (`waitcondition-hook-for-aws-fargate-task`), que es una solución nativa de la nube diseñada para organizar tareas AWS Fargateen clústeres de Amazon Elastic Container Service (Amazon ECS).

El WaitCondition gancho es una AWS Cloud Development Kit (AWS CDK) construcción diseñada específicamente para su integración con. AWS CloudFormation El WaitCondition gancho ofrece las siguientes funciones clave:

- Actúa como un mecanismo de condición de espera y detiene la ejecución de la CloudFormation pila hasta que se complete una tarea específica de Fargate, lo que ayuda a organizar las implementaciones y el aprovisionamiento de recursos.
- Soporta TypeScript Python, lo que lo hace ideal para AWS CDK proyectos.
- Permite a los desarrolladores y arquitectos orquestar las implementaciones coordinando la finalización de las tareas y la administración de los recursos para las aplicaciones en contenedores en AWS.
- Permite ejecutar tareas de Fargate con uno o varios contenedores integrados en un CloudFormation ciclo de vida, y puede gestionar los errores de las tareas y revertir la CloudFormation pila después de un error en las tareas.
- Proporciona flexibilidad para agregar dependencias entre los recursos y los resultados de la ejecución de tareas de Fargate, lo que permite personalizar tareas o invocar otros puntos de conexión. Por ejemplo, puede pausar una CloudFormation pila y esperar a que se realice una migración de base de datos (realizada mediante una tarea de Fargate) y aprovisionar otros recursos que podrían depender del éxito de la migración de la base de datos.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.

- AWS Cloud Development Kit (AWS CDK) Interfaz de línea de comandos (CLI) instalada en una estación de trabajo local. Para obtener más información, consulte la referencia de AWS CDK CLI en la AWS CDK documentación.
- Gestor de paquetes de nodos (npm), instalado en una estación de trabajo local y configurado para entrar.AWS CDK TypeScript Para obtener más información, consulte Descarga e instalación de Node.js y npm en la documentación de npm.
- Yarn instalado en un equipo de trabajo local. Para más información, consulte Installation en la documentación de Yarn.

Limitaciones

- Esta solución se implementa en una sola. Cuenta de AWS
- El código de retorno esperado del contenedor es `0` para indicar que es correcto. Cualquier otro código devuelto indica un error y la CloudFormation pila se revertirá.
- Algunos Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

En el siguiente diagrama se muestra la arquitectura del constructo.

En el diagrama siguiente se muestra el flujo de trabajo de `waitcondition-hook-for-aws-fargate-task`:

1. `WaitCondition`y `WaitConditionHandler` están aprovisionados para escuchar la respuesta de las funciones. AWS Lambda
2. Según el resultado de la tarea, se desencadena `CallbackFunction` o `ErrorHandlerFunction` al finalizar la tarea de Fargate.
3. La función de Lambda envía una señal de CORRECTO o ERROR a `WaitConditionHandler`.
4. `WaitConditionHandler` continúa aprovisionando los recursos si el resultado de la ejecución de la tarea de Fargate es correcto o revierte la pila si se produjo un error en la tarea.

En el diagrama siguiente se muestra un ejemplo de un flujo de trabajo para hacer una migración de bases de datos.

El flujo de trabajo de ejemplo utiliza el constructo `waitcondition-hook-for-aws-fargate-task` para hacer una migración de base de datos de la manera siguiente:

1. Una instancia de Amazon Relational Database Service (Amazon RDS) aprovisionada.
2. El constructo `waitcondition-hook-for-aws-fargate-task` ejecuta la tarea de migración de la base de datos y detiene la pila como una instancia de Amazon Elastic Compute Cloud (Amazon EC2).
3. Si la tarea de migración finaliza correctamente, envía una señal de éxito a CloudFormation. De lo contrario, envía una señal de error a la pila CloudFormation y la revierte.

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir la infraestructura de nube en código y a aprovisionarla CloudFormation.
- CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todo el Cuentas de AWS mundo Regiones de AWS.
- Amazon le CloudWatch ayuda a supervisar las métricas de sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores escalable y rápido que ayuda a ejecutar, detener y administrar contenedores en un clúster.
- AWS Fargate le permite ejecutar contenedores sin necesidad de administrar servidores o instancias de Amazon EC2. Se utiliza en conjunto con Amazon ECS.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

- AWS Step Functionses un servicio de organización sin servidor que le ayuda a combinar AWS Lambda funciones y otras Servicios de AWS para crear aplicaciones esenciales para la empresa.
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de utilizar la infraestructura escalable de AWS.

Otras herramientas

- npm es un registro de software que se ejecuta en un entorno Node.js y se utiliza para compartir o tomar prestados paquetes y administrar la implementación de paquetes privados.
- Yarn es un administrador de paquetes de código abierto que puede usar para administrar las dependencias en JavaScript los proyectos. Yarn puede serle útil para instalar, actualizar, configurar y eliminar las dependencias de los paquetes.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub waitcondition-hook-for-aws-fargate-task.

Prácticas recomendadas

- Al crear su AWS CDK aplicación, siga las prácticas recomendadas para desarrollar e implementar una infraestructura de nube que figuran AWS CDK en la documentación de la versión 2. AWS CDK
- Para la AWS Fargate tarea, siga las prácticas recomendadas para las imágenes de contenedores de Amazon ECS de la documentación de Amazon ECS.

Epics

Configure el AWS CDK

Tarea	Descripción	Habilidades requeridas
Instale el AWS CDK.	Para instalarlo AWS CDK en su máquina local u otro entorno, ejecute el siguiente comando:	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`npm install -g aws-cdk@latest`	
Inicie el AWS CDK.	El arranque es el proceso para preparar un entorno para la implementación. Para iniciar su AWS CDK kit de herramientas para el objetivo Cuenta de AWS Región de AWS, ejecute el siguiente comando: `cdk bootstrap aws://ACCOUNT-NUMBER-1/REGION-1` Este comando crea una CloudFormation pila llamada. `CDKToolkit`	Arquitecto de la nube

Ejecute el WaitCondition enlace para la construcción de AWS Fargate tareas

Tarea	Descripción	Habilidades requeridas
Crear el proyecto de CDK	Cree un proyecto de CDK con el lenguaje que prefiera. Este patrón usa TypeScript. Para crear un proyecto de CDK mediante TypeScript, ejecute el siguiente comando: `cdk init app –language typescript`	Arquitecto de la nube
Instale el paquete.	Ejecute `npm install` en la ruta raíz de su proyecto de	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	CDK. Después de instalar la biblioteca de CDK, ejecute el comando siguiente para instalar `waitcondition-hook-for-aws-fargate-task` : `yarn add waitcondition-hook-for-aws-fargate-task`	

Tarea	Descripción	Habilidades requeridas

Cree su aplicación de CDK y los componentes de Amazon ECS.	Cree el proyecto de CDK. Se requiere un recurso de definición de tareas de Amazon ECS. Para obtener información acerca de la creación de una definición de tareas, consulte Definiciones de tareas de Amazon ECS en la documentación de Amazon ECS.
	
	El ejemplo siguiente utiliza este constructo:
	
	`import * as cdk from 'aws-cdk-lib';`
	`import { Vpc } from 'aws-cdk-lib/aws-ec2';`
	`import * as ecr from 'aws-cdk-lib/aws-ecr';`
	`import * as ecs from 'aws-cdk-lib/aws-ecs';`
	`import { Construct } from 'constructs';`
	`import { FargateRunner } from 'waitcondition-hook-for-aws-fargate-task';`
	`import { Queue } from 'aws-cdk-lib/aws-sqs';`
	
	`export class FargateRunnerStack extends cdk.Stack {`
		Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas

	constructor(scope: Construct, id: string, props?: cdk.StackProps) {
	super(scope, id, props);
	// Define the VPC
	const vpc = new Vpc(this, 'MyVpc')
	// Define the Fargate Task
	const taskDefinition = new ecs.FargateTaskDefinition(this, 'MyTask', {});
	// Import exiting ecr repo
	const repo = ecr.Repository.fromRepositoryName(this, 'MyRepo', 'RepoName');
	// Add a container to the task
	taskDefinition.addContainer('MyContainer', {
	image: ecs.ContainerImage.fromEcrRepository(repo),
	});
	// Create the Fargate runner
	const myFargateRunner = new FargateRunner(this, 'MyRunner', {
	fargateTaskDef: taskDefinition,
	timeout: `${60 * 5}`,	

Tarea	Descripción	Habilidades requeridas

	<pre>vpc: vpc,
	});
	// Create the SQS queue
	const myQueue = new Queue(this, 'MyQueue', {});
	// Add dependency
	myQueue.node.addDependency(myFargateRunner);
	}
	}</pre>	

Sintetice y lance la aplicación de CDK.	1. Para generar los activos y la CloudFormation plantilla, ejecute el siguiente comando en la ruta raíz de la CDK:
	`cdk synth`
	2. Una vez que el comando `synth` se ejecute correctamente, ejecute el comando siguiente para implementar los recursos:
	`cdk deploy`
	
	El constructo `waitcondition-hook-for-aws-fargate-task` ejecuta la tarea de Fargate.
		Arquitecto de la nube

Limpieza

Tarea	Descripción	Habilidades requeridas
Eliminación de recursos.	Para limpiar los recursos aprovisionados en el paso anterior, ejecute el comando siguiente: `cdk destroy`	Arquitecto de la nube

Resolución de problemas

Problema	Solución
Fallo general en la CloudFormation pila	Para ayudar a solucionar los errores generales de la CloudFormation pila, añade la `--no-rollback` marca como se muestra en el siguiente ejemplo: `cdk deploy --no-rollback` Este comando hará que la CloudFormation pila deje de revertirse, lo que te proporcionará recursos para solucionar problemas. Para obtener más información, consulte Elegir cómo gestionar los errores al aprovisionar recursos en la CloudFormation documentación.
AWS Step Functions error	Es posible que una máquina de AWS Step Functions estados no se ejecute por diferente s motivos. Una vez configurado `–disable-rollback` , haga lo siguiente para solucionar un error:

Problema	Solución
	1. Inicie sesión en Consola de administración de AWS, introduzca Step Functions en el campo de búsqueda y, a continuación, seleccione el servicio Step Functions. 2. En el panel de navegación izquierdo, elija Máquinas de estado y, a continuación, seleccione la máquina de estado aprovisio nada por la CloudFormation pila. 3. En Ejecuciones, elija el nombre de la ejecución en la que se produjo el error inesperado. 4. En la vista Eventos, elija el paso del error. Para obtener más información, consulte Solución de problemas en Step Functions y Visualización de los detalles de ejecución en la consola de Step Functions en la AWS Step Functions documentación.

Problema	Solución
AWS Lambda fallo de función	Este constructo proporciona dos funciones de Lambda: `CallbackFunction` y `ErrorhandlerFunction`. Pueden producirse error por varios motivos, como excepciones no controladas. Haga lo que se indica a continuación para solucionar un error: 1. Inicie sesión en Consola de administración de AWS, introduzca CloudWatchen el campo de búsqueda y, a continuación, seleccione el CloudWatch servicio. 2. En el panel de navegación izquierdo, elija Registros, Grupos de registros. 3. En el campo de búsqueda, introduzca el nombre de la función de Lambda. 4. Elija el nombre de grupo de registros que se asocia a la función de Lambda. 5. Para ir al resultado de la ejecución de la función de Lambda, elija el flujo de registro más reciente. Para obtener más información, consulte Solución de problemas en Lambda en la AWS Lambda documentación.

Recursos relacionados

AWS documentación

- AWS CDK Construye una referencia de API
- Cómo empezar con el AWS CDK
- Aprenda a crear y utilizar los recursos de Amazon ECS
- Aprenda cómo empezar a usar Step Functions

- ¿Qué es AWS CDK?

Otros recursos

- Waitcondition Hook for AWS Fargate task (npm)
- waitcondition-hook-for-aws-fargate-task 1.0.6 (pypi.org)

Utilice repositorios de código fuente de Git de terceros en AWS CodePipeline

Kirankumar Chandrashekar, Amazon Web Services

Resumen

Este patrón describe cómo usar AWS CodePipeline con repositorios de código fuente de Git de terceros.

AWS CodePipeline es un servicio de entrega continua que automatiza las tareas de creación, prueba e implementación del software. Actualmente, el servicio es compatible con los repositorios de Git gestionados por GitHub AWS CodeCommit y Atlassian Bitbucket. Sin embargo, algunas empresas utilizan repositorios Git de terceros que están integrados con su servicio de inicio de sesión único (SSO) y Microsoft Active Directory para la autenticación. Puedes usar estos repositorios de Git de terceros como fuentes CodePipeline creando acciones personalizadas y webhooks.

Un webhook es una notificación HTTP que detecta eventos en otra herramienta, como un GitHub repositorio, y conecta esos eventos externos a una canalización. Cuando creas un webhook en CodePipeline, el servicio devuelve una URL que puedes usar en el webhook de tu repositorio de Git. Si insertas código en una rama específica del repositorio de Git, el webhook de Git inicia el CodePipeline webhook a través de esta URL y establece la etapa de origen de la canalización como En progreso. Cuando la canalización se encuentra en este estado, el trabajador CodePipeline busca el trabajo personalizado, lo ejecuta y envía un estado de éxito o fracaso a. CodePipeline En este caso, dado que la canalización se encuentra en la fase de origen, el trabajador obtiene el contenido del repositorio de Git, lo comprime y lo carga en el depósito de Amazon Simple Storage Service (Amazon S3), donde se almacenan los artefactos de la canalización, utilizando la clave de objeto proporcionada por el trabajo sondeado. También puedes asociar una transición para la acción personalizada a un evento en Amazon CloudWatch e iniciar el trabajo en función del evento. Esta configuración te permite usar repositorios Git de terceros que el servicio no admite de forma nativa como fuentes. CodePipeline

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un repositorio de Git que admite webhooks y puede conectarse a una URL de CodePipeline webhook a través de Internet

- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada con la cuenta de AWS

Arquitectura

El patrón incluye los siguientes pasos:

1. El usuario confirma el código en un repositorio de Git.
2. Se llama el webhook de Git.
3. Se llama CodePipeline webhook.
4. La canalización está configurada En curso y la etapa de origen está configurada en el estado En curso.
5. La acción de la etapa de origen inicia una regla de CloudWatch eventos, lo que indica que se ha iniciado.
6. El CloudWatch evento inicia una función Lambda.
7. La función de Lambda obtiene los detalles del trabajo de acción personalizado.
8. La función Lambda inicia CodeBuild AWS y le pasa toda la información relacionada con el trabajo.
9. CodeBuild obtiene la clave SSH pública o las credenciales de usuario para el acceso a HTTPS Git desde Secrets Manager.
10. CodeBuild clona el repositorio de Git para una rama específica.
11. CodeBuild comprime el archivo y lo carga en el depósito de S3 que sirve como almacén de CodePipeline artefactos.

Tools (Herramientas)

- AWS CodePipeline: AWS CodePipeline es un servicio de entrega continua totalmente gestionado que le ayuda a automatizar sus procesos de lanzamiento para obtener actualizaciones rápidas y fiables de las aplicaciones y la infraestructura. CodePipeline automatiza las fases de creación, prueba e implementación del proceso de publicación para cada cambio de código, en función del modelo de publicación que defina. Le permite entregar características y actualizaciones de forma rápida y de confianza. Puede integrar AWS CodePipeline con servicios de terceros, como GitHub su propio complemento personalizado.

- AWS Lambda: AWS Lambda le permite ejecutar código sin aprovisionar ni administrar servidores. Con Lambda, puede ejecutar código para prácticamente cualquier tipo de aplicación o servicio backend sin necesidad de administración. Sólo tiene que cargar su código y Lambda se encarga de todo lo necesario para ejecutar y escalar su código con alta disponibilidad. Puede configurar el código para que se active automáticamente desde otros servicios de AWS o puede llamarlo directamente desde cualquier aplicación web o móvil.
- AWS CodeBuild: AWS CodeBuild es un servicio de integración continua totalmente gestionado que compila el código fuente, ejecuta pruebas y produce paquetes de software listos para su implementación. Con CodeBuild, no necesita aprovisionar, administrar ni escalar sus propios servidores de compilación. CodeBuild escala de forma continua y procesa varias compilaciones simultáneamente, para que sus compilaciones no se queden esperando en una cola. Puede comenzar con rapidez usando entornos de compilación preempaquetados, o crear sus propios entornos de compilación personalizados que utilicen sus propias herramientas de compilación.
- AWS Secrets Manager: AWS Secrets Manager le ayuda a proteger los secretos necesarios para acceder a sus aplicaciones, servicios y recursos de TI. El servicio le permite rotar, administrar y recuperar fácilmente credenciales de bases de datos, claves de API y otros datos confidenciales durante todo su ciclo de vida. Los usuarios y las aplicaciones recuperan los secretos llamando a Secrets Manager APIs, sin tener que codificar información confidencial en texto plano. Secrets Manager ofrece rotación secreta con integración integrada para Amazon Relational Database Service (Amazon RDS), Amazon Redshift y Amazon DocumentDB. El servicio se puede ampliar para admitir otros tipos de secretos, incluidas las claves y los OAuth tokens de API. Además, Secrets Manager le permite controlar el acceso a los datos secretos mediante permisos detallados y auditar la rotación de secretos de forma centralizada para los recursos de la nube de AWS, los servicios de terceros y los entornos locales.
- Amazon CloudWatch: Amazon CloudWatch es un servicio de monitoreo y observación creado para DevOps ingenieros, desarrolladores, ingenieros de confiabilidad de sitios (SREs) y administradores de TI. CloudWatch le proporciona datos e información útil para supervisar sus aplicaciones, responder a los cambios en el rendimiento de todo el sistema, optimizar la utilización de los recursos y obtener una visión unificada del estado de las operaciones. CloudWatch recopila datos operativos y de supervisión en forma de registros, métricas y eventos, lo que le proporciona una visión unificada de los recursos, las aplicaciones y los servicios de AWS que se ejecutan en AWS y en servidores locales. Puede utilizarlos CloudWatch para detectar comportamientos anómalos en sus entornos, configurar alarmas, visualizar registros y métricas uno al lado del otro, tomar medidas automatizadas, solucionar problemas y descubrir información para que sus aplicaciones sigan funcionando sin problemas.

- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que le permite almacenar y proteger cualquier cantidad de datos para diversos casos de uso, tales como sitios web, aplicaciones móviles, copia de seguridad y restauración, archivado, aplicaciones empresariales, dispositivos IoT y análisis de macrodatos. Amazon S3 ofrece funciones easy-to-use de administración que le ayudan a organizar sus datos y configurar controles de acceso ajustados con precisión para cumplir con sus requisitos empresariales, organizativos y de conformidad específicos.

Epics

Cree una acción personalizada en CodePipeline

Tarea	Descripción	Habilidades requeridas
Cree una acción personalizada mediante AWS CLI o AWS CloudFormation.	Este paso implica la creación de una acción de origen personalizada que se pueda utilizar en la fase de origen de una canalización en su cuenta de AWS en una región concreta. Debe usar AWS CLI o AWS CloudFormation (no la consola) para crear la acción de origen personalizada. Para obtener más información sobre los comandos y los pasos descritos en esta y otras epics, consulte la sección «Recursos relacionados» al final de este patrón. En AWS CLI, utilice el create-custom-action-type comando. Utilice --configuration-properties para proporcionar todos los parámetros necesarios para que el trabajador del trabajo	AWS general

Tarea	Descripción	Habilidades requeridas
	los procese cuando busca un trabajo CodePipeline . Asegúrese de anotar los valores proporcionados a las opciones --provider y --action-version, de modo que puedas usar los mismos valores al crear la canalización con esta etapa fuente personali zada. También puede crear la acción de origen personali zada en AWS CloudForm ation mediante el tipo de recurso AWS::CodePipeline: :CustomActionType.	

Configuración de la autenticación

Tarea	Descripción	Habilidades requeridas
Cree un par de claves SSH.	Cree un par de claves Secure Shell (SSH). Para obtener instrucciones, consulte la GitHub documentación.	Sistemas/ingeniero DevOps
Crear un secreto en AWS Secrets Manager.	Copie el contenido de la clave privada del par de claves SSH y cree un secreto en AWS Secrets Manager. Este secreto se utiliza para la autenticación al acceder al repositorio de Git.	AWS general
Añada la clave pública al repositorio de Git.	Añada la clave pública del par de claves SSH a la configura	Ingeniero/sistema DevOps

Tarea	Descripción	Habilidades requeridas
	ción de la cuenta del repositor io de Git para autenticarte con la clave privada.	

Crear una canalización y un webhook

Tarea	Descripción	Habilidades requeridas
Crear una canalización que incluya la acción de origen personalizada.	Crea una canalización en CodePipeline. Al configurar la etapa de origen, elija la acción de origen personalizada que creó anteriormente. Puede hacerlo en la CodePipel ine consola de AWS o en la CLI de AWS. CodePipel ine le solicita las propiedad es de configuración que ha establecido en la acción personalizada. Esta informaci ón es necesaria para que el trabajador procese el trabajo para la acción personalizada. Siga las instrucciones del asistente y cree la siguiente etapa para la canalización.	AWS general
Crea un CodePipeline webhook.	Cree un webhook para la canalización que creócon la acción de origen personali zada. Debe usar AWS CLI o AWS CloudFormation (no la consola) para crear el webhook. En AWS CLI, ejecute el comando put-webho	AWS general

Tarea	Descripción	Habilidades requeridas
	ok y proporcione los valores adecuados para las opciones de webhook. Anote la URL del webhook que devuelve el comando. Si utiliza AWS CloudFormation para crear el webhook, utilice el tipo AWS::CodePipeline::Webhook de recurso. Asegúrese de generar la URL del webhook del recurso creado y anotarla.	

Tarea	Descripción	Habilidades requeridas
Cree una función y CodeBuild un proyecto de Lambda.	En este paso, utiliza Lambda CodeBuild para crear un trabajador laboral que sondee las solicitudes de trabajo CodePipeline para la acción personalizada, ejecute el trabajo y devuelva el resultado de estado al. CodePipeline Cree una función Lambda que se inicie mediante una regla de Amazon CloudWatch Events cuando la etapa de acción de origen personalizada de la canalización pase a «En curso». Cuando se inicia la funciónde Lambda, debe obtener los detalles del trabajo de acción personalizado consultando los trabajos. Puede utilizar la PollForJobs API para devolver esta información. Una vez obtenida la información del trabajo sondeada, la función de Lambda debe devolver un acuse de recibo y, a continuación, procesar la información con los datos que obtiene de las propiedades de configuración de la acción personalizada. Cuando el trabajador esté listo para comunicarse con el repositorio de Git, puedes iniciar un CodeBuild	AWS general, desarrollador de código

Tarea	Descripción	Habilidades requeridas
	proyecto, ya que es convenien te gestionar las tareas de Git mediante el cliente SSH.	

Crea un evento en CloudWatch

Tarea	Descripción	Habilidades requeridas
Crea una regla de CloudWatc h eventos.	Cree una regla de CloudWatc h eventos que inicie la función Lambda como objetivo siempre que la etapa de acción personalizada de la canalización pase a «En curso».	AWS general

Recursos relacionados

Crear una acción personalizada en CodePipeline

- Cree y añada una acción personalizada en CodePipeline
- AWS::CodePipeline::CustomActionType recurso

Configurar la autenticación

- Creación y administración de secretos con AWS Secrets Manager

Crear una canalización y un webhook

- Crea una canalización en CodePipeline
- Referencia del comando put-webhook
- AWS::CodePipeline::Webhook recurso
- PollForJobs Referencia de la API

- Crea y añade una acción personalizada en CodePipeline
- Cree un proyecto de compilación en AWS CodeBuild

Creación de un evento

- Detecte los cambios en el estado de la canalización y reaccione ante ellos con Amazon CloudWatch Events

Referencias adicionales

- Trabajando con canalizaciones en CodePipeline
- Guía para desarrolladores de AWS Lambda

Cree una CI/CD canalización para validar las configuraciones de Terraform mediante AWS CodePipeline

Aromal Raj Jayarajan y Vijesh Vijayakumaran Nair, Amazon Web Services

Resumen

Este patrón muestra cómo probar las configuraciones de HashiCorp Terraform mediante una canalización de integración y entrega continuas (CI/CD) implementada por AWS. CodePipeline

Terraform es una aplicación de interfaz de la línea de comandos que le ayuda a usar código para aprovisionar y administrar la infraestructura y los recursos de la nube. La solución que se proporciona en este patrón crea una CI/CD canalización que le ayuda a validar la integridad de las configuraciones de Terraform mediante cinco etapas: CodePipeline

1. `"checkout"`extrae la configuración de Terraform que está probando de un repositorio de AWS CodeCommit .
2. `"validate"`ejecuta herramientas de validación de infraestructura como código (IaC), incluidas tfsec y checkov. TFLint La etapa también ejecuta los siguientes comandos de validación de Terraform IaC: `terraform validate` y `terraform fmt`.
3. `"plan"` muestra qué cambios se aplicarán a la infraestructura si se aplica la configuración de Terraform.
4. `"apply"` utiliza el plan generado para aprovisionar la infraestructura requerida en un entorno de prueba.
5. `"destroy"` elimina la infraestructura de prueba que se creó durante la `"apply"` etapa.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de AWS (AWS CLI)instalada y configurada
- Git, instalado y configurado en su equipo local
- Terraform, instalado y configurado en su equipo local

Limitaciones

- El enfoque de este patrón implementa AWS CodePipeline en una sola cuenta de AWS y solo en una región de AWS. Se requieren cambios de configuración para las implementaciones de varias cuentas y regiones.
- El rol de AWS Identity and Access Management (IAM) que proporciona este patrón (codepipeline_iam_role) sigue el principio de privilegio mínimo. Los permisos de este rol de IAM deben actualizarse en función de los recursos específicos que necesite crear su canalización.

Versiones de producto

- Versión de AWS CLI 2.9.15 o posterior
- Versión de Terraform 1.3.7 o posterior

Arquitectura

Pila de tecnología de destino

- AWS CodePipeline
- AWS CodeBuild
- AWS CodeCommit
- AWS IAM
- Amazon Simple Storage Service (Amazon S3)
- AWS Key Management Service (AWS KMS)
- Terraform

Arquitectura de destino

El siguiente diagrama muestra un ejemplo de flujo de trabajo en CI/CD canalización para probar las configuraciones de Terraform. CodePipeline

En el diagrama, se muestra el siguiente flujo de trabajo:

1. En CodePipeline, un usuario de AWS inicia las acciones propuestas en un plan de Terraform ejecutando el `terraform apply` comando en la CLI de AWS.
2. AWS CodePipeline asume una función de servicio de IAM que incluye las políticas necesarias para acceder CodeCommit a AWS KMS y Amazon S3. CodeBuild

3. CodePipeline ejecuta la etapa de `"checkout"` canalización para extraer la configuración de Terraform de un CodeCommit repositorio de AWS para probarla.
4. CodePipeline ejecuta la `"validate"` etapa para probar la configuración de Terraform ejecutando las herramientas de validación de IaC y los comandos de validación de Terraform IaC en un proyecto. CodeBuild
5. CodePipeline ejecuta la `"plan"` etapa para crear un plan en el CodeBuild proyecto basado en la configuración de Terraform. El usuario de AWS puede revisar este plan antes de aplicar los cambios al entorno de prueba.
6. Code Pipeline ejecuta la `"apply"` fase de implementación del plan utilizando el CodeBuild proyecto para aprovisionar la infraestructura requerida en el entorno de prueba.
7. CodePipeline ejecuta la `"destroy"` etapa, que se utiliza CodeBuild para eliminar la infraestructura de prueba que se creó durante la `"apply"` etapa.
8. Un bucket de Amazon S3 almacena los artefactos de la canalización, que se cifran y descifran mediante una clave administrada por el cliente de AWS KMS.

Tools (Herramientas)

Herramientas

Servicios de AWS

- AWS le CodePipeline ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.
- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otros servicios

- HashiCorp Terraform es una aplicación de interfaz de línea de comandos que le ayuda a usar código para aprovisionar y administrar la infraestructura y los recursos de la nube.

Código

El código de este patrón está disponible en el repositorio. GitHub aws-codepipeline-terraform-cicdsamples El repositorio contiene las configuraciones de Terraform necesarias para crear la arquitectura de destino descrita en este patrón.

Epics

Aprovisionar los componentes de la solución

Tarea	Descripción	Habilidades requeridas
Clona el GitHub repositorio.	Clone el GitHub aws-codepipeline-terraform-cicdsamplesrepositorio ejecutando el siguiente comando en una ventana de terminal: `git clone https://github.com/aws-samples/aws-codepipeline-terraform-cicd-samples.git` Para obtener más información, consulte Clonación de un repositorio en la GitHub documentación.	DevOps ingeniero
Cree un archivo de definiciones de variables de Terraform.	Cree un archivo `terraform.tfvars` en función de los requisitos del caso de uso. Puede actualizar las variables del archivo `examples/`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`terraform.tfvars` que se encuentra en el repositorio clonado. Para obtener más información, consulte Asignación de valores a las variables del módulo raíz en la documentación de Terraform. **Note** El archivo `Readme.md` del repositorio incluye más información sobre las variables obligatorias.	
Configure AWS como proveedor de Terraform.	1. En un editor de código, abra el archivo `main.tf` del repositorio clonado. 2. Añada las configuraciones necesarias para establecer la conectividad con la cuenta de AWS de destino. Para obtener más información, consulte AWS provider en la documentación de Terraform.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Actualice la configuración del proveedor de Terraform para crear el bucket de replicación de Amazon S3.	1. Ejecute el siguiente comando para abrir el directorio S3 del repositorio: `cd ./modules/s3` 2. Actualice la configuración del proveedor de Terraform para crear el depósito de replicación de Amazon S3 actualizando el valor `region` en del archivo `tf`. Asegúrese de introducir la región en la que desea que Amazon S3 replique los objetos. 3. (Opcional) De forma predeterminada, Terraform usa archivos estatales locales para la administr ación estatal. Si desea añadir Amazon S3 como backend remoto, debe actualizar la configuración de Terraform. Para obtener más información, consulte Configuración de backend en la documentación de Terraform. **Note** La replicación activa la copia de objetos entre	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	buckets de Amazon S3 de forma automática y asincrónica.	
Inicialice la configuración de Terraform.	Para inicializar el directorio de trabajo que contiene los archivos de configuración de Terraform, ejecute el siguiente comando en la carpeta raíz del repositorio clonado: `terraform init`	DevOps ingeniero
Crear el plan Terraform.	Para crear un plan de Terraform, ejecuta el siguiente comando en la carpeta raíz del repositorio clonado: `terraform plan --var-file=terraform.tfvars -out=tfplan` **Note** Terraform evalúa los archivos de configuración para determinar el estado objetivo de los recursos declarados. A continuación, compara el estado objetivo con el estado actual y crea un plan.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Verifique el plan de Terraform.	Revise el plan Terraform y confirme que configura la arquitectura requerida en su cuenta de AWS de destino.	DevOps ingeniero
Implemente la solución.	1. Para aplicar el plan Terraform, ejecute el siguiente comando en la carpeta raíz del repositorio clonado: `terraform apply "tfplan"` 2. Escriba sí para confirmar que desea implementar los recursos. **Note** Terraform crea, actualiza o destruye la infraestructura para alcanzar el estado objetivo declarado en los archivos de configuración.	DevOps ingeniero

Validar las configuraciones de Terraform ejecutando la canalización

Tarea	Descripción	Habilidades requeridas
Configurar el repositorio de código fuente.	1. De la salida de Terraform , obtenga los detalles del	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	repositorio de origen del repositorio que contiene las configuraciones de Terraform que desea validar. 2. Inicie sesión en la Consola de administración de AWS. Luego, abre la CodeCommit consola. 3. Cree una nueva rama en el repositorio de origen denominado `main`. Para obtener instrucciones, consulte Crear una rama en AWS CodeCommit en la CodeCommit documentación. 4. Clone la rama `main` del repositorio de origen en su estación de trabajo local. Para obtener instrucciones, consulte los pasos de configuración de las conexiones HTTPS a CodeCommit los repositorios de AWS en Windows con el asistente de credenciales de la CLI de AWS en la documentación. CodeCommit 5. Copie la **`templates`** carpeta del GitHub aws-codepipeline-terraform-cicdsamplesrepositorio	

Tarea	Descripción	Habilidades requeridas
	ejecutando el siguiente comando: `cp -r templates $YOUR_CODECOMMIT_REPO_ROOT` **Note** La carpeta `templates` contiene los archivos de especificaciones de compilación y el script de validación del directorio raíz del repositorio de origen. 6. Añada las configuraciones de Terraform iAC necesarias a la carpeta raíz del repositorio de origen. 7. Agñada los detalles del backend remoto en la configuración de Terraform de su proyecto. Para obtener más información, consulte S3 en la documentación de Terraform. 8. (Opcional) Actualice las variables de la carpeta `templates` para activar	

Tarea	Descripción	Habilidades requeridas
	o desactivar los escaneos preconfigurados, cambiar las versiones de las herramientas y especificar su directorio en archivos de script personalizados. Para obtener más informaci ón, consulte la sección Información adicional de este patrón. 9. Envía los cambios a la rama `main` del repositorio de origen.	

Tarea	Descripción	Habilidades requeridas
Valide las etapas de la canalización.	1. Inicie sesión en la consola de administración de AWS y abra la consola de CodePipeline . 2. En el resultado generado por el `terraform apply "tfplan"` comando de la sección anterior de Epic, busca el nombre del generado CodePipeline. 3. Abre la canalización en la CodePipeline consola y selecciona Release change. 4. Revise cada etapa de la canalización y confirma que funciona según lo esperado. Para obtener más información, consulte Ver los detalles y el historial de la canalización (consola) en la Guía del CodePipeline usuario de AWS. **Important** Cuando se confirma un cambio en la ramificación principal del repositorio de origen, la canalización	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	de pruebas se activa automáticamente.	
Verifique el resultado del informe.	1. En la CodePipeline consola, en el panel de navegación izquierdo, selecciona Construir. A continuación, seleccione Historial de informes. 2. Revise los informes de escaneo tfsec y checkov que genera la canalización. Estos informes pueden ayudarle a identificar problemas mediante visualizaciones y representaciones gráficas. **Note** El `<project_name>-validate` CodeBuild proyecto genera informes de vulnerabilidad para el código durante la `"validate"` fase.	DevOps ingeniero

Eliminación de sus recursos

Tarea	Descripción	Habilidades requeridas
Limpie la canalización y los recursos asociados.	Para eliminar los recursos de prueba de su cuenta de AWS, ejecute el siguiente comando en la carpeta raíz del repositorio clonado: `terraform destroy --var-file=terraform.tfvars`	DevOps ingeniero

Resolución de problemas

Problema	Solución
Recibes un AccessDenied error durante la `"apply"` etapa.	1. Revise los registros de ejecución del CodeBuild proyecto asociados a la `"apply"` etapa para identificar los permisos de IAM que falten. Para obtener más información, consulte Ver los detalles de la compilación en AWS CodeBuild en la Guía del CodeBuild usuario de AWS. 2. En un editor de código, abra la carpeta del repositorio clonado `modules` . A continuación, navegue hasta la carpeta `iam-role` y abra el archivo `main.tf` que se encuentra en esa carpeta. 3. En la declaración `codepipeline_policy` , añada las políticas de IAM necesarias para aprovisionar recursos en su cuenta de AWS.

Recursos relacionados

- Bloques de módulos (documentación de Terraform)
- Cómo implementar y configurar CI/CD los servicios de seguridad de AWS con Terraform (entrada del blog de AWS)
- Uso de roles vinculados a servicios (documentación de IAM)
- create-pipeline (documentación de AWS CLI)
- Configurar el cifrado del lado del servidor para los artefactos almacenados en Amazon S3 para (documentación de CodePipeline AWS CodePipeline)
- Cuotas para AWS CodeBuild (CodeBuild documentación de AWS)
- Protección de datos en AWS CodePipeline (CodePipeline documentación de AWS)

Información adicional

Módulos Terraform personalizados

La siguiente es una lista de los módulos personalizados de Terraform que se utilizan en este patrón:

- `codebuild_terraform`crea los CodeBuild proyectos que forman cada etapa del proceso.
- `codecommit_infrastructure_source_repo`captura y crea el CodeCommit repositorio de origen.
- `codepipeline_iam_role` crea las funciones de IAM necesarias para la canalización.
- `codepipeline_kms` crea la clave de AWS KMS necesaria para el cifrado y descifrado de objetos de Amazon S3.
- `codepipeline_terraform`crea la canalización de pruebas para el CodeCommit repositorio de origen.
- `s3_artifacts_bucket` crea un bucket de Amazon S3 para administrar los artefactos de canalización.

Cree archivos de especificaciones

La siguiente es una lista de los archivos de especificaciones de compilación (buildspec) que este patrón utiliza para ejecutar cada etapa de la canalización:

- `buildspec_validate.yml` ejecuta la etapa `"validate"`.

- `buildspec_plan.yml` ejecuta la etapa `"plan"`.
- `buildspec_apply.yml` ejecuta la etapa `"apply"`.
- `buildspec_destroy.yml` ejecuta la etapa `"destroy"`.

Cree variables del archivo de especificaciones

Cada archivo de especificaciones de compilación utiliza las siguientes variables para activar diferentes ajustes específicos de la compilación:

Variable	Predeterminado	Description (Descripción)
`CODE_SRC_DIR`	"."	Define el CodeCommit directorio de origen
`TF_VERSION`	«1.3.7»	Define la versión de Terraform para el entorno de compilación

El archivo `buildspec_validate.yml`también admite las siguientes variables para activar diferentes ajustes específicos de la compilación:

Variable	Predeterminado	Description (Descripción)
`SCRIPT_DIR`	»./templates/scripts»	Define el directorio de scripts
`ENVIRONMENT`	«dev»	Define el nombre del entorno
`SKIPVALIDATIONFAILURE`	«Y»	Omite la validación en caso de errores
`ENABLE_TFVALIDATE`	«Y»	Activa la validación de Terraform
`ENABLE_TFFORMAT`	«Y»	Activa el formato Terraform
`ENABLE_TFCHECKOV`	«Y»	Activa el análisis de checkov
`ENABLE_TFSEC`	«Y»	Activa el análisis de TFSec

TFSEC_VERSION	«v1.28.1»	Define la versión tfsec

Más patrones

- Acceda a aplicaciones de contenedores de forma privada en Amazon EKS mediante AWS PrivateLink y un Network Load Balancer
- Asociar un AWS CodeCommit repositorio de una cuenta Cuenta de AWS a Amazon SageMaker AI Studio Classic de otra cuenta
- Automatice la creación de cuentas mediante el acelerador de zonas de aterrizaje en AWS
- Automatice la adición o actualización de entradas de registro de Windows con AWS Systems Manager
- Automatizar las copias de seguridad de las instancias de base de datos de Amazon RDS para PostgreSQL mediante AWS Batch
- Automatice la implementación de aplicaciones anidadas mediante SAM de AWS
- Automatice la implementación del controlador de terminación de nodos en Amazon EKS mediante una CI/CD canalización
- Automatizar la configuración de RabbitMQ en Amazon MQ
- Automatice la replicación de las instancias de Amazon RDS en Cuentas de AWS
- Cree e implemente automáticamente una aplicación Java en Amazon EKS mediante una CI/CD canalización
- Generación automática de un modelo de PynamoDB y funciones CRUD para Amazon DynamoDB mediante una aplicación de Python
- Valide e implemente automáticamente las políticas y funciones de IAM mediante CodePipeline IAM Access Analyzer y macros de AWS CloudFormation
- Realice copias de seguridad de los servidores Sun SPARC en el emulador Stromasys Charon-SSP del Nube de AWS
- Cree una canalización de datos para incorporar, transformar y analizar los datos de Google Analytics con el kit de AWS DataOps desarrollo
- Cree un PAC de servidor empresarial Micro Focus con Amazon EC2 Auto Scaling y Systems Manager
- Cree una canalización para imágenes de contenedores reforzadas con EC2 Image Builder y Terraform
- Cree un MLOps flujo de trabajo con Amazon SageMaker AI y Azure DevOps
- Centralice la resolución de DNS mediante AWS Managed Microsoft AD Microsoft Active Directory local

- Limpie los recursos de AWS Account Factory for Terraform (AFT) de forma segura después de la pérdida de archivos estatales
- Configure el registro para las aplicaciones.NET en Amazon CloudWatch Logs mediante NLog
- Copie imágenes de contenedores de Amazon ECR en y Cuentas de AWS Regiones de AWS
- Cree una imagen de contenedor Docker personalizada SageMaker y úsela para el entrenamiento de modelos en AWS Step Functions
- Cree una canalización en Regiones de AWS que no admiten AWS CodePipeline
- Cree alarmas para métricas personalizadas mediante la detección de CloudWatch anomalías de Amazon
- Personalice los nombres de los roles predeterminados mediante AWS CDK aspectos y trampillas de escape
- Implementación de una canalización que detecte simultáneamente los problemas de seguridad en varios entregables de código
- Implementar y administrar un lago de datos sin servidor en la nube de AWS mediante el uso de la infraestructura como código
- Implemente aplicaciones en contenedores si se AWS IoT Greengrass V2 ejecutan como un contenedor Docker
- Implementar recursos y paquetes de Kubernetes con Amazon EKS y un repositorio de gráficos de Helm en Amazon S3
- Implemente aplicaciones de varias pilas mediante AWS CDK con TypeScript
- Implemente la validación de seguridad de la codificación en tiempo real mediante un servidor MCP con Kiro y otros asistentes de codificación
- Implemente instancias de clústeres de conmutación por error de SQL Server en Amazon EC2 y Amazon FSx mediante Terraform
- Implemente las automatizaciones de seguridad para la AWS WAF solución mediante Terraform
- Desarrolle asistentes avanzados de IA generativa basados en chat mediante RAG y solicitudes ReAct
- Habilita Amazon de GuardDuty forma condicional mediante plantillas AWS CloudFormation
- Habilite el modo automático de Amazon EKS en todos los clústeres de EKS mediante GitHub acciones
- Configuración del escalado automático basado en eventos en Amazon EKS mediante Amazon EKS Pod Identity y KEDA
- Genere recomendaciones personalizadas y reclasificadas con Amazon Personalize

- Reciba notificaciones de Amazon SNS cuando cambie el estado de clave de una clave de AWS KMS
- Control de los conjuntos de permisos para varias cuentas mediante Account Factory for Terraform
- Identificación automática de las imágenes de contenedor duplicadas al migrar a un repositorio de Amazon ECR
- Implementación del control de versiones de API basado en rutas mediante dominios personalizados en Amazon API Gateway
- Mejore el rendimiento operativo habilitando Amazon DevOps Guru en varias regiones y cuentas de AWS y OUs con la CDK de AWS
- Instalación del agente SSM en los nodos de trabajo de Amazon EKS mediante Kubernetes DaemonSet
- Integrar el controlador universal Stonebranch con AWS Mainframe Modernization
- Modernización del mainframe: DevOps adelante AWS con Rocket Software Enterprise Suite
- Administre los conjuntos de AWS IAM Identity Center permisos como código mediante AWS CodePipeline
- Administre los conjuntos de AWS permisos de forma dinámica mediante Terraform
- Gestión de las aplicaciones de contenedores en las instalaciones mediante la configuración de Amazon ECS Anywhere con AWS CDK
- Gestione AWS Organizations las políticas como código mediante AWS CodePipeline Amazon Bedrock
- Migración de registros DNS de forma masiva a una zona alojada privada de Amazon Route 53
- Migre IIS-hosted aplicaciones a Amazon EC2 mediante appcmd.exe
- Supervise el uso de una imagen de máquina de Amazon compartida en múltiples Cuentas de AWS
- Organice una canalización de ETL con validación, transformación y particionamiento mediante AWS Step Functions
- Automatice blue/green las implementaciones de las bases de datos globales de Amazon Aurora mediante los principios de la IaC
- Preserve el espacio IP enrutable en los diseños de VPC de varias cuentas para subredes que no son de carga de trabajo
- Aprovisione un producto de Terraform AWS Service Catalog mediante un repositorio de código
- Puesta en marcha de las tareas de Automatización de AWS Systems Manager de forma sincrónica desde AWS Step Functions

- Configure una CI/CD canalización para cargas de trabajo híbridas en Amazon ECS Anywhere mediante AWS CDK y GitLab
- Configure una CI/CD canalización para la migración de bases de datos mediante Terraform
- Configure una infraestructura Multi-AZ para una FCI Always On de SQL Server mediante Amazon FSx
- Configure automáticamente los bots de UiPath RPA en Amazon EC2 mediante AWS CloudFormation
- Simplificación de la autenticación de aplicaciones con TLS mutuo en Amazon ECS mediante el equilibrador de carga de aplicación
- Incorporación de inquilinos en la arquitectura SaaS para el modelo de silo mediante C# y AWS CDK
- Usa Terraform para habilitar Amazon automáticamente GuardDuty para una organización
- Uso de agentes de Amazon Bedrock para automatizar la creación de controles de entrada de acceso en Amazon EKS mediante peticiones basadas en texto
- Validar Account Factory para el código Terraform (AFT) localmente
- Visualice los resultados del AI/ML modelo con Flask y AWS Elastic Beanstalk

infraestructura

Temas

- Acceda a un host bastión mediante Session Manager y Amazon EC2 Instance Connect
- Centralice la resolución de DNS mediante AWS Managed Microsoft AD Microsoft Active Directory local
- Centralice la supervisión mediante Amazon CloudWatch Observability Access Manager
- Comprueba EC2 las instancias para ver si hay etiquetas obligatorias en el lanzamiento
- Limpie los recursos de AWS Account Factory for Terraform (AFT) de forma segura después de la pérdida de archivos estatales
- Cree una canalización en Regiones de AWS que no admiten AWS CodePipeline
- Personalice los nombres de los roles predeterminados mediante AWS CDK aspectos y trampillas de escape
- Implemente un clúster de Cassandra en Amazon EC2 con estática privada IPs para evitar el reequilibrio
- Amplíe VRFs su alcance a AWS mediante AWS Transit Gateway Connect
- Reciba notificaciones de Amazon SNS cuando cambie el estado de clave de una clave de AWS KMS
- Preserve el espacio IP enrutable en los diseños de VPC de varias cuentas para subredes que no son de carga de trabajo
- Aprovisione un producto de Terraform AWS Service Catalog mediante un repositorio de código
- Registre varios Cuentas de AWS con una sola dirección de correo electrónico mediante Amazon SES
- Configure la resolución de DNS para redes híbridas en un entorno de AWS de una sola cuenta
- Configure automáticamente los bots de UiPath RPA en Amazon EC2 mediante AWS CloudFormation
- Configure una PeopleSoft arquitectura de alta disponibilidad en AWS
- Configure la recuperación ante desastres para Oracle JD Edwards EnterpriseOne con AWS Elastic Disaster Recovery
- Configure la detección de CloudFormation desviaciones en una organización multirregional y multicuenta
- Importación correcta de un bucket de S3 como CloudFormation pila de AWS

- Sincronice los datos entre los sistemas de archivos de Amazon EFS en distintas regiones de AWS mediante AWS DataSync
- Pruebe AWS la infraestructura mediante LocalStack Terraform Tests
- Actualice los clústeres de SAP Pacemaker de a ENSA1 ENSA2
- Utilice zonas de disponibilidad coherentes en VPCs diferentes cuentas de AWS
- Utilice el usuario IDs en las políticas de IAM para el control de acceso y la automatización
- Validar Account Factory para el código Terraform (AFT) localmente
- Más patrones

Acceda a un host bastión mediante Session Manager y Amazon EC2 Instance Connect

Piotr Chotkowski y Witold Kowalik, Amazon Web Services

Resumen

Un host bastión, también denominado jump box, es un servidor que proporciona un único punto de acceso desde una red externa a los recursos ubicados en una red privada. Un servidor expuesto a una red pública externa, como Internet, supone un posible riesgo de seguridad en caso de acceso no autorizado. Es importante proteger y controlar el acceso a estos servidores.

Este patrón describe cómo puede utilizar Session Manager y Amazon EC2 Instance Connect para conectarse de forma segura a un host bastión de Amazon Elastic Compute Cloud (Amazon EC2) implementado en su Cuenta de AWS servidor. El administrador de sesiones es una capacidad de AWS Systems Manager. Las ventajas de este patrón incluyen:

- El host bastión implementado no tiene ningún puerto de entrada abierto expuesto a la Internet pública. Esto reduce la posible superficie expuesta a ataques.
- No necesita almacenar ni mantener las claves de Secure Shell (SSH) de larga duración en su Cuenta de AWS. En su lugar, cada usuario genera un nuevo key pair de claves SSH cada vez que se conecta al host bastión. AWS Identity and Access Management Las políticas (IAM) que se adjuntan a las AWS credenciales del usuario controlan el acceso al host bastión.

Destinatarios previstos

Este patrón está dirigido a lectores que tengan experiencia con conocimientos básicos de Amazon EC2, Amazon Virtual Private Cloud (Amazon VPC) y Hashicorp Terraform.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- AWS Command Line Interface (AWS CLI) versión 2, instalada y configurada
- Se ha instalado el AWS CLI complemento Session Manager para
- CLI de Terraform, instalada

- Almacenamiento para el estado de Terraform, como un bucket de Amazon Simple Storage Service (Amazon S3) y una tabla de Amazon DynamoDB que sirven como un backend remoto para almacenar el estado de Terraform. Para obtener más información sobre el uso de backends remotos para el estado de Terraform, consulte los backends de Amazon S3 (documentación de Terraform). Para ver un ejemplo de código que configura la administración remota del estado con un backend de Amazon S3, consulte remote-state-s3-backend (Terraform Registry). Tenga en cuenta los siguientes requisitos:
  - El bucket de Amazon S3 y la tabla de DynamoDB deben estar en la misma Región de AWS.
  - Al crear la tabla de DynamoDB, la clave de partición debe ser `LockID` (distingue entre mayúsculas y minúsculas) y el tipo de clave de partición debe ser `String`. Todos los demás valores de la tabla deben estar en sus valores predeterminados. Para obtener más información, consulte Acerca de las claves principales y Crear una tabla en la documentación de DynamoDB.
- Un cliente SSH, instalado.

Limitaciones

- Este patrón pretende ser una prueba de concepto (PoC) o una base para un mayor desarrollo. No debe utilizarse en su forma actual en entornos de producción. Antes de la implementación, ajuste el código de muestra del repositorio para que se adapte a sus requisitos y a su caso de uso.
- Este patrón supone que el host bastión de destino utiliza Amazon Linux 2 como sistema operativo. Si bien es posible utilizar otras Amazon Machine Images (AMIs), otros sistemas operativos están fuera del alcance de este patrón.

> **Note**
>
> Se acerca el fin de la compatibilidad de Amazon Linux 2. Para obtener más información, consulte Amazon Linux 2 FAQs.

- En este patrón, el host bastión está ubicado en una subred privada sin una puerta de enlace NAT ni una puerta de enlace de Internet. Este diseño aísla la EC2 instancia de Amazon de la Internet pública. Puede añadir una configuración de red específica que le permita comunicarse con Internet. Para obtener más información, consulte Conectar su nube privada virtual (VPC) a otras redes en la documentación de Aamazon VPC. Del mismo modo, siguiendo el principio de privilegios mínimos, el host del bastión no tiene acceso a ningún otro recurso suyo a Cuenta de AWS menos que le concedas permisos de forma explícita. Para más información, consulte Políticas basadas en recursos en la documentación de IAM.

Versiones de producto

- CLI de AWS versión 2
- Terraform versión 1.3.9

Arquitectura

Pila de tecnología de destino

- Una VPC con una única subred privada
- Los siguientes puntos de conexión de VPC de interfaz:
  - `amazonaws.<region>.ssm`— El punto final del AWS Systems Manager servicio.
  - `amazonaws.<region>.ec2messages`: Systems Manager utiliza este punto de conexión para realizar llamadas desde SSM Agent al servicio de Systems Manager.
  - `amazonaws.<region>.ssmmessages`— Session Manager usa este punto final para conectarse a tu EC2 instancia de Amazon a través de un canal de datos seguro.
- Una EC2 instancia de `t3.nano` Amazon que ejecuta Amazon Linux 2
- Rol de IAM y perfil de instancia
- Grupos de seguridad de Amazon VPC y reglas de grupos de seguridad para los puntos de conexión y la instancia de Amazon EC2

Arquitectura de destino

El diagrama muestra el proceso siguiente:

1. El usuario asume un rol de IAM que tiene permisos para hacer lo siguiente:
   - Autenticar, autorizar y conectarse a la instancia de Amazon EC2
   - Iniciar una sesión con Session Manager
2. El usuario inicia una sesión SSH a través de Session Manager.
3. Session Manager autentica al usuario, verifica los permisos de las políticas de IAM asociadas, comprueba los ajustes de configuración y envía un mensaje al agente SSM para abrir una conexión bidireccional.

4. El usuario envía la clave pública SSH al host del bastión a través de los metadatos de Amazon. EC2 Esto debe hacerse antes de cada conexión. La clave pública SSH permanece disponible durante 60 segundos.
5. El host bastión se comunica con los puntos finales de la interfaz de VPC para Systems Manager y Amazon. EC2
6. El usuario accede al host bastión a través de Session Manager mediante un canal de comunicación bidireccional cifrado con TLS 1.2.

Automatizar y escalar

Las siguientes opciones están disponibles para automatizar la implementación o escalar esta arquitectura:

- Puede implementar la arquitectura mediante una canalización de integración y entrega continuas (CI/CD).
- Puede modificar el código para cambiar el tipo de instancia del host bastión.
- Puede modificar el código para implementar varios hosts bastión. En el archivo `bastion-host/main.tf`, en el bloque de recursos `aws_instance`, añada el meta argumento `count`. Para obtener más información, consulte la documentación de Terraform.

Tools (Herramientas)

Servicios de AWS

- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar Servicios de AWS mediante los comandos de su shell de línea de comandos.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática escalable en el Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Systems Manager lo ayuda a administrar las aplicaciones y la infraestructura que se ejecutan en la Nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo necesario para detectar y resolver problemas operativos y le ayuda a administrar sus AWS recursos de forma segura y a escala. Este patrón utiliza el Administrador de sesiones, una capacidad de Administrador de sistemas.

- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Otras herramientas

- HashiCorp Terraform es una herramienta de infraestructura como código (IaC) que facilita usar el código para aprovisionar y administrar los recursos y la infraestructura en la nube. Este patrón usa Terraform CLI.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub Access a bastion mediante el administrador de sesiones y el repositorio Amazon EC2 Instance Connect.

Prácticas recomendadas

- Recomendamos usar herramientas de escaneo de código automatizadas para mejorar la seguridad y la calidad del código. Este patrón se escaneó con Checkov, una herramienta de análisis de código estático para IaC. Como mínimo, le recomendamos que realice comprobaciones básicas de validación y formato mediante los comandos `terraform validate` y `terraform fmt -check -recursive` de Terraform.
- Es una buena práctica añadir pruebas automatizadas para la iAC. Para obtener más información sobre los diferentes enfoques para probar el código de Terraform, consulte Probar HashiCorp Terraform (entrada del blog de Terraform).
- Durante la implementación, Terraform usa la EC2 instancia de Amazon que reemplaza cada vez que se detecta una nueva versión de la AMI de Amazon Linux 2. Esto implementa la nueva versión del sistema operativo, que incluye los parches y las actualizaciones. Si el programa de implementación no es frecuente, esto puede suponer un riesgo para la seguridad, ya que la instancia no tiene los parches actualizados. Es importante actualizar y aplicar con frecuencia los parches de seguridad a las EC2 instancias de Amazon desplegadas. Para obtener más información, consulta Gestión de actualizaciones en Amazon EC2.
- Como este patrón es una prueba de concepto, utiliza políticas AWS gestionadas, como`AmazonSSMManagedInstanceCore`. AWS las políticas administradas cubren casos de uso comunes, pero no otorgan permisos con privilegios mínimos. Según sea necesario en su caso, le recomendamos que cree políticas personalizadas que concedan permisos con privilegios mínimos para los recursos implementados en esta arquitectura. Para obtener más información, consulte

Comenzar con las políticas AWS administradas y avanzar hacia los permisos con privilegios mínimos.

- Use una contraseña para proteger el acceso a las claves SSH y guarde las claves en un lugar seguro.
- Configure el registro y la supervisión del host bastión. El registro y la supervisión son partes importantes del mantenimiento de los sistemas, tanto desde una perspectiva operativa como de seguridad. Existen varias formas de supervisar las conexiones y la actividad en su host bastión. Para obtener más información, consulte los siguientes temas en la documentación de Systems Manager.
  - Supervisión AWS Systems Manager
  - Inicio de sesión y supervisión AWS Systems Manager
  - Auditoría de la actividad de sesiones
  - Registro de la actividad de la sesión

Epics

Implementación de recursos

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código.	1. En una interfaz de la línea de comandos, cambie el directorio de trabajo a la ubicación en la que desee almacenar los archivos de muestra. 2. Escriba el siguiente comando. `git clone https://github.com/aws-samples/secured-bastion-host-terraform.git`	DevOps ingeniero, desarrollador

Tarea	Descripción	Habilidades requeridas
Inicialice el directorio de trabajo de Terraform.	Este paso solo es necesario para la primera implement ación. Si va a realizar una reimplementación del patrón, vaya al paso siguiente. En el directorio raíz del repositorio clonado, introduzca el siguiente comando, donde: • `$S3_STATE_BUCKET` es el nombre del bucket de Amazon S3 que contiene el estado de Terraform • `$PATH_TO_STATE_FIL E` es la clave del archivo de estado de Terraform, como `infra/bastion-host/ tetfstate` • `$AWS_REGION` es la región donde se implementa el bucket de Amazon S3 `terraform init \ -backend-config="b ucket=$S3_STATE_BU CKET" \ -backend-config="k ey=$PATH_TO_STATE_ FILE" \ -backend-config="r egion=$AWS_REGION`	DevOps ingeniero, desarroll ador, Terraform

Tarea	Descripción	Habilidades requeridas
	Note También puede abrir el archivo config.tf y, en la sección `terraform` , proporcionar estos valores manualmente.	
Implementación de recursos.	1. En el directorio raíz del repositorio clonado, introduzca el siguiente comando. `terraform apply -var-file="dev.tfvars"` 2. Revise la lista de todos los cambios que se le aplicarán y Cuenta de AWS, a continuación, confirme la implementación. 3. Espere a que se implement en todos los recursos.	DevOps ingeniero, desarroll ador, Terraform

Configurar el entorno local

Tarea	Descripción	Habilidades requeridas
Configure la conexión SSH.	Actualice el archivo de configuración de SSH para permitir las conexiones SSH a través de Session Manager. Para obtener instrucciones,	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	consulte Permitir conexiones SSH para Session Manager. Esto permite a los usuarios autorizados introducir un comando proxy que inicia una sesión de Session Manager y transfiere todos los datos a través de una conexión bidireccional.	
Genere las claves SSH.	Introduzca el siguiente comando para general un par de claves de SSH locales privadas y publicas. Use este par de claves para conectarse al host bastión. `ssh-keygen -t rsa -f my_key`	DevOps ingeniero, desarroll ador

Conectarse al host bastión mediante Session Manager

Tarea	Descripción	Habilidades requeridas
Obtenga el ID de la instancia.	1. Para poder conectarte al host bastión implement ado, necesitas el ID de la EC2 instancia de Amazon. Realice una de las siguiente s acciones para localizar la ID: • Abre la EC2 consola de Amazon. En el panel de navegación, seleccione	AWS general

Tarea	Descripción	Habilidades requeridas

	Instances (Instancias). Localice la instancia del host bastión.
	• En el AWS CLI, introduce el siguiente comando.
	`aws ec2 describe-instances`
	Para filtrar los resultados, introduzca el siguiente comando, donde `$BASTION_HOST_TAG` es la etiqueta que asignó al host bastión. El valor predeterminado para esta etiqueta es `sandbox-dev-bastion-host` .
	`aws ec2 describe-instances \ --filters "Name=tag:Name,Values=$BASTION_HOST_TAG" \ --output text \ --query 'Reservations[*].Instances[*].InstanceId' \ --output text`
	2. Copia el ID de la EC2 instancia de Amazon. Usará este ID más tarde.	

Tarea	Descripción	Habilidades requeridas
Envíe la clave pública SSH.	**Note** En esta sección, debe cargar la clave pública en los metadatos de la instancia del host bastión. Una vez cargada la clave, dispone de 60 segundos para iniciar una conexión con el host bastión. Transcurridos 60 segundos, se elimina la clave pública. Para obtener más información, consulte la sección Solución de problemas de este patrón. Complete los siguientes pasos rápidamente para evitar que se extraiga la clave antes de conectarse al host bastión. 1. Envíe la clave SSH al host del bastión mediante Amazon Instance EC2 Connect. Escriba el siguiente comando, cuando:	AWS general

Tarea	Descripción	Habilidades requeridas
	• `$INSTANCE_ID` es el ID de la EC2 instancia de Amazon • `$PUBLIC_KEY_FILE` es la ruta al archivo de claves públicas, como `my_key.pub` **Important** Asegúrese de usar la clave pública y no la clave privada. `aws ec2-instance-connect send-ssh-public-key \ --instance-id $INSTANCE_ID \ --instance-os-user ec2-user \ --ssh-public-key file://$PUBLIC_KEY_FILE` 2. Espere hasta que reciba un mensaje que indique que la clave se ha cargado correctamente. Continúe inmediatamente al siguiente paso.	

Tarea	Descripción	Habilidades requeridas
Conéctese al host bastión.	1. Por ejemplo, introduzca el siguiente comando para conectarse al host bastión a través de Session Manager, donde: • `$PRIVATE_KEY_FILE` es la ruta a su clave privada, como `my_key` • `$INSTANCE_ID` es el ID de la EC2 instancia de Amazon `ssh -i $PRIVATE_KEY_FILE ec2-user@$INSTANCE_ID` 2. Confirme la conexión introduciendo `yes`. Esto abre una conexión SSH mediante Session Manager. **Note** Existen otras opciones para abrir una conexión SSH con el host bastión. Para obtener más información, consulte Enfoques alternativos para establecer una conexión SSH con el host bastión en la sección de Informaci	AWS general

Tarea	Descripción	Habilidades requeridas
	ón adicional de este patrón.	

(Opcional) Limpieza

Tarea	Descripción	Habilidades requeridas
Elimine los recursos implementados.	1. Para eliminar todos los recursos implement ados, ejecute el siguiente comando del directorio raíz del repositorio clonado. `terraform destroy -var-file="dev.tfvars"` 2. Confirme la eliminación de los recursos.	DevOps ingeniero, desarroll ador, Terraform

Resolución de problemas

Problema	Solución
`TargetNotConnected` error al intentar conectarse al host bastión	1. Reinicia el host bastión según las instrucci ones de Reinicia tu instancia en la EC2 documentación de Amazon. 2. Cuando la instancia se haya reiniciado correctamente, vuelva a enviar la clave pública al host bastión y vuelva a intentar la conexión.
`Permission denied` error al intentar conectarse al host bastión	Una vez cargada la clave pública en el host bastión, solo dispondrá de 60 segundos para

Problema	Solución
	iniciar la conexión. Transcurridos 60 segundos, la clave se elimina automáticamente y no puede usarla para conectarse a la instancia. Si esto ocurre, puede repetir el paso para volver a enviar la clave a la instancia.

Recursos relacionados

AWS documentación

- AWS Systems Manager Session Manager (documentación de Systems Manager)
- Instalación del plugin de Session Manager para la AWS CLI (documentación de Systems Manager)
- Permitir conexiones SSH para Session Manager (documentación de Systems Manager)
- Acerca del uso de EC2 Instance Connect (EC2 documentación de Amazon)
- Conéctese mediante EC2 Instance Connect (EC2 documentación de Amazon)
- Gestión de identidad y acceso para Amazon EC2 (EC2 documentación de Amazon)
- Uso de una función de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon (documentación de IAM)
- Prácticas recomendadas de seguridad en IAM (documentación de IAM)
- Control del tráfico hacia los recursos mediante grupos de seguridad (documentación de Amazon VPC)

Otros recursos

- Página web para desarrolladores de Terraform
- Comando: validar (documentación de Terraform)
- Comando: fmt (documentación de Terraform)
- Probando HashiCorp Terraform (entrada de blog) HashiCorp
- Página web Checkov

Información adicional

Enfoques alternativos para establecer una conexión SSH con el host bastión

Enrutamiento de puertos

Puede usar la opción `-D 8888` para abrir una conexión SSH con reenvío dinámico de puertos. Para más información, consulte las instrucciones en explainshell.com. El siguiente es un ejemplo de un comando para abrir una conexión SSH mediante el reenvío de puertos.

```
ssh -i $PRIVATE_KEY_FILE -D 8888 ec2-user@$INSTANCE_ID
```

Este tipo de conexión abre un proxy SOCKS que puede reenviar el tráfico de su navegador local a través del host bastión. Si utiliza Linux o macOS, para ver todas las opciones, introduzca `man ssh`. Se mostrará el manual de referencia de SSH.

Uso del script proporcionado

En lugar de ejecutar manualmente los pasos descritos en Conectar al host bastión mediante Session Manager en la sección Epics, puede utilizar el script connect.sh incluido en el repositorio de código. Este script genera el par de claves SSH, envía la clave pública a la EC2 instancia de Amazon e inicia una conexión con el host del bastión. Al ejecutar el script, se pasan la etiqueta y el nombre de la clave como argumentos. A continuación se muestra un ejemplo del comando para ejecutar el script.

```
./connect.sh sandbox-dev-bastion-host my_key
```

Centralice la resolución de DNS mediante AWS Managed Microsoft AD Microsoft Active Directory local

Brian Westmoreland, Amazon Web Services

Resumen

Este patrón proporciona orientación para centralizar la resolución de DNS en un entorno de AWS varias cuentas mediante AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) y Amazon Route 53. En este patrón, el espacio de nombres AWS DNS es un subdominio del espacio de nombres DNS local. Este patrón también proporciona instrucciones sobre cómo configurar los servidores DNS locales para que reenvíen consultas AWS cuando la solución DNS local utilice Microsoft Active Directory.

Requisitos previos y limitaciones

Requisitos previos

- Un entorno AWS de varias cuentas configurado mediante. AWS Organizations
- Conectividad de red establecida entre Cuentas de AWS.
- Conectividad de red establecida entre el entorno local AWS y el entorno local (mediante el uso de AWS Direct Connect cualquier tipo de conexión VPN).
- AWS Command Line Interface (AWS CLI) configurado en una estación de trabajo local.
- AWS Resource Access Manager (AWS RAM) se utiliza para compartir las reglas de Route 53 entre cuentas. Por lo tanto, el uso compartido debe estar habilitado en el AWS Organizations entorno, como se describe en la sección Epics.

Limitaciones

- AWS Managed Microsoft AD La Edición Estándar tiene un límite de 5 acciones.
- AWS Managed Microsoft AD La Edición Enterprise tiene un límite de 125 acciones.
- La solución de este patrón se limita a Regiones de AWS que el soporte se comparta a través de él AWS RAM.

Versiones de producto

- Microsoft Active Directory ejecutado en Windows Server 2008, 2012, 2012 R2 o 2016.

Arquitectura

Arquitectura de destino

En este diseño, AWS Managed Microsoft AD se instala en los servicios compartidos Cuenta de AWS. Si bien no es un requisito, este patrón presupone dicha configuración. Si lo configuras AWS Managed Microsoft AD de forma diferente Cuenta de AWS, es posible que tengas que modificar los pasos de la sección Epics en consecuencia.

Este diseño emplea Route 53 Resolvers para admitir la resolución de nombres mediante el uso de reglas de Route 53. Si la solución de DNS en las instalaciones usa Microsoft DNS, no es fácil crear una regla de reenvío condicional para el espacio de nombres de AWS (`aws.company.com`), que es un subdominio del espacio de nombres DNS (`company.com`) de la empresa. Si intenta crear un reenviador condicional tradicional, se producirá un error. Esto se debe a que Microsoft Active Directory ya se considera autorizado para cualquier subdominio de `company.com`. Para evitar este error, primero debe crear una delegación para `aws.company.com` que permita delegar la autoridad de ese espacio de nombres. A continuación, puede crear el reenviador condicional.

La nube privada virtual (VPC) de cada cuenta radial puede tener su propio espacio de nombres DNS único basado en el espacio de nombres raíz. AWS En este diseño, cada cuenta radial añade una abreviatura del nombre de cuenta al espacio de nombres base de AWS. Una vez creadas las zonas alojadas privadas en la cuenta de radio, las zonas se asocian a la VPC local de la cuenta de radio y a la VPC de la cuenta de red central. AWS Esto permite que la cuenta de AWS red central responda a las consultas de DNS relacionadas con las cuentas de radio. De esta manera, tanto Route 53 como Route 53 AWS Managed Microsoft AD trabajan juntos para compartir la responsabilidad de administrar el espacio de AWS nombres ()`aws.company.com`.

Automatización y escala

Este diseño utiliza los puntos finales de Route 53 Resolver para escalar las consultas de DNS entre el entorno local AWS y el entorno local. Cada punto de conexión de Route 53 Resolver incluye varias interfaces de red elásticas (distribuidas en varias zonas de disponibilidad), y cada interfaz de red puede gestionar hasta 10 000 consultas por segundo. Route 53 Resolver admite hasta 6 direcciones IP por punto de conexión, por lo que, en total, este diseño admite hasta 60 000 consultas de DNS por segundo distribuidas en varias zonas de disponibilidad para lograr una alta disponibilidad.

Además, este patrón tiene en cuenta automáticamente el crecimiento futuro en AWS. No es necesario modificar las reglas de reenvío de DNS configuradas localmente para que sean

compatibles con las zonas alojadas privadas nuevas VPCs y las asociadas que se agreguen a ellas. AWS

Tools (Herramientas)

Servicios de AWS

- AWS Directory Service for Microsoft Active Directorypermite que sus cargas de trabajo y AWS recursos compatibles con directorios utilicen Microsoft Active Directory en. Nube de AWS
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar varias cuentas Cuentas de AWS en una organización que puede crear y administrar de forma centralizada.
- AWS Resource Access Manager (AWS RAM) le ayuda a compartir sus recursos de forma segura Cuentas de AWS para reducir la sobrecarga operativa y ofrecer visibilidad y capacidad de auditoría.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.

Herramientas

- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que te ayuda a interactuar Servicios de AWS mediante los comandos de tu consola de línea de comandos. En este patrón, AWS CLI se usa para configurar las autorizaciones de Route 53.

Epics

Cree y comparta un directorio AWS Managed Microsoft AD

Tarea	Descripción	Habilidades requeridas
Implementar AWS Managed Microsoft AD.	1. Crear y configurar un nuevo directorio. Para ver los pasos detallados, consulte Cree su AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service .	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	2. Registre las direcciones IP de los controladores de AWS Managed Microsoft AD dominio. Se emplearán en un paso posterior.	
Compartir el directorio.	Una vez creado el directorio, compártalo con otros miembros Cuentas de AWS de la AWS organización. Para obtener más instrucciones, consulte Cómo compartir su directorio en la Guía de administración de AWS Directory Service . **Note** AWS Managed Microsoft AD La Edición Estándar tiene un límite de 5 acciones. La Edición Enterprise tiene un límite de 125 acciones.	Administrador de AWS

Configure Route 53

Tarea	Descripción	Habilidades requeridas
Cree Route 53 Resolvers.	Los solucionadores Route 53 facilitan la resolución de consultas de DNS entre el	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	centro de datos local AWS y el centro de datos local. 1. Instale Route 53 Resolvers siguiendo las instrucciones de la Guía del desarrollador de Route 53. 2. Configure los resolvers de Route 53 en subredes privadas de al menos dos zonas de disponibilidad dentro de la VPC de la cuenta de AWS red central para obtener una alta disponibilidad. **Note** Si bien el uso de la VPC de la cuenta de AWS red central no es obligatorio, en los pasos restantes se asume esta configura ción.	

Tarea	Descripción	Habilidades requeridas

Cree reglas de Route 53.	Es posible que su caso de uso específico requiera una gran cantidad de reglas de Route 53, pero tendrá que configurar las siguientes reglas como base:
	• Una regla de salida para el espacio de nombres en las instalaciones (`company.com`) mediante el uso de instancias de Route 53 Resolver de salida de la cuenta de red central. Las direcciones IP de destino son los servidores DNS en las instalaciones.
	  • Asocie esta regla a la VPC de la cuenta de red central.
	• Una regla de salida para el espacio de AWS nombres (`aws.company.com`) mediante la cuenta de red central Outbound Route 53 Resolvers. Las direcciones IP de destino son las direcciones IP entrantes de Route 53 Resolver de la cuenta de red central.
	  • No asocie esta regla a la cuenta de AWS red central VPC (que alberga los Route 53 Resolvers).
		Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	• Una segunda regla de salida para el espacio de AWS nombres (`aws.company.com`) que apunta a los controladores de AWS Managed Microsoft AD dominio (utilice la IPs de la epopeya anterior).
	  • Asocie esta regla a la cuenta de AWS red central VPC (que aloja los Route 53 Resolvers).
	  • No comparta ni asocie esta regla con otras Cuentas de AWS.
	
	Para más información, consulte Gestión de reglas de reenvío en la Guía del desarrollador de Route 53.	

Tarea	Descripción	Habilidades requeridas
Configure un perfil de Route 53.	Puede usar un perfil de Route 53 para compartir las reglas con las cuentas de radio. 1. Cree un nuevo perfil de Route 53 en la cuenta de red central siguiendo las instrucciones de la Guía para desarrolladores de Route 53. 2. Agregue la regla para el espacio de nombres en las instalaciones (`company.com`) al perfil. 3. Agregue al perfil la primera regla para el espacio de AWS nombres (`aws.company.com`), que apunta a las direcciones IP de los resolutores entrantes de Route 53. 4. Comparta el perfil de Route 53 con la organización. AWS 5. Acepte el recurso compartido del perfil de Route 53 en cada cuenta radial. 6. Asocie el perfil de Route 53 a cada VPC de cuenta radial.	Administrador de AWS

Configure el DNS de Active Directory en las instalaciones

Tarea	Descripción	Habilidades requeridas
Cree la delegación.	Use el complemento DNS de Microsoft (`dnsmgmt.msc`) para crear una nueva delegación para el espacio de nombres `company.com` de Active Directory. El nombre del dominio delegado debe ser `aws`. Esto lo convierte en el nombre completo del dominio (FQDN) de la delegación `aws.company.com`. Utilice las direcciones IP de los controladores de dominio para los valores de IP del servidor de nombres y `server.aws.company.com` utilícelas para el nombre. (Esta delegación solo se usa en la redundancia, ya que se creará un reenviador condicional para este espacio de nombres que tendrá prioridad sobre la delegación).	Active Directory
Cree el reenviador condicional.	Use el complemento DNS de Microsoft (`dnsmgmt.msc`) para crear un nuevo reenviador condicional para `aws.company.com`. Utilice las direcciones IP de los AWS Route 53 Resolvers entrantes del DNS Cuenta de AWS central	Active Directory

Tarea	Descripción	Habilidades requeridas
	como destino del reenviador condicional.	

Cree zonas alojadas privadas de Route 53 para los radios Cuentas de AWS

Tarea	Descripción	Habilidades requeridas
Cree las zonas alojadas privadas de Route 53.	Crear una zona alojada privada de Route 53 en cada cuenta radial. Asocie esta zona alojada privada con la VPC de la cuenta radial. Para ver los pasos detallados, consulte Crear una zona alojada privada en la Guía del desarrollador de Route 53.	Administrador de AWS
Cree autorizaciones.	Utilice el AWS CLI para crear una autorización para la VPC de la cuenta AWS de red central. Ejecute este comando desde el contexto de cada Cuenta de AWS radial: `aws route53 create-vpc-association-authorization --hosted-zone-id <hosted-zone-id> \ --vpc VPCRegion=<region>,VPCId=<vpc-id>` donde:	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	• <hosted-zone-id> es la zona alojada privada de Route 53 en la cuenta radial. • <region>y <vpc-id> son el Región de AWS ID de VPC de la cuenta de AWS red central VPC.	
Cree asociaciones.	Cree la asociación de zonas alojadas privadas de Route 53 para la VPC de la cuenta de AWS red central mediante. AWS CLI Ejecute este comando desde el contexto de la cuenta de AWS red central: `aws route53 associate-vpc-with-hosted-zone --hosted-zone-id <hosted-zone-id> \ --vpc VPCRegion=<region>,VPCId=<vpc-id>` donde: • <hosted-zone-id> es la zona alojada privada de Route 53 en la cuenta radial. • <region>y <vpc-id> son el Región de AWS ID de VPC de la cuenta de AWS red central.	Administrador de AWS

Recursos relacionados

- Simplifique la administración del DNS en un entorno con varias cuentas con Route 53 Resolver (AWS entrada del blog)
- Creando su AWS Managed Microsoft AD (AWS Directory Service documentación)
- Compartir un AWS Managed Microsoft AD directorio (AWS Directory Service documentación)
- ¿Qué es Amazon Route 53 Resolver? (Documentación de Amazon Route 53)
- Creación de una zona alojada privada (documentación de Amazon Route 53)
- Qué es Perfiles de Amazon Route 53? (Documentación de Amazon Route 53)

Centralice la supervisión mediante Amazon CloudWatch Observability Access Manager

Anand Krishna Varanasi, JAGDISH KOMAKULA, Ashish Kumar, Jimmy Morgan, Sarat Chandra Pothula, Vivek Thangamuthu y Balaji Vedagiri, Amazon Web Services

Resumen

La observabilidad es fundamental para la supervisión, la comprensión y la solución de problemas de las aplicaciones. Las aplicaciones que abarcan varias cuentas, como las AWS Control Tower implementaciones de landing zone, generan una gran cantidad de registros y datos de rastreo. Para solucionar problemas rápidamente o comprender los análisis de usuarios o empresariales, necesita una plataforma de observabilidad común en todas las cuentas. El Amazon CloudWatch Observability Access Manager le permite acceder a varios registros de cuentas y controlarlos desde una ubicación central.

Puede usar Observability Access Manager para ver y administrar los registros de datos de observabilidad generados por las cuentas de origen. Las cuentas de origen son individuales y Cuentas de AWS generan datos de observabilidad para sus recursos. Las cuentas de origen comparten sus datos de observabilidad con la cuenta de monitoreo. Los datos de observabilidad compartidos pueden incluir métricas en Amazon CloudWatch, registros en Amazon CloudWatch Logs y rastreos. AWS X-Ray Para más información, consulte la documentación de Observability Access Manager.

Este patrón es para los usuarios que tienen aplicaciones o infraestructuras que se ejecutan en varias direcciones Cuentas de AWS y necesitan un lugar común para ver los registros. En él se explica cómo puede configurar Observability Access Manager mediante Terraform para supervisar el estado y el estado de estas aplicaciones o infraestructuras. Puede instalar esta solución de varias maneras:

- Como un módulo Terraform independiente que puede configurar manualmente
- Mediante el uso de una canalización de integración y entrega continuas (CI/CD)
- Mediante la integración con otras soluciones, como Generador de cuentas para Terraform (AFT) de AWS Control Tower

Las instrucciones de la sección Epics tratan sobre la implementación manual. Para ver los pasos de instalación de AFT, consulte el archivo README del repositorio de GitHub Observability Access Manager.

Requisitos previos y limitaciones

Requisitos previos

- Terraform está instalado o referenciado en su sistema o en canalizaciones automatizadas. (Le recomendamos que utilice la última versión.)
- Una cuenta que puede usar como cuenta de monitoreo central. Otras cuentas crean enlaces a la cuenta de monitoreo central para ver los registros.
- (Opcional) Un repositorio de código fuente como GitHub Atlassian Bitbucket o un sistema similar. AWS CodeCommit No es necesario disponer de un repositorio de código fuente si utilizas canalizaciones automatizadas. CI/CD
- (Opcional) Permisos para crear solicitudes de cambios (PRs) para revisar el código y colaborar con él. GitHub

Limitaciones

Observability Access Manager tiene las siguientes Service quotas, que no se pueden cambiar. Tenga en cuenta estas cuotas antes de implementar esta característica. Para obtener más información, consulta las cuotas de CloudWatch servicio en la CloudWatch documentación.

- Vínculos de cuentas de origen: puede vincular cada cuenta de origen a un máximo de cinco cuentas de supervisión.
- Depósitos: puedes crear varios depósitos para una cuenta, pero solo Región de AWS se permite un depósito por cuenta.

Además:

- Los sumideros y los enlaces deben crearse de la misma manera Región de AWS; no pueden ser de una región a otra.

Supervisión entre cuentas y entre regiones

Para la supervisión entre regiones y cuentas, puede elegir una de las siguientes opciones:

- Cree CloudWatch paneles de control multicuentas y regiones para alarmas y métricas. Esta opción no admite registros ni rastreos.
- Implemente el registro centralizado mediante Amazon OpenSearch Service.

- Cree un colector por región a partir de todas las cuentas de los inquilinos, transfiera las métricas a una cuenta de supervisión centralizada (como se describe en este patrón) y, a continuación, utilice los flujos de CloudWatch métricas para enviar los datos a un destino externo común o a productos de supervisión de terceros, como Datadog, Dynatrace, Sumo Logic, Splunk o New Relic.

Arquitectura

Componentes

CloudWatch Observability Access Manager consta de dos componentes principales que permiten la observabilidad entre cuentas:

- Un receptor permite a las cuentas de origen enviar datos de observabilidad a la cuenta de monitoreo central. Básicamente, un receptor proporciona una puerta de enlace a la que se pueden conectar las cuentas de origen. Solo puede haber una puerta de enlace o conexión receptora y varias cuentas pueden conectarse a ella.
- Cada cuenta de origen tiene un enlace al cruce de la puerta de enlace receptora y los datos de observabilidad se envían a través de este enlace. Debe crear un receptor antes de crear enlaces desde cada cuenta de origen.

Arquitectura

El siguiente diagrama ilustra Observability Access Manager y sus componentes.

Tools (Herramientas)

Servicios de AWS

- Amazon le CloudWatch ayuda a supervisar las métricas de sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar múltiples cuentas Cuentas de AWS en una organización que usted crea y administra de forma centralizada.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.

Herramientas

- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.
- AWS Control Tower Account Factory for Terraform (AFT) configura una canalización de Terraform para ayudarte a aprovisionar y personalizar las cuentas. AWS Control Tower Si lo desea, puede utilizar AFT para configurar Observability Access Manager de forma escalable en varias cuentas.

Repositorio de código

El código de este patrón está disponible en el repositorio de GitHub Observability Access Manager.

Prácticas recomendadas

- En AWS Control Tower los entornos, marque la cuenta de registro como la cuenta de supervisión central (receptáculo).
- Si tiene varias organizaciones con varias cuentas AWS Organizations, le recomendamos que incluya las organizaciones en lugar de las cuentas individuales en la política de configuración. Si tiene un número reducido de cuentas o si las cuentas no forman parte de una organización en la política de configuración de destino, puede optar por incluir cuentas individuales en su lugar.

Epics

Configure el módulo de receptor

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Clona el repositorio GitHub de Observability Access Manager: `git clone https://github.com/aws-samples/cloudwatch-observability-access-manager-terraform`	AWS DevOps, administrador de la nube, administrador de AWS
Especifique los valores de las propiedades del módulo receptor.	En el archivo `main.tf` (en la carpeta `deployments/aft-account-cus`	AWS DevOps, administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	`tomizations/LOGGIN G/terraform/` del repositorio), especifique los valores de las siguientes propiedades: • `sink_name` : El nombre del CloudWatch sumidero. • `allowed_oam_resour ce_types` : Observability Access Manager admite actualmente CloudWatc h métricas, grupos de registros y AWS X-Ray rastreos. • `allowed_source_acc ounts` : Las cuentas de origen que pueden enviar registros a la cuenta receptora CloudWatch central. • `allowed_source_org anizations` : Las AWS Control Tower organizac iones de origen a las que se les permite enviar registros a la cuenta CloudWatch receptora central. Para obtener más información, consulte AWS::Oam::Sinkla CloudFormation documenta ción.	

Tarea	Descripción	Habilidades requeridas

Instale el módulo receptor.	Exporte las credenciales de la cuenta Cuenta de AWS que haya seleccionado como cuenta de monitoreo e instale el módulo receptor Observability Access Manager:
	`Terraform Init`
	`Terrafom Plan`
	`Terraform Apply`
		AWS DevOps, administrador de la nube, administrador de AWS

Configure el módulo receptor

Tarea	Descripción	Habilidades requeridas

Especifique los valores de las propiedades del módulo de enlace.	En el archivo `main.tf` (en la carpeta `deployments/aft-account-customizations/LOGGING/terraform/` del repositorio), especifique los valores de las siguientes propiedades:
	• `account_label` : utilice uno de los siguientes valores:
	  • `$AccountName` : el nombre de la cuenta.
	  • `$AccountEmail` : una dirección de correo electrónico única a nivel mundial, que incluye el dominio del correo
		AWS DevOps, administrador de nube, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	electrónico (por ejemplo, `hello@example.com`) • `$AccountEmailNoDomain` : una dirección de correo electrónico sin el nombre de dominio. • `allowed_oam_resource_types` : Observability Access Manager admite actualmente CloudWatch métricas, grupos de registros y AWS X-Ray rastreos. Para obtener más información, consulte AWS::Oam::Link la CloudFormation documentación.	

Instale el módulo de enlace para cuentas individuales.	Exporte las credenciales de las cuentas individuales e instale el módulo de enlace Observability Access Manager:
	
	`Terraform Plan`
	`Terraform Apply`
	
	Puede configurar el módulo de enlace de forma individual para cada cuenta o usar AFT para instalar automáticamente este módulo en una gran cantidad de cuentas.
		AWS DevOps, administrador de nube, arquitecto de nube

Apruebe sink-to-link las conexiones

Tarea	Descripción	Habilidades requeridas
Verifique el mensaje del estado.	1. Inicie sesión en la cuenta de supervisión. 2. Abra la consola de CloudWatch . 3. En el panel de navegación izquierdo, elija Configuración. A la derecha, debería ver el mensaje de estado Supervisar la cuenta con una cuenta habilitada con una marca de verificación verde. Esto significa que la cuenta de monitoreo tiene un receptor de Observability Access Manager al que se conectarán los enlaces de otras cuentas.	
Apruebe las link-to-sink conexiones.	1. Elija la opción Recursos para vincular cuentas situada debajo del mensaje de estado. La información confirma que se trata de la cuenta de monitoreo, muestra los datos que se comparten desde las cuentas de origen del inquilino (registros, métricas, rastreos) y muestra la etiqueta de la	AWS DevOps, administrador de nube, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	cuenta como $AccountName. Esta pantalla ofrece dos opciones para vincular las cuentas de los inquilinos a la cuenta de monitoreo : aprobación a nivel de organización o aprobación a nivel de cuenta. Para cada opción, puede elegir entre descargar una CloudFormation plantilla para la aprobación o aprobar cada cuenta de forma individual. 2. Para simplificar, elija Cualquier cuenta para aprobarla en cada nivel de cuenta. Esta opción proporciona un enlace de aprobación para la cuenta. 3. Seleccione Copiar URL para copiar el enlace. 4. Inicie sesión en cada cuenta de origen. 5. En una ventana del navegador, pegue el enlace y seleccione Aprobar enlace conectar con el receptor. 6. Repita la operación para todas las demás cuentas de origen.	

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte Vincular las cuentas de supervisión con las cuentas de origen en la CloudWatch documentación.	

Verificar los datos de observabilidad entre cuentas

Tarea	Descripción	Habilidades requeridas
Ver datos entre cuentas.	1. Inicie sesión en la cuenta central de monitoreo. 2. Abra la consola de CloudWatch . 3. En el panel de navegación izquierdo, elija las opciones para ver los registros, las métricas y los seguimientos entre cuentas.	AWS DevOps, administrador de nube, arquitecto de nube

(Opcional) Habilite las cuentas de origen para que confíen en la cuenta de monitoreo

Tarea	Descripción	Habilidades requeridas
Consulte las métricas, los paneles, los registros, los widgets y las alarmas de otras cuentas.	Como función adicional, puede compartir CloudWatch las métricas, los paneles, los registros, los widgets y las alarmas con otras cuentas. Cada cuenta utiliza un rol de IAM denominado CloudWatch: CrossAccountSharingRole para acceder a estos datos.	AWS DevOps, administrador de nube, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	Las cuentas de origen que tienen una relación de confianza con la cuenta de supervisión central pueden asumir esta función y ver los datos de la cuenta de supervisión. CloudWatch proporciona un ejemplo de CloudFormation script para crear el rol. Elija Administrar el rol en IAM y ejecute este script en las cuentas en las que desee ver los datos. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": [ "arn:aws:iam::XXXXXXXXXX:root", "arn:aws:iam::XXXXXXXXXX:root", "arn:aws:iam::XXXXXXXXXX:root", "arn:aws:iam::XXXXXXXXXX:root" ]`	

Tarea	Descripción	Habilidades requeridas

	<pre> },
	            "Action":
	"sts:AssumeRole"
	        }
	    ]
	}</pre>
	Para obtener más información, consulte Habilitar la funcionalidad multicuenta CloudWatch en la CloudWatch documentación.	

(Opcional) Ver las cuentas y Regiones cruzadas desde la cuenta de monitoreo

Tarea	Descripción	Habilidades requeridas
Configuración del acceso entre cuentas y regiones.	En la cuenta de supervisión central, si lo desea, puede añadir un selector de cuentas para cambiar fácilmente de una cuenta a otra y ver sus datos sin tener que autenticarse. 1. Inicie sesión en la cuenta central de monitoreo. 2. Abra la consola de CloudWatch . 3. En el panel de navegación izquierdo, elija Configuración. 4. En la sección Ver varias cuentas en todas las	AWS DevOps, administrador de nube, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	regiones, seleccione Configure (Configurar). 5. Seleccione Activar y, a continuación, seleccione la casilla Mostrar el selector en la consola. 6. Elija una de estas opciones: • Introducir el identific ador de cuenta: esta opción le pide que introduzca manualmen te el identificador de la cuenta siempre que desee cambiar de cuenta para ver los datos de varias cuentas. • Selector de cuentas de AWS Organization: si se ha integrado CloudWatch con AWS Organizations, esta opción proporciona un selector desplegable con una lista completa de las cuentas de la organización. • Selector de cuentas personalizado: esta opción le permite introducir manualmen te una lista de cuentas IDs para completar el selector. 7. Seleccione Save changes (Guardar cambios).	

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte la CloudWatch consola multicuentas y regiones en la documentación. CloudWatch	

Recursos relacionados

- CloudWatch observabilidad entre cuentas (documentación de Amazon CloudWatch)
- Referencia de la API de Amazon CloudWatch Observability Access Manager (CloudWatch documentación de Amazon)
- Recurso: aws_oam_sink (documentación de Terraform)
- Origen de datos: aws_oam_link (documentación de Terraform)
- CloudWatchObservabilityAccessManager(documentación de AWS Boto3)

Comprueba EC2 las instancias para ver si hay etiquetas obligatorias en el lanzamiento

Susanne Kangnoh y Archit Mathur, Amazon Web Services

Resumen

Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de Amazon Web Services (AWS). El uso de Amazon EC2 elimina la necesidad de invertir en hardware por adelantado, por lo que puede desarrollar e implementar aplicaciones más rápido.

Puede usar el etiquetado para categorizar los recursos de AWS de diferentes maneras. EC2 El etiquetado de instancias resulta útil cuando tiene muchos recursos en su cuenta y quiere identificar rápidamente un recurso específico en función de las etiquetas. Puedes asignar metadatos personalizados a tus EC2 instancias mediante etiquetas. Una etiqueta es una marca que consta de una clave y un valor definidos por el usuario. Le recomendamos que cree un conjunto de etiquetas coherente para satisfacer los requisitos de su organización.

Este patrón proporciona una CloudFormation plantilla de AWS que le ayuda a supervisar EC2 las instancias para etiquetas específicas. La plantilla crea un evento de Amazon CloudWatch Events que vigila los UntagResourceeventos de AWS para detectar el etiquetado CloudTrail TagResourceo la eliminación de etiquetas de nuevas EC2 instancias. Si falta una etiqueta predefinida, llama una función de AWS Lambda, que envía un mensaje de infracción a la dirección de correo electrónico que usted proporcione mediante Amazon Simple Notification Service (Amazon SNS).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Cargue el código de Lambda proporcionado en un bucket de Amazon Simple Storage Service (Amazon S3).
- Una dirección de correo electrónico en la que desee recibir las notificaciones de infracciones.

Limitaciones

- Esta solución es compatible con CloudTrail TagResourcenuestros UntagResourceeventos. No crea notificaciones para ningún otro evento.

- Esta solución solo comprueba las claves de las etiquetas. No supervisa los valores clave.

Arquitectura

Arquitectura de flujo de trabajo

Automatización y escala

- Puede utilizar la CloudFormation plantilla de AWS varias veces para distintas regiones y cuentas de AWS. Debe ejecutar la plantilla solo una vez en cada región o cuenta.

Tools (Herramientas)

Servicios de AWS

- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona una capacidad informática segura y de tamaño variable en la nube. Se ha diseñado para facilitar a los desarrolladores la computación en la nube en la Web.
- AWS CloudTrail: CloudTrail es un servicio de AWS que le ayuda con la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de su cuenta de AWS. Las acciones realizadas por un usuario, un rol o un servicio de AWS se registran como eventos en CloudTrail.
- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS. CloudWatch Events se da cuenta de los cambios operativos a medida que se producen y toma las medidas correctivas necesarias, mediante el envío de mensajes en respuesta al entorno, la activación de funciones, la introducción de cambios y la recopilación de información sobre el estado.
- AWS Lambda: Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable que se puede utilizar para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio web que permite a las aplicaciones, los usuarios finales y los dispositivos enviar y recibir al instante notificaciones desde la nube.

Codigo

Este patrón incluye un adjunto con dos archivos:

- `index.zip` es un archivo comprimido que incluye el código de Lambda de este patrón.
- `ec2-require-tags.yaml`es una CloudFormation plantilla que despliega el código Lambda.

Consulte la sección Epics para obtener información sobre cómo usar estos archivos.

Epics

Implementar el código de Lambda

Tarea	Descripción	Habilidades requeridas
Cargue el código en un bucket de S3.	Cree un bucket de S3 nuevo o utilice un bucket de S3 ya existente para cargar el archivo adjunto `index.zip` (código de Lambda). Este depósito debe estar en la misma región de AWS que los recursos (EC2 instancias) que desee supervisar.	Arquitecto de la nube
Implemente la CloudFormation plantilla.	Abra la consola de Cloudform ation en la misma región de AWS que el bucket de S3 e implemente el archivo `ec2-require-tags.yaml` que se incluye en el archivo adjunto. En la siguiente Epic, proporcione los valores de los parámetros.	Arquitecto de la nube

Complete los parámetros de la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Proporcione el nombre del bucket de S3.	Escriba el nombre del bucket de S3 que ha creado o seleccionado en la primera Epic. Este bucket de S3 contiene el archivo.zip del código Lambda y debe estar en la misma región de AWS que CloudFormation la plantilla y EC2 las instancias que desea monitorear.	Arquitecto de la nube
Proporcione la clave de S3.	Proporcione la ubicación del archivo .zip del código de Lambda en su bucket de S3, sin barras diagonales iniciales (por ejemplo, `index.zip` o `controls/index.zip`).	Arquitecto de la nube
Proporcione una dirección de correo electrónico.	Proporcione una dirección de correo electrónico activa en la que desee recibir notificac iones de infracciones.	Arquitecto de la nube
Defina un nivel de registro.	Especifique el nivel de registro y el detalle. `Info` designa mensajes informativos detallados sobre el progreso de la aplicación y solo debe usarse para la depuración. `Error` designa los eventos de error que aún podrían permitir que la aplicación siguiera ejecutándose. `Warning`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	designa situaciones potencial mente dañinas.	
Ingrese las claves de etiqueta requeridas.	Escriba las claves de etiqueta que desea comprobar. Si desea especificar varias claves, sepárelas con comas, sin espacios. (Por ejemplo, `ApplicationId,Crea tedBy,Environment, Organization` busca cuatro claves). El evento CloudWatch Events busca estas claves de etiquetas y envía una notificación si no las encuentra.	Arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirme la suscripción de correo electrónico.	Cuando la CloudFormation plantilla se implementa correctamente, envía un mensaje de correo electrónico de suscripción a la dirección de correo electrónico que has proporcionado. Debe confirmar esta suscripción de correo electrónico para recibir notificaciones.	Arquitecto de la nube

Recursos relacionados

- Creación de un bucket (documentación de Amazon S3)
- Carga de objetos (documentación de Amazon S3)
- Etiquete sus EC2 recursos de Amazon (EC2 documentación de Amazon)
- Creación de una regla de CloudWatch eventos que se active en una llamada a la API de AWS mediante AWS CloudTrail (CloudWatch documentación de Amazon)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Limpie los recursos de AWS Account Factory for Terraform (AFT) de forma segura después de la pérdida de archivos estatales

Gokendra Malviya, Amazon Web Services

Resumen

Cuando usa AWS Account Factory for Terraform (AFT) para administrar su AWS Control Tower entorno, AFT genera un archivo de estado de Terraform para rastrear el estado y la configuración de los recursos creados por Terraform. La pérdida del archivo de estado de Terraform puede suponer importantes desafíos para la administración y limpieza de los recursos. Este patrón proporciona un enfoque sistemático para identificar y eliminar de forma segura los recursos relacionados con la AFT y, al mismo tiempo, mantener la integridad de su entorno. AWS Control Tower

El proceso está diseñado para garantizar la eliminación adecuada de todos los componentes de AFT, incluso sin la referencia del archivo de estado original. Este proceso proporciona un camino claro para restablecer y reconfigurar correctamente la AFT en su entorno, a fin de garantizar una interrupción mínima de sus operaciones. AWS Control Tower

Para obtener más información sobre AFT, consulte la documentación de AWS Control Tower.

Requisitos previos y limitaciones

Requisitos previos

- Un conocimiento detallado de la arquitectura de AFT.
- Acceso de administrador a las siguientes cuentas:
  - Cuenta de administración de AFT
  - AWS Control Tower Cuenta de administración
  - Cuenta del archivo de registro
  - Cuenta de auditoría
- Verificación de que ninguna política de control de servicios (SCPs) contiene restricciones o limitaciones que puedan bloquear la eliminación de los recursos relacionados con AFT.

Limitaciones

- Este proceso puede limpiar los recursos de forma eficaz, pero no puede recuperar los archivos de estado perdidos, y algunos recursos pueden requerir una identificación manual.

- La duración del proceso de limpieza depende de la complejidad del entorno y puede tardar varias horas.
- Este patrón se probó con la versión 1.12.2 de AFT y elimina los siguientes recursos. Si está utilizando una versión diferente de AFT, es posible que deba eliminar recursos adicionales.

Nombre del servicio	Número de recursos
AWS CodeBuild	6
AWS CodeCommit	4
AWS CodePipeline	4
Amazon DynamoDB	5
Amazon Elastic Compute Cloud (Amazon EC2)	16
Amazon EventBridge	4
AWS Identity and Access Management (IAM) funciones	40
AWS Key Management Service (AWS KMS)	2
AWS Lambda	17
Amazon Simple Storage Service (Amazon S3)	2
Amazon Simple Notification Service (Amazon SNS)	2
Amazon Simple Queue Service (Amazon SQS)	2
AWS Systems Manager	62
AWS Step Functions	4

> **Important**
>
> Los recursos que se eliminan mediante los pasos de este patrón no se pueden recuperar. Antes de seguir estos pasos, compruebe cuidadosamente los nombres de los recursos y asegúrese de que fueron creados por AFT.

Arquitectura

En el siguiente diagrama se muestran los componentes de AFT y el flujo de trabajo de alto nivel. AFT configura una canalización de Terraform que le ayuda a aprovisionar y personalizar varias cuentas de AWS Control Tower. AFT sigue un GitOps modelo para automatizar los procesos de aprovisionamiento de cuentas en. AWS Control Tower Puede crear un archivo de Terraform para una solicitud de cuenta y confirmarlo en un repositorio, que proporciona la entrada que activa el flujo de trabajo de AFT para el aprovisionamiento de la cuenta. Una vez completado el aprovisionamiento de la cuenta, AFT puede ejecutar automáticamente pasos de personalización adicionales.

En esta arquitectura:

- AWS Control Tower La cuenta de administración es una Cuenta de AWS que está dedicada al AWS Control Tower servicio. Por lo general, también se denomina cuenta de pagador de AWS o cuenta de administración de AWS Organizations .
- La cuenta de administración de AFT está dedicada a las operaciones de administración de AFT. Cuenta de AWS Es diferente de la cuenta de administración de su organización.
- La cuenta vendida es una Cuenta de AWS que contiene todos los componentes y controles básicos que seleccionó. AFT utiliza AWS Control Tower para vender una cuenta nueva.

Para obtener información adicional sobre esta arquitectura, consulte Introducción a la AFT en el AWS Control Tower taller.

Tools (Herramientas)

Servicios de AWS

- AWS Control Towerle ayuda a configurar y gobernar un entorno de AWS múltiples cuentas, siguiendo las mejores prácticas prescriptivas.

- AWS Account Factory for Terraform (AFT) establece una canalización de Terraform para ayudarlo a aprovisionar y personalizar cuentas y recursos. AWS Control Tower
- AWS Organizationsle ayuda a gestionar y gobernar su entorno de forma centralizada a medida que crece y escala sus AWS recursos. Con Organizations, puede crear nuevas cuentas y asignar recursos, agrupar cuentas para organizar sus flujos de trabajo, aplicar políticas con fines de gobernanza y simplificar la facturación mediante un único método de pago para todas sus cuentas.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos. Este patrón requiere roles y permisos de IAM.

Otras herramientas

- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.

Prácticas recomendadas

- Para ello AWS Control Tower, consulte las prácticas recomendadas para AWS Control Tower administradores en la documentación. AWS Control Tower
- Para más información de IAM, consulte Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Eliminación de los recursos de AFT en la cuenta de administración de AFT

Tarea	Descripción	Habilidades requeridas
Elimine los recursos que identifique la etiqueta AFT.	1. Inicie sesión en la cuenta de administración de AFT con permisos administr ativos. 2. Abra la consola de Grupos de recursos de AWS.	Administrador de AWS DevOps, DevOps ingeniero de AWS

Tarea	Descripción	Habilidades requeridas
	3. Seleccione la región en la que se AWS Control Tower ha implementado. 4. En el panel de navegación, elija Editor de etiquetas. 5. En Tipos de recursos, elija Todos los tipos de recursos compatibles. 6. En Etiquetas, escriba managed_by como clave de la etiqueta y AFT como valor de la etiqueta. 7. Seleccione Buscar recursos. Esta búsqueda muestra todos los recursos creados por AFT. 8. Identifique los nombres de los recursos y elimínelos mediante las consolas de servicio correspondientes. Por ejemplo, para eliminar los recursos del almacén de parámetros: a. Abra la consola de AWS Systems Manager. b. En el panel de navegación, elija Parameter Store (Almacén de parámetros). c. En el cuadro de búsqueda, haga clic	

Tarea	Descripción	Habilidades requeridas
	para mostrar el menú desplegable, elija Nombre, elija igual que y, a continuación, escriba / aft. d. Elimine los parámetros en lotes de 10. (Este es el número máximo que puede eliminar al mismo tiempo). Para la versión 1.12.2 de AFT, podrá eliminar aproximadamente 62 recursos del almacén de parámetros. Todos los nombres de los parámetros comenzarán por /aft. Sin embargo, no todos los recursos se pueden identific ar mediante Grupos de recursos de AWS. En los pasos siguientes, encontrar á y eliminará los recursos restantes.	

Tarea	Descripción	Habilidades requeridas
Elimine roles de IAM.	1. Inicie sesión en la cuenta de administración de AFT con permisos administr ativos. 2. Abra la consola de IAM. 3. Elimine estos roles en el orden indicado (el orden es importante debido a las dependencias): • `aft-*` • `AWSAFTAdmin` • `AWSAFTExecution` • `AWSAFTService` • `codebuild_trigger_role`	Administrador de AWS DevOps, DevOps ingeniero de AWS
Elimine la bóveda AWS Backup de respaldo.	1. Abra la consola de AWS Backup. 2. Localice el almacén de copias de seguridad denominado `aws_backup_vault` . 3. Confirme que el almacén no contiene ninguna copia de seguridad activa. 4. Elimine `aws_backup_vault` .	Administrador de AWS DevOps, DevOps ingeniero de AWS

Tarea	Descripción	Habilidades requeridas
Elimina CloudWatch los recursos de Amazon.	1. Abra la consola de CloudWatch . 2. Elimine los siguientes recursos en el orden que se indica a continuación: a. Bus de eventos: eliminar `aws_cloudwatch_event_bus` . b. Registros: busque el prefijo AFT y elimine todos los grupos de registros relacionados. c. Definiciones de consultas: elimine las siguientes consultas: • `Customization Logs by Account ID` • `Customization Logs by Customization Request ID`	Administrador de AWS DevOps, DevOps ingeniero de AWS
Eliminar AWS KMS recursos.	1. Cambie a la región secundaria, que sirve como backend para realizar el seguimiento del estado de AFT. 2. Abra la consola de AWS KMS. 3. Elimine el alias denominado AFT.	Administrador de AWS DevOps, DevOps ingeniero de AWS

Eliminación de recursos de AFT en la cuenta del archivo de registros

Tarea	Descripción	Habilidades requeridas
Elimine buckets de S3.	1. Inicie sesión en la cuenta del archivo de registros con permisos de administrador. 2. Abra la consola de Amazon S3. 3. Vacíe los siguientes buckets: • `aws-aft-logs-471112509802-us-east-1` • `aws-aft-s3-access-logs-471112509802-us-east-1` (Reemplace `111122223333` por su ID de cuenta). 4. Elimine los dos buckets.	Administrador de AWS DevOps, DevOps ingeniero de AWS
Elimine roles de IAM.	1. Abra la consola de IAM. 2. Compruebe que ningún servicio activo usa los siguientes roles: • `AWSAFTService` • `AWSAFTExecution` 3. Elimine los dos roles.	Administrador de AWS DevOps, DevOps ingeniero de AWS

Eliminación de recursos de AFT en la cuenta de auditoría

Tarea	Descripción	Habilidades requeridas
Elimine roles de IAM.	1. Inicie sesión en la cuenta de auditoría con permisos de administrador. 2. Abra la consola de IAM. 3. Compruebe que ningún servicio activo usa los siguientes roles: • `AWSAFTService` • `AWSAFTExecution` 4. Elimine los dos roles.	Administrador de AWS DevOps, DevOps ingeniero de AWS

Elimine los recursos de AFT de la cuenta AWS Control Tower de administración

Tarea	Descripción	Habilidades requeridas
Elimine roles de IAM.	1. Inicie sesión en la cuenta AWS Control Tower de administración con permisos de administrador. 2. Abra la consola de IAM. 3. Compruebe que ningún servicio activo usa los siguientes roles: • `AWSAFTService` • `AWSAFTExecution` • `aft-control-tower-events-rule` 4. Elimine los tres roles.	Administrador de AWS DevOps, DevOps ingeniero de AWS

Tarea	Descripción	Habilidades requeridas
Eliminar EventBridge reglas.	1. Abre la EventBridge consola de Amazon. 2. En el panel de navegación izquierdo, seleccione Rules (Reglas). 3. Busque y seleccione la regla denominada `aft-capture-ct-events` . 4. Cuando se le pida, elija Eliminar y confirme la eliminación.	Administrador de AWS DevOps, DevOps ingeniero de AWS

Resolución de problemas

Problema	Solución
No se pudo desconectar la puerta de enlace de Internet.	Mientras elimina los recursos identificados mediante la etiqueta AFT, si se encuentras con este problema al desconectar o eliminar la puerta de enlace de Internet, primero debe eliminar los puntos de conexión de VPC: 1. Inicie sesión en la cuenta de administración de AFT y luego abra la consola de Amazon VPC. 2. En el panel de navegación, en la lista Filtrar por VPC, elija la VPC nombrada. aft-management-vpc 3. En el panel de navegación, elija Puntos de conexión. 4. Seleccione los puntos finales que están asociados a la VPC aft-management-vpc.

Problema	Solución
	• Compruebe la columna ID de VPC antes de eliminarla para evitar eliminar los puntos de conexión incorrectos. • Asegúrese de eliminar únicamente los puntos de conexión asociados con la VPC de AFT. 5. Elija Acciones, Eliminar puntos de conexión de VPC. 6. En el cuadro de diálogo de confirmación, escriba eliminar y luego elija Eliminar. 7. Espere a que su punto de conexión cambie de estado a Eliminado. El proceso de eliminación puede tardar unos minutos en completarse.

Problema	Solución
No puede encontrar las consultas CloudWatch especificadas.	Si no puede encontrar las CloudWatch consultas que creó AFT, siga estos pasos: 1. Inicie sesión en la cuenta de administración de AFT y, a continuación, abra la CloudWatch consola. 2. En el panel de navegación, en Registros, elija Información de registros. 3. En la esquina superior derecha, elija el ícono Gonsultas guardadas y de ejemplo. Ahora debería poder ver las consultas de AFT. Para ver una captura de pantalla, consulte la sección de Información adicional. 4. Seleccione las siguientes consultas y, a continuación, elija Acciones y Eliminar para eliminarlas. • `Customization Logs by Account ID` • `Customization Logs by Customization Request ID`

Recursos relacionados

- AFT:
  - GitHub Repositorio
  - Taller
  - Documentación
- AWS Control Tower documentación

Información adicional

Para ver las consultas AFT en el panel de control de CloudWatch Logs Insights, selecciona el icono de consultas guardadas y de muestra en la esquina superior derecha, como se muestra en la siguiente captura de pantalla:

Cree una canalización en Regiones de AWS que no admiten AWS CodePipeline

Anand Krishna Varanasi, Amazon Web Services

Resumen

AWS CodePipeline es un servicio de organización de entrega continua (CD) que forma parte de un conjunto de DevOps herramientas de Amazon Web Services (AWS). Se integra con una gran variedad de fuentes (como sistemas de control de versiones y soluciones de almacenamiento), productos y servicios de integración continua (CI) de AWS nuestros socios AWS y productos de código abierto para proporcionar un servicio de flujo de trabajo integral que permite un despliegue rápido de aplicaciones e infraestructuras.

Sin embargo, CodePipeline no es compatible en todos los Regiones de AWS casos y es útil contar con un orquestador invisible que conecte los servicios. AWS CI/CD Este patrón describe cómo implementar una canalización de flujo de trabajo integral en Regiones de AWS lugares donde aún CodePipeline no es compatible mediante el uso de AWS CI/CD servicios como AWS CodeCommit AWS CodeBuild, y AWS CodeDeploy.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- AWS Cloud Development Kit (AWS CDK) CLI versión 2.28 o posterior

Arquitectura

El siguiente diagrama muestra una canalización que se creó en una región que no es compatible CodePipeline, como la región de África (Ciudad del Cabo). Un desarrollador envía los archivos de CodeDeploy configuración (también denominados scripts de enlace del ciclo de vida de despliegue) al repositorio de Git que aloja. CodeCommit (Consulta el GitHub repositorio que se proporciona con este patrón). Se inicia CodeBuild automáticamente una EventBridge regla de Amazon.

Los archivos CodeDeploy de configuración se obtienen CodeCommit como parte de la etapa de origen de la canalización y se transfieren a ella. CodeBuild

En la siguiente fase, CodeBuild realiza las siguientes tareas:

1. Descargue el archivo TAR del código fuente de la aplicación. Puede configurar el nombre de este archivo mediante el almacén de parámetros, una capacidad de AWS Systems Manager.
2. Descarga los archivos CodeDeploy de configuración.
3. Crea un archivo combinado de código fuente de la aplicación y archivos de CodeDeploy configuración específicos del tipo de aplicación.
4. Inicia el CodeDeploy despliegue en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) mediante el archivo combinado.

Tools (Herramientas)

AWS servicios

- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- AWS CodeCommit es un servicio de control de versiones que permite almacenar y administrar repositorios de Git de forma privada, sin necesidad de administrar su propio sistema de control de origen.
- AWS CodeDeployautomatiza las implementaciones en Amazon EC2 o en instancias locales, AWS Lambda funciones o servicios de Amazon Elastic Container Service (Amazon ECS).
- AWS CodePipeline permite diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software y automatizar los pasos necesarios para lanzar los cambios en el software de manera continua.
- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir y aprovisionar Nube de AWS la infraestructura en código.

Código

El código de este patrón está disponible en el repositorio de GitHub CodePipeline Unsupported Regions.

Epics

Configurar la estación de trabajo de desarrollador

Tarea	Descripción	Habilidades requeridas
Instale la AWS CDK CLI.	Para obtener instrucciones, consulte la documentación de AWS CDK.	AWS DevOps
Instalar un cliente Git.	Para crear confirmaciones, puedes usar un cliente Git instalado en tu computadora local y, a continuación, enviar tus confirmaciones al CodeCommit repositorio. Para configurarlo CodeCommit con tu cliente Git, consulta la CodeCommit documentación.	AWS DevOps
Instale npm.	Instale el administrador de paquetes npm. Para obtener más información, consulte la documentación npm.	AWS DevOps

Configurar la canalización

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código.	Clone el repositorio de Regions GitHub CodePipeline no compatibles en su máquina local ejecutando el siguiente comando. `git clone https://github.com/aws-samp`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	les/invisible-code pipeline-unsupported-regions	

Tarea	Descripción	Habilidades requeridas
Establezca los parámetros en cdk.json.	Abra el archivo `cdk.json` y proporcione valores para los siguientes parámetros: `"pipeline_account" :"XXXXXXXXXXXX", "pipeline_region":" us-west-2", "repo_name": "app-dev-repo", "ec2_tag_key": "test-vm", "configName" : "cbdeployconfig", "deploymentGroupNa me": "cbdeploygroup", "applicationName" : "cbdeployapplicati on", "projectName" : "CodeBuildProject"` donde: • `pipeline_account` es Cuenta de AWS donde se construirá el oleoducto. • `pipeline_region` es el Región de AWS lugar donde se construirá el oleoducto. • `repo_name` es el nombre del CodeCommit repositorio. • `ec2_tag_key` es la etiqueta adjunta a la instancia de Amazon EC2 en la que desea implement ar el código.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• `configName` es el nombre del archivo de CodeDeploy configuración. • `deploymentGroupNam e` es el nombre del grupo CodeDeploy de implement ación. • `applicationName` es el nombre CodeDeploy de la aplicación. • `projectName` es el nombre CodeBuild del proyecto.	

Configure la biblioteca de AWS CDK construcción.	En el GitHub repositorio clonado, utilice los siguiente s comandos para instalar la biblioteca de AWS CDK construcción, compilar la aplicación y sintetizar para generar la AWS CloudForm ation plantilla de la aplicación.
	`npm i aws-cdk-lib`
	`npm run build`
	`cdk synth`
		AWS DevOps

Implemente la AWS CDK aplicación de muestra.	Implemente el código ejecutando el siguiente comando en una región no compatible (por ejemplo `af-south-1`). `cdk deploy`	AWS DevOps

Configure el CodeCommit repositorio para CodeDeploy

Tarea	Descripción	Habilidades requeridas
Configure CI/CD para la aplicación.	Clone el CodeCommit repositorio que especificó en el `cdk.json` archivo (se denomina de forma `app-dev-repo` predeterminada) para configurar la CI/CD canalización de la aplicación. `git clone https://git-codecommit.us-west-2.amazonaws.com/v1/repos/app-dev-repo` donde el nombre y la región del repositorio dependen de los valores que haya proporcionado en el archivo `cdk.json`.	AWS DevOps

Prueba la canalización

Tarea	Descripción	Habilidades requeridas
Pruebe la canalización con las instrucciones de implementación.	La `CodeDeploy_Files` carpeta del repositorio de regiones GitHub CodePipeline no compatibles incluye archivos de muestra que indican cómo CodeDeploy implementar la aplicación. El `appspec.yml` archivo es un archivo CodeDeploy de configuración que contiene enlaces para controlar el	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	flujo de implementación de la aplicación. Puede usar los archivos de muestra `index.html` , `start_server.sh` , `stop_server.sh` y `install_dependencies.sh` para actualizar un sitio web alojado en Apache. Estos son ejemplos: puede usar el código del GitHub repositorio para implementar cualquier tipo de aplicación. Cuando los archivos se envían al CodeCommit repositorio, la canalización invisible se inicia automáticamente. Para ver los resultados de la implementación, compruebe los resultados de las fases individuales en las CodeDeplo y consolas CodeBuild y consolas.	

Recursos relacionados

- Cómo empezar (AWS CDK documentación)
- Introducción al AWS Cloud Development Kit (AWS CDK) (AWS Workshop Studio)
- AWS CDK Taller

Personalice los nombres de los roles predeterminados mediante AWS CDK aspectos y trampillas de escape

SANDEEP SINGH y James Jacob, Amazon Web Services

Resumen

Este patrón muestra cómo personalizar los nombres predeterminados de los roles que se crean mediante componentes fijos. AWS Cloud Development Kit (AWS CDK) La personalización de los nombres de los roles suele ser necesaria si la organización tiene restricciones específicas basadas en las convenciones de nomenclatura. Por ejemplo, su organización puede establecer límites de permisos AWS Identity and Access Management (IAM) o políticas de control de servicios (SCPs) que requieran un prefijo específico en los nombres de las funciones. En esos casos, es posible que los nombres de los roles predeterminados generados por AWS CDK las construcciones no cumplan estas convenciones y sea necesario modificarlos. Este patrón aborda esos requisitos mediante el uso de vías de escape y aspectos de AWS CDK. Utilice las vías de escape para definir los nombres de los roles personalizados y los aspectos para aplicar un nombre personalizado a todos los roles, a fin de garantizar el cumplimiento de las políticas y restricciones de la organización.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Requisitos previos especificados en la documentación de AWS CDK

Limitaciones

- Los aspectos filtran los recursos en función de los tipos de recursos, por lo que todos los roles comparten el mismo prefijo. Si necesita prefijos de rol diferentes para roles distintos, es necesario aplicar filtros adicionales en función de otras propiedades. Por ejemplo, para asignar distintos prefijos a los roles que están asociados a AWS Lambda funciones, puede filtrar por atributos o etiquetas de rol específicos y aplicar un prefijo para los roles relacionados con Lambda y un prefijo diferente para los demás roles.
- Los nombres de los roles de IAM tienen una longitud máxima de 64 caracteres, por lo que los nombres de los roles modificados deben recortarse para cumplir con esta restricción.

- Algunos Servicios de AWS no están disponibles en todos. Regiones de AWS Para conocer la disponibilidad de las regiones, consulte Servicios de AWS by Region. Para los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

Pila de tecnología de destino

- AWS CDK
- AWS CloudFormation

Arquitectura de destino

- Una AWS CDK aplicación consta de una o más CloudFormation pilas, que se sintetizan e implementan para administrar AWS los recursos.
- Para modificar una propiedad de un recurso AWS CDK administrado que no esté expuesta por una construcción de capa 2 (L2), se utiliza una vía de escape para anular las CloudFormation propiedades subyacentes (en este caso, el nombre de la función) y un aspecto para aplicar la función a todos los recursos de la AWS CDK aplicación durante el proceso de síntesis de la pila. AWS CDK

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir y aprovisionar la Nube de AWS infraestructura en el código.
- AWS CDK La interfaz de línea de comandos (AWS CDK CLI) (también conocida como kit de AWS CDK herramientas) es un kit de desarrollo en la nube de línea de comandos que le ayuda a interactuar con su AWS CDK aplicación. El `cdk` comando CLI es la herramienta principal para interactuar con AWS CDK la aplicación. Ejecuta tu aplicación, consulta el modelo de aplicación que has definido y produce e implementa las CloudFormation plantillas generadas por el. AWS CDK
- CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y administrarlos a lo largo de su ciclo de vida en todas Cuentas de AWS las regiones.

Repositorio de código

El código fuente y las plantillas de este patrón están disponibles en el repositorio GitHub CDK Aspects Override.

Prácticas recomendadas

Consulte las mejores prácticas para usar el AWS CDK in TypeScript para crear proyectos de IaC en el sitio web de la Guía AWS prescriptiva.

Epics

Instalación de la AWS CDK CLI

Tarea	Descripción	Habilidades requeridas
Instale la AWS CDK CLI.	Para instalar la AWS CDK CLI globalmente, ejecute el comando: `npm install -g aws-cdk`	AWS DevOps
Verificar la versión.	Ejecute el comando: `cdk --version` Confirme que está utilizando la versión 2 de la AWS CDK CLI.	AWS DevOps
Inicie el AWS CDK entorno.	Antes de implementar las CloudFormation plantillas, prepare la cuenta Región de AWS que desea usar. Ejecute el comando: `cdk bootstrap <account> /<Region>`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte el proceso de [AWS CDK arranque en] la documentación. AWS	

Implemente la AWS CDK aplicación para demostrar el uso de los aspectos

Tarea	Descripción	Habilidades requeridas

Configure el proyecto.	1. Clona el GitHub repositorio de este patrón en tu computadora local:
	`git clone https://github.com/aws-samples/cdk-aspects-override`
	2. Vaya al directorio del proyecto en el equipo local.
	3. Instale las dependencias del proyecto:
	`npm ci`
		AWS DevOps

Implemente pilas con los nombres de rol predeterminados asignados por AWS CDK.	Implemente dos CloudFormation pilas (`ExampleStack1 yExampleStack2 `) que contengan las funciones de Lambda y sus funciones asociadas: `npm run deploy:ExampleAppWithoutAspects`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	El código no transfiere explícitamente las propiedad es de los roles, por lo que los nombres de los roles los construirá AWS CDK. Para obtener un ejemplo de resultado, consulte la sección Información adicional.	

Tarea	Descripción	Habilidades requeridas

Implemente pilas con aspectos.	En este paso, se aplica un aspecto que impone una convención de nombres de roles añadiendo un prefijo a todos los roles de IAM que se implementan en el proyecto. AWS CDK El aspecto se define en el archivo `lib/aspects.ts` . El aspecto utiliza una vía de escape para anular el nombre del rol mediante la adición de un prefijo. El aspecto se aplica a las pilas del archivo `bin/app-with-aspects.ts` . En este ejemplo, el prefijo del nombre del rol es `dev-unicorn` .
	
	1. Edite el archivo `bin/app-with-aspects.ts` .
	2. En el archivo, actualice la variable `ROLE_NAME_PREFIX` con el prefijo `dev-unicorn` :
	
	`const app = new cdk.App();`
	
	`// Define a prefix for the role names`
	`const ROLE_NAME_PREFIX = 'dev-unicorn';`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	``
	// Instantiate the
	 RoleNamingConventi
	onAspect with the
	 desired prefix
	const roleNamin
	gConventionAspect
	 = new RoleNamin
	gConventionAspect(
	ROLE_NAME_PREFIX);
	``
	3. Implemente la AWS CDK aplicación con los siguiente s aspectos:
	``
	npm run deploy:Ex
	ampleAppWithAspects
	``
	Para obtener un ejemplo de resultado, consulte la sección Información adicional.	

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Elimine sus AWS CloudForm ation pilas.	Cuando termine este patrón, ejecute el comando siguiente para eliminar los recursos y evitar incurrir en costos adicionales: ``` cdk destroy --all -f && cdk --app npx ts-node bin/app-with-aspec ts.ts' destroy --all - f ```	AWS DevOps

Resolución de problemas

Problema	Solución
Tiene problemas al utilizar el AWS CDK.	Consulte Solución de AWS CDK problemas comunes en la AWS CDK documentación.

Recursos relacionados

- AWS Cloud Development Kit (AWS CDK)
- AWS CDK documentación
- AWS CDK en GitHub
- Vías de escape
- Aspectos y el AWS CDK

Información adicional

Nombres de roles creados por CloudFormation sin aspectos

```
Outputs:
ExampleStack1WithoutAspects.Function1RoleName = example-stack1-without-as-
Function1LambdaFunctionSe-y7FYTY6FXJXA
ExampleStack1WithoutAspects.Function2RoleName = example-stack1-without-as-
Function2LambdaFunctionSe-dDZV4rkWqWnI
...

Outputs:
ExampleStack2WithoutAspects.Function3RoleName = example-stack2-without-as-
Function3LambdaFunctionSe-ygMv49iTyMq0
```

Nombres de rol creados por CloudFormation With Aspects

```
Outputs:
ExampleStack1WithAspects.Function1RoleName = dev-unicorn-
Function1LambdaFunctionServiceRole783660DC
ExampleStack1WithAspects.Function2RoleName = dev-unicorn-
Function2LambdaFunctionServiceRole2C391181
...
```

```
Outputs:
ExampleStack2WithAspects.Function3RoleName = dev-unicorn-
Function3LambdaFunctionServiceRole4CAA721C
```

Implemente un clúster de Cassandra en Amazon EC2 con estática privada IPs para evitar el reequilibrio

Dipin Jain, Amazon Web Services

Resumen

La IP privada de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) se conserva durante todo su ciclo de vida. Sin embargo, la IP privada puede cambiar durante un bloqueo planificado o imprevisto del sistema; por ejemplo, durante una actualización de Imagen de máquina de Amazon (AMI). En algunos escenarios, retener una IP estática privada puede mejorar el rendimiento y el tiempo de recuperación de las cargas de trabajo. Por ejemplo, el uso de una IP estática para un nodo raíz de Apache Cassandra evita que el clúster incurra en una sobrecarga de reequilibrio.

Este patrón describe cómo conectar una interfaz de red elástica secundaria a EC2 las instancias para mantener la IP estática durante el realojamiento. El patrón se centra en los clústeres de Cassandra, pero puedes usar esta implementación para cualquier arquitectura que se beneficie de la estática privada. IPs

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa

Versiones de producto

- DataStax versión 5.11.1
- Sistema operativo: Ubuntu 16.04.6 LTS

Arquitectura

Arquitectura de origen

La fuente podría ser un clúster de Cassandra en una máquina virtual (VM) local o en EC2 instancias de la nube de AWS. En el siguiente diagrama se ilustra el segundo escenario. Este ejemplo incluye cuatro nodos en el clúster: tres nodos raíz y un nodo de administración. En la arquitectura de origen, cada nodo tiene una única interfaz de red conectada.

Arquitectura de destino

El clúster de destino se aloja en EC2 instancias con una interfaz de red elástica secundaria conectada a cada nodo, como se muestra en el siguiente diagrama.

Automatización y escala

También puede automatizar la conexión de una segunda interfaz de red elástica a un grupo de EC2 Auto Scaling, tal y como se describe en un vídeo del AWS Knowledge Center.

Epics

Configurar un clúster de Cassandra en Amazon EC2

Tarea	Descripción	Habilidades requeridas
Lanza EC2 nodos para alojar un clúster de Cassandra.	En la EC2 consola de Amazon, lanza cuatro EC2 instancias para tus nodos de Ubuntu en tu cuenta de AWS. Se utilizan tres nodos (iniciales) para el clúster de Cassandra y el cuarto nodo actúa como nodo de administración de clústeres en el que se instalará DataStax Enterprise (DSE) OpsCenter . Para obtener instrucciones, consulta la EC2 documentación de Amazon.	Ingeniero de nube
Confirmar las comunicaciones de los nodos.	Asegúrese de que los cuatro nodos se puedan comunicar entre sí a través de los puertos de administración de la base de datos y el clúster.	Ingeniero de redes

Tarea	Descripción	Habilidades requeridas
Instale el DSE OpsCenter en el nodo de administración.	Instale DSE OpsCenter 6.1 desde el paquete Debian en el nodo de gestión. Para obtener instrucciones, consulte la documentación de DataStax .	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree una interfaz de red secundaria.	Cassandra genera un identificador único universal (UUID) para cada nodo en función de la dirección IP de la EC2 instancia de ese nodo. Este UUID se utiliza para distribuir los nodos virtuales (vnodes) en el anillo. Cuando Cassandra se implementa en EC2 las instancias, las direcciones IP se asignan automáticamente a las instancias a medida que se crean. En caso de que se produzca una interrupción planificada o imprevista, la dirección IP de la nueva EC2 instancia cambia, la distribución de los datos cambia y es necesario reequilibrar todo el anillo. Esta situación no es deseable. Para conservar la dirección IP asignada, utilice una interfaz de red elástica secundaria con una dirección IP fija. 1. En la EC2 consola de Amazon, selecciona Interfaces de red, Crear interfaz de red. 2. En Subred, selecciona la subred en la que creaste la EC2 instancia.	Ingeniero de nube

Tarea	Descripción	Habilidades requeridas
	3. En IPv4 Dirección privada, selecciona Asignación automática. 4. Para los Grupos de seguridad, seleccione un grupo de seguridad y, a continuación, seleccione Crear interfaz de red. Para obtener más información sobre la creación de una interfaz de red, consulta la EC2 documentación de Amazon.	

Tarea	Descripción	Habilidades requeridas
Conectar la interfaz de red secundaria a los nodos del clúster.	1. En la EC2 consola de Amazon, selecciona Instances. 2. Selecciona la casilla de verificación de la EC2 instancia que creaste anteriormente. 3. Elija Acciones, Redes, Conectar interfaz de red. 4. Seleccione la interfaz de red que creó en el paso anterior y, a continuación, seleccione Conectar. Para obtener más información sobre cómo conectar una interfaz de red, consulta la EC2 documentación de Amazon.	Ingeniero de nube

Tarea	Descripción	Habilidades requeridas
Añade rutas en Amazon EC2 para abordar el enrutamiento asimétrico.	Al conectar la segunda interfaz de red, es muy probable que la red realice un enrutamiento asimétrico. Para evitarlo, puede agregar rutas para las nuevas interfaces de red. Para obtener una explicaci ón detallada y corregir el enrutamiento asimétrico, consulte el vídeo del AWS Knowledge Center o Cómo superar el enrutamiento asimétrico en servidores multihogar (artículo publicado por Patrick en Linux Journal McManus, el 5 de abril de 2004).	Ingeniero de redes
Actualizar las entradas de DNS para que apunten a la IP de la interfaz de red secundari a.	Apunte el nombre de dominio completo (FQDN) del nodo a la IP de la interfaz de red secundaria.	Ingeniero de redes
Instale y configure el clúster de Cassandra mediante DSE. OpsCenter	Cuando los nodos del clúster estén listos con las interface s de red secundarias, podrá instalar y configurar el clúster de Cassandra.	Administrador de base de datos

Recuperar el clúster de un fallo de nodo

Tarea	Descripción	Habilidades requeridas
Crear una AMI para el nodo raíz del clúster.	Haga una copia de seguridad de los nodos para poder restaurarlos con los archivos binarios de la base de datos en caso de que fallen los nodos. Para obtener instrucciones, consulte Crear una AMI en la EC2 documentación de Amazon.	Administrador de copias de seguridad
Recuperarse del fallo de un nodo.	Sustituya el nodo fallido por una nueva EC2 instancia lanzada desde la AMI y conecte la interfaz de red secundaria del nodo fallido.	Administrador de copias de seguridad
Verificar que el clúster de Cassandra está en buen estado.	Cuando el nodo de reemplazo esté activo, compruebe el estado del clúster en el DSE OpsCenter.	Administrador de base de datos

Recursos relacionados

- Instalación del DSE OpsCenter 6.1 desde el paquete Debian (DataStax documentación)
- Cómo hacer que una interfaz de red secundaria funcione en una EC2 instancia de Ubuntu (vídeo del AWS Knowledge Center)
- Prácticas recomendadas para ejecutar Apache Cassandra en Amazon EC2 (entrada del blog de AWS)

Amplíe VRFs su alcance a AWS mediante AWS Transit Gateway Connect

Adam Till, Yashar Araghi, Vikas Dewangan y Mohideen, de Amazon Web Services HajaMohideen

Resumen

El enrutamiento y el reenvío virtuales (VRF) son una característica de las redes tradicionales. Utiliza dominios de enrutamiento lógico aislados, en forma de tablas de enrutamiento, para separar el tráfico de red dentro de la misma infraestructura física. Puede configurar AWS Transit Gateway para que admita el aislamiento de VRF al conectar su red en las instalaciones a AWS. Este patrón utiliza una arquitectura de ejemplo para conectarse de forma local a diferentes tablas de rutas de las pasarelas de tránsito. VRFs

Este patrón utiliza interfaces virtuales de tránsito (VIFs) en los archivos adjuntos de AWS Direct Connect y Transit Gateway Connect para ampliar la VRFs. Un VIF de tránsito se utiliza para acceder a una o más puertas de enlace de tránsito de Amazon VPC asociadas a las puertas de enlace de Direct Connect. Una conexión de Transit Gateway Connect conecta una puerta de enlace de tránsito con un dispositivo virtual de terceros que se ejecuta en una VPC. Una conexión de Transit Gateway Connect admite el protocolo de túnel de encapsulación de enrutamiento genérico (GRE) para un alto rendimiento y el protocolo de puerta de enlace fronteriza (BGP) para el enrutamiento dinámico.

El enfoque descrito en este patrón tiene los siguientes beneficios:

- Con Transit Gateway Connect, puede anunciar hasta 1000 rutas en el dispositivo homólogo de Transit Gateway Connect y recibir hasta 5000 rutas de este. El uso de la característica VIF de tránsito Direct Connect sin Transit Gateway Connect está limitado a 20 prefijos por puerta de enlace.
- Puede mantener el aislamiento del tráfico y utilizar Transit Gateway Connect para proporcionar servicios con host en AWS, independientemente de los esquemas de direcciones IP que utilicen sus clientes.
- No es necesario que el tráfico de VRF atraviese una interfaz virtual pública. Esto facilita el cumplimiento de los requisitos de cumplimiento y seguridad en muchas organizaciones.
- Cada túnel de GRE admite hasta 5 Gbps y puede tener hasta cuatro túneles de GRE por cada conexión de Transit Gateway Connect. Es más rápido que muchos otros tipos de conexión, como las conexiones Site-to-Site VPN de AWS que admiten hasta 1,25 Gbps.

Requisitos previos y limitaciones

Requisitos previos

- Se han creado las cuentas de AWS necesarias (consulte la arquitectura para obtener más información)
- Permisos para asumir un rol de AWS Identity and Access Management (IAM) en cada cuenta.
- Los roles de IAM de cada cuenta deben tener permisos para aprovisionar los recursos de AWS Transit Gateway y AWS Direct Connect. Para obtener más información, consulte Autenticación y control de acceso para sus puertas de enlace y Administración de identidad y acceso para Direct Connect.
- Las conexiones Direct Connect se crearon correctamente. Para obtener más información, consulte Creación de una conexión mediante el asistente de conexión.

Limitaciones

- Hay límites para las conexiones de Transit Gateway a VPCs las cuentas de producción, control de calidad y desarrollo. Para obtener más información, consulte Conexión de puerta de enlace de tránsito a una VPC.
- Existen límites para la creación y el uso de puertas de enlace de Direct Connect. Para obtener más información, consulte Cuotas AWS Direct Connect.

Arquitectura

Arquitectura de destino

El siguiente ejemplo de arquitectura proporciona una solución reutilizable para implementar Transit VIFs con los archivos adjuntos Transit Gateway Connect. Esta arquitectura proporciona resiliencia mediante el uso de varias ubicaciones de Direct Connect. Para obtener más información, consulte Resiliencia máxima en la documentación de Direct Connect. La red local tiene producción, control de calidad y desarrollo VRFs que se extienden a AWS y se aíslan mediante tablas de rutas dedicadas.

En el entorno de AWS, hay dos cuentas dedicadas a ampliarla VRFs: una cuenta de Direct Connect y una cuenta de hub de red. La cuenta Direct Connect contiene la conexión y el tránsito VIFs de cada router. El tránsito se crea VIFs desde la cuenta de Direct Connect, pero se despliega en la cuenta del concentrador de red para poder asociarlo a la puerta de enlace de Direct Connect en la cuenta del

concentrador de red. La cuenta del hub de red contiene la puerta de enlace de Direct Connect y la puerta de enlace de tránsito. Los recursos de AWS están conectados de la siguiente manera:

1. Transit VIFs conecta los enrutadores de las ubicaciones de Direct Connect con AWS Direct Connect en la cuenta de Direct Connect.
2. Un VIF de tránsito conecta Direct Connect con la puerta de enlace Direct Connect de la cuenta del hub de red.
3. Una asociación de puertas de enlace de tránsito conecta la puerta de enlace Direct Connect con la puerta de enlace de tránsito de la cuenta del hub de red.
4. Los accesorios Transit Gateway Connect conectan la pasarela de tránsito con VPCs las cuentas de producción, control de calidad y desarrollo.

Arquitectura Transit VIF

El siguiente diagrama muestra los detalles de configuración del tránsito VIFs. En este ejemplo de arquitectura se utiliza una VLAN para la fuente del túnel, pero también se puede utilizar un bucle invertido.

A continuación se muestran los detalles de configuración, como los números de sistema autónomo (ASNs), del tránsito VIFs.

Recurso	Elemento	Detalle
router-01	ASN	65534
router-02	ASN	65534
router-03	ASN	65534
router-04	ASN	65534
Gateway de Direct Connect	ASN	64601
Puerta de enlace de tránsito	ASN	64600
	Bloque CIDR	10,100,254,0/24

Arquitectura Transit Gateway Connect

El diagrama y las tablas siguientes describen cómo configurar un VRF único a través de una conexión Transit Gateway Connect. Además VRFs, asigne direcciones IP GRE de túnel IDs, pasarela de tránsito y BGP únicos dentro de los bloques CIDR. La dirección IP GRE homóloga coincide con la dirección IP homóloga del router del VIF de tránsito.

La siguiente tabla contiene detalles de configuración del enrutador.

Enrutador	Túnel	Dirección IP	Origen	Destino
router-01	Túnel 1	169.254.101.17	VLAN 60	10,100,254.1
			169,254,1001	
router-02	Túnel 11	169,254,101,81	VLAN 61	10,100254,11
			169,254,1005	
router-03	Túnel 21	169,254,101,145	VLAN 62	10,100254,21
			169,254,1009	
router-04	Túnel 31	169,254,101,209	VLAN 63	10,100254,31
			169,254100,13	

La siguiente tabla contiene detalles de la puerta de enlace de tránsito.

Túnel	Dirección IP GRE de puerta de enlace	Direcciones IP GRE del mismo nivel	BGP dentro de los bloques CIDR
Túnel 1	10,100254.1	VLAN 60	169,254,101,16/29
		169,254,1001	
Túnel 11	10,100254,11	VLAN 61	169,254,101,80/29
		169,254,1005	

Túnel 21	10,100254,21	VLAN 62 169,254,1009	169,254.101.144/29
Túnel 31	10,100254,31	VLAN 63 169,254100,13	169,254,101.208/29

Implementación

La sección Epics describe cómo implementar un ejemplo de configuración para un único VRF en varios enrutadores de clientes. Una vez completados los pasos 1 a 5, puede crear nuevas conexiones de Transit Gateway Connect siguiendo los pasos 6 y 7 para cada VRF nuevo que extienda a AWS:

1. Cree la puerta de enlace de tránsito.
2. Crear una tabla de enrutamiento de la puerta de enlace de tránsito para cada VRF.
3. Cree las interfaces virtuales de tránsito.
4. Cree una puerta de enlace Direct Connect.
5. Cree la interfaz virtual de la puerta de enlace Direct Connect y las asociaciones de puerta de enlace con los prefijos permitidos.
6. Cree una conexión de Connect de puerta de enlace de tránsito.
7. Crear pares de Transit Gateway Connect.
8. Asocie las conexiones de Transit Gateway Connect con la tabla de enrutamiento.
9. Anuncie las rutas a los enrutadores.

Tools (Herramientas)

Servicios de AWS

- AWS Direct Connect vincula su red interna con una ubicación de Direct Connect a través de un cable estándar Ethernet de fibra óptica. Con esta conexión, puede crear interfaces virtuales directamente en servicios públicos de AWS omitiendo a los proveedores de servicios de Internet en su ruta de acceso a la red.
- AWS Transit Gateway es un centro central que conecta nubes privadas virtuales (VPCs) y redes locales.

- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Epics

Planifique la arquitectura

Tarea	Descripción	Habilidades requeridas
Cree diagramas de arquitectura personalizados.	1. En la sección Attachments (Conexiones), descargue la plantilla de diagrama. 2. Abra el diagrama adjunto en Microsoft Office PowerPoint. 3. En la diapositiva Architecture overview (Descripción general de la arquitectura), personalice el diagrama de arquitectura para su entorno. Identifique las instalaciones locales VRFs que deben extenderse a su entorno de AWS. 4. En la diapositiva Transit VIF (VIF de tránsito), personalice el diagrama de arquitectura. Identifique los números de AS de los enrutadores, la puerta de enlace de Direct Connect y la puerta de enlace de tránsito. Identifique las direcciones IP en cada extremo del VIF de tránsito.	Arquitecto de la nube, administrador de redes

Tarea	Descripción	Habilidades requeridas
	5. En la diapositiva Transit Gateway Connect, personalice un diagrama de arquitectura para cada VRF. Identifique todas las direcciones IP necesaria s para configurar los enrutadores y los pares de Transit Gateway Connect.	

Cree los recursos de la puerta de enlace de tránsito.

Tarea	Descripción	Habilidades requeridas
Cree la puerta de enlace de tránsito.	1. Inicie sesión en la cuenta del hub de red. 2. Siga las instrucciones de Crear una puerta de enlace de tránsito. Tenga en cuenta lo siguiente para este patrón: • En Amazon side Autonomous System Number (ASN) (Número de sistema autónomo (ASN) de Amazon), ingrese el ASN único. A los efectos de este ejemplo, el ASN es `64600`. • Seleccione DNS support (Compatibilidad de DNS).	Administrador de redes, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	• Para este ejemplo de arquitectura, no se requieren la compatibilidad con ECMP de VPN, la Asociación de tablas de enrutamiento predeterminada, la Prórroga de la tabla de enrutamiento predeterminada ni la Compatibilidad con multidifusión. • En el caso de los bloques CIDR de Transit Gateway, introduzca los bloques IPv4 CIDR de su pasarela de tránsito. A los efectos de este ejemplo, el bloque de CIDR es `10.100.254.0/24` .	

Tarea	Descripción	Habilidades requeridas
Cree una tabla de enrutamiento para la puerta de enlace de tránsito.	Siga las instrucciones de Crear una tabla de enrutamiento para la puerta de enlace de tránsito. Tenga en cuenta lo siguiente para este patrón: • En Name tag (Nombre de la etiqueta), escriba un nombre para la tabla de enrutamiento de la puerta de enlace de tránsito. Recomendamos usar un nombre que corresponda al VRF, como `routetable-dev-vrf` . • En Transit Gateway ID (ID de gateway de tránsito), elija la puerta de enlace de tránsito que creó.	Arquitecto de la nube, administrador de redes

Cree las interfaces virtuales de tránsito

Tarea	Descripción	Habilidades requeridas
Cree las interfaces virtuales de tránsito.	1. Inicie sesión en la cuenta Direct Connect. 2. Siga las instrucciones para Crear una interfaz virtual de tránsito en la puerta de enlace de Direct Connect. Tenga en cuenta lo siguiente para este patrón:	Arquitecto de la nube, administrador de redes

Tarea	Descripción	Habilidades requeridas
	• En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual. Recomendamos usar un nombre que corresponda al enrutador, como `transit-vif-router01` . • En Connection (Conexión), seleccione el enrutador, por ejemplo `router-01` . • Para el Virtual interface owner (Propietario de la interfaz virtual), introduzca el ID de cuenta de la cuenta del hub de red. Para obtener instrucciones, consulte Ver el ID de su cuenta de AWS. • Para la puerta de enlace Direct Connect, no haga ninguna selección. La puerta de enlace Direct Connect se conecta en un paso posterior. • Para la VLAN, introduzca la VLAN del enrutador, por ejemplo `60`. • Para ASN BGP, introduzca el ASN del enrutador, por ejemplo `65534`.	

Tarea	Descripción	Habilidades requeridas

	• En Additional Settings (Configuración adicional), haga lo siguiente:
	  • Elija IPv4.
	  • Para la IP homóloga de su enrutador, introduzca la dirección IP homóloga del enrutador, por ejemplo `169.254.100.1` .
	  • Para la IP homóloga del enrutador Amazon, introduzca la dirección IP homóloga del enrutador de Amazon, por ejemplo `169.254.100.2` .
	  • Para la clave de autenticación BGP, se requiere una contraseña. Si se deja en blanco, AWS crea una clave a la que solo se puede acceder en esta cuenta.
	3. Repite estas instrucciones para crear todo el tránsito VIFs para el VRF.	

Cree los recursos de Direct Connect

Tarea	Descripción	Habilidades requeridas
Cree una puerta de enlace de Direct Connect.	1. Inicie sesión en la cuenta del hub de red. 2. Siga las instrucciones de Creación de una puerta de enlace de Direct Connect. Tenga en cuenta lo siguiente para este patrón: • Para el ASN de Amazon, introduzca el ASN de la puerta de enlace Direct Connect, como `64601`. • No elija una puerta de enlace privada virtual.	Arquitecto de la nube, administrador de redes
Conecte la puerta de enlace Direct Connect al transporte público VIFs.	1. En la cuenta del hub de red, abra la consola AWS Direct Connect en la versión https://console.aws.amazon.com/directconnect/2/. 2. En el panel de navegación, elija Virtual Interfaces. 3. Seleccione un nuevo VIF de tránsito y, a continuación, elija Accept (Aceptar). 4. Elija la puerta de enlace Direct Connect que creó. 5. Repita estas instrucciones para cada VIF de tránsito.	Arquitecto de la nube, administrador de redes
Cree las asociaciones de puerta de enlace Direct	En la cuenta del hub de red, siga las instrucciones de Para	Arquitecto de la nube, administrador de redes

Tarea	Descripción	Habilidades requeridas
Connect con los prefijos permitidos.	asociar una puerta de enlace de tránsito. Tenga en cuenta lo siguiente para este patrón: • En Transit Gateway ID (ID de puerta de enlace de tránsito), elija la puerta de enlace de tránsito que creó. • En Allowed prefixes (Prefijos permitidos), introduzca el bloque CIDR asignado a la puerta de enlace de tránsito, por ejemplo `10.100.254.0/24` . Al crear esta asociación, se crea automáticamente una conexión de puerta de enlace de tránsito que tiene un tipo de recurso Direct Connect Gateway. No es necesario que esta conexión esté asociada a una tabla de enrutamiento de puerta de enlace de tránsito.	

Tarea	Descripción	Habilidades requeridas
Cree una conexión de Connect de puerta de enlace de tránsito.	1. En la cuenta del hub de red, abre la consola de Amazon VPC en. https://console.aws.amazon.com/vpc/ 2. En el panel de navegación, elija Transit gateway attachments (Conexiones de puerta de enlace de tránsito). 3. Elija Create transit gateway attachment (Crear conexión de puerta de enlace de tránsito). 4. En Name (Nombre), escriba un nombre para la conexión. Recomendamos usar un nombre que corresponda al VRF, como `PROD-VRF`. 5. En Transit Gateway ID (ID de puerta de enlace de tránsito), elija la puerta de enlace de tránsito que creó. 6. En Attachment type (Tipo de conexión), elija Connect. 7. Para el Transport attachment ID (ID de conexión de transporte), elija la puerta de enlace de Direct Connect que creó anteriormente. 8. Elija Create transit gateway attachment (Crear conexión	Arquitecto de la nube, administrador de redes

Tarea	Descripción	Habilidades requeridas
	de puerta de enlace de tránsito). 9. Repita este paso para cada VRF que vaya a ampliar.	

Tarea	Descripción	Habilidades requeridas
Crear pares de Transit Gateway Connect.	1. En la cuenta del hub de red, siga las instrucciones de Crear un homólogo de Transit Gateway Connect (túnel de GRE). Tenga en cuenta lo siguiente para este patrón: • En Name tag (Nombre de la etiqueta), puede escribir un nombre para la puerta de enlace de tránsito. Recomendamos usar un nombre que corresponda al enrutador, como `connectpeer-router01`. • Para la dirección GRE de Transit Gateway, introduzca la dirección IP asignada desde el bloque CIDR, por ejemplo `10.100.254.1`. • Para la dirección GRE homóloga, introduzca la dirección IP asignada a la VLAN creada en el enrutador para el VIF de tránsito, por ejemplo `169.254.100.1`. Siempre que AWS pueda acceder a la dirección IP, puede utilizar cualquier interfaz, como VLAN	

Tarea	Descripción	Habilidades requeridas
	o Loopback, para la dirección GRE homóloga. • Para BGP dentro de los bloques CIDR (IPv4), introduzca la dirección IP del BGP dentro del bloque CIDR, por ejemplo `169.254.101.16/29` • Para ASN homólogo, introduzca el ASN del enrutador, por ejemplo `65534`. 2. Repita estas instrucciones para crear un túnel de GRE para cada enrutador.	

Anuncie las rutas a los enrutadores.

Tarea	Descripción	Habilidades requeridas
Anuncie las rutas.	Asocie la nueva conexión de puerta de enlace de Connect a la tabla de enrutamiento que creó anteriormente para este VRF. Por ejemplo, asocie las conexiones de Transit Gateway Connect de producción con la tabla de enrutamiento `Production-VRF`.	Administrador de redes, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Cree una ruta estática para el prefijo que se anuncia en los enrutadores. 1. Inicie sesión en la cuenta del hub de red. 2. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/. 3. En el panel de navegación, bajo Transit Gateways (Puertas de enlace de tránsito) elija Transit gateway route tables (Tablas de enrutamiento de puerta de enlace de tránsito). 4. Seleccione la tabla de enrutamiento de la `Production-VRF` . 5. En el menú Actions (Acciones), elija Create static route (Crear ruta estática). 6. Para CIDR, introduzca el bloque CIDR para la ruta anunciada a la conexión de puerta de enlace de tránsito en la VPC de destino, como `10.100.1.0/24` . 7. En Choose Attachment (Elegir conexión), seleccione la conexión de	

Tarea	Descripción	Habilidades requeridas
	Transit Gateway Connect correspondiente. 8. Elija Create static route (Crear ruta estática).	

Recursos relacionados

Documentación de AWS

- Documentación de Direct Connect
  - Uso de puertas de enlace de Direct Connect
  - Asociaciones de la puerta de enlace de tránsito
  - Interfaces virtuales de AWS Direct Connect
- Documentación de Transit Gateway
  - Usar puertas de enlace de tránsito
  - Conexiones de puertas de enlace de tránsito a una puerta de enlace de Direct Connect
  - Conexiones de puertas de enlace de tránsito y pares de Transit Gateway Connect
  - Crear una conexión Transit gateway Connect

Publicaciones del blog de AWS

- Segmentación de redes híbridas con AWS Transit Gateway Connect
- Uso de AWS Transit Gateway connect para ampliar VRFs y aumentar la publicidad de prefijos de IP

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Reciba notificaciones de Amazon SNS cuando cambie el estado de clave de una clave de AWS KMS

Shubham Harsora, Aromal Raj Jayarajan y Navdeep Pareek, Amazon Web Services

Resumen

Los datos y los metadatos asociados con una clave de AWS Key Management Service (AWS KMS) se pierden al eliminarla. Esta eliminación es irreversible, y no se pueden recuperar los datos perdidos (incluidos los datos cifrados). Puede evitar la pérdida de datos configurando un sistema de notificaciones que le avise de los cambios de estado en los estados de clave de sus claves de AWS KMS.

Este patrón le muestra cómo supervisar los cambios de estado en las claves de AWS KMS mediante Amazon EventBridge y Amazon Simple Notification Service (Amazon SNS) para emitir notificaciones automáticas siempre que el estado clave de una clave de AWS KMS cambie a o. `Disabled` `PendingDeletion` Por ejemplo, si un usuario intenta deshabilitar o eliminar una clave de AWS KMS, recibirá una notificación por correo electrónico con detalles sobre el intento de cambio de estado. También puede usar este patrón para programar la eliminación de las claves de AWS KMS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS con un usuario de AWS Identity and Access Management (IAM)
- Una clave de AWS KMS

Arquitectura

Pila de tecnología

- Amazon EventBridge
- AWS Key Management Service (AWS KMS)
- Amazon Simple Notification Service (Amazon SNS)

Arquitectura de destino

El siguiente diagrama muestra una arquitectura para crear un proceso automatizado de supervisión y notificación que detecta cualquier cambio en el estado de una clave de AWS KMS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario deshabilita o programa la eliminación de una clave de AWS KMS.
2. Una EventBridge regla evalúa la programación `Disabled` o el `PendingDeletion` evento.
3. La EventBridge regla invoca el tema Amazon SNS.
4. Amazon SNS envía un mensaje de notificación por correo electrónico a los usuarios.

> **Note**
>
> Puede personalizar el mensaje de correo electrónico para adaptarlo a las necesidades de su organización. Recomendamos incluir información sobre las entidades en las que se usa la clave de AWS KMS. Esto puede ayudar a los usuarios a comprender el impacto de eliminar la clave de AWS KMS. También puede programar una notificación de recordatorio por correo electrónico que se envíe uno o dos días antes de eliminar la clave de AWS KMS.

Automatización y escala

La CloudFormation pila de AWS implementa todos los recursos y servicios necesarios para que este patrón funcione. Puede implementar el patrón de forma independiente en una sola cuenta o mediante AWS CloudFormation StackSets para varias cuentas o unidades organizativas independientes en AWS Organizations.

Tools (Herramientas)

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS. La CloudFormation plantilla de este patrón describe todos los recursos de AWS que desee y los CloudFormation aprovisiona y configura automáticamente.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. EventBridge ofrece un flujo de datos en tiempo real desde sus propias aplicaciones y servicios de AWS, y dirige esos datos a objetivos

como AWS Lambda. EventBridge simplifica el proceso de creación de arquitecturas basadas en eventos.

- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.

Código

El código de este patrón está disponible en el repositorio GitHub Monitor AWS KMS Keys Disable and Scheduled Delete.

Epics

Implemente la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Clone el repositorio de claves, deshabilitación y eliminación programada de claves de AWS KMS de GitHub Monitor en su máquina local ejecutando el siguiente comando: `git clone https://github.com/aws-samples/aws-kms-deletion-notification`	Administrador de AWS, arquitecto de la nube
Actualice los parámetros de la plantilla.	En un editor de código, abra la `Alerting-KMS-Events.yaml` CloudFormation plantilla que ha clonado del repositorio y, a continuación, actualice los siguientes parámetros:	Administrador de AWS, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	• En `DestinationEmailAddress`, introduzca la dirección de correo electrónico activa en la que desee recibir la notificación de SNS. • Para `SNSTopicName`, ingrese un nombre para su tema SNS.	

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla.	1. Inicie sesión en la consola de administración de AWS y abra la consola de CloudFormation . 2. En el panel de navegación, seleccione Crear pila y, a continuación, seleccione Con nuevos recursos (estándar). 3. En la página Identificar recursos, seleccione Siguiente. 4. En la página Especificar plantilla, en Origen de la plantilla, seleccione Cargar un archivo de plantilla. 5. Elija Elegir archivo, seleccione el `Alerting-KMS-Events.yaml` archivo del GitHub repositorio clonado y, a continuación, elija Siguiente. 6. En Nombre de la pila, introduzca el nombre de la pila. 7. Seleccione Enviar.	Administrador de AWS, arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirme la suscripción por correo electrónico.	Una vez que la CloudFormation plantilla se haya	Administrador de AWS, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	implementado correctamente, Amazon SNS envía un mensaje de confirmación de suscripción a la dirección de correo electrónico que proporcionó en CloudFormation la plantilla. Debe confirmar esta suscripción de correo electrónico para recibir notificaciones. Para obtener más información, consulte Cómo confirmar la suscripción en la Guía para desarrolladores de Amazon SNS.	

Pruebe la notificación de la suscripción

Tarea	Descripción	Habilidades requeridas
Deshabilite las claves de AWS KMS.	1. Inicie sesión en la consola de administración de AWS y abra la consola de AWS KMS. 2. Para cambiar la región, elija el nombre de la región que se muestra actualmente y, a continuación, seleccione la región a la que desee cambiar. 3. En el panel de navegación, elija Claves administradas por el cliente.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	4. Seleccione la casilla de verificación de las claves de AWS KMS que quiere habilitar o deshabilitar. 5. Para deshabilitar una clave de AWS KMS, seleccione Key actions (Acciones de claves), y posteriormente, Disable (Deshabilitar).	
Valide la suscripción.	Confirme que ha recibido la notificación de Amazon SNS por correo electrónico.	Administrador de AWS

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Elimine la pila CloudFormation .	1. Inicie sesión en la consola de administración de AWS y abra la consola de CloudFormation . 2. En el panel de navegación, seleccione Stacks (Pilas). 3. Seleccione la pila que creó anteriormente y, a continuación, seleccione Eliminar.	Administrador de AWS

Recursos relacionados

- AWS CloudFormation (documentación de AWS)

- Creación de una pila en la CloudFormation consola de AWS (CloudFormation documentación de AWS)
- Creación de arquitecturas basadas en eventos en AWS (documentación de AWS Workshop Studio)
- Prácticas recomendadas de AWS Key Management Service (documento técnico de AWS)
- Prácticas recomendadas de seguridad para AWS Key Management Service (AWS KMS) (Guía del desarrollador de AWS KMS)

Información adicional

Amazon SQS proporciona cifrado en tránsito de forma predeterminada. Para satisfacer las prácticas recomendadas de seguridad, también puede habilitar el cifrado en el servidor para Amazon SNS mediante una clave de AWS KMS gestionada por el cliente.

Preserve el espacio IP enrutable en los diseños de VPC de varias cuentas para subredes que no son de carga de trabajo

Adam Spicer, Amazon Web Services

Resumen

Amazon Web Services (AWS) ha publicado prácticas recomendadas que animan a usar subredes dedicadas en una nube privada virtual (VPC) tanto para conexiones de puerta de enlace de tránsito como para los puntos de conexión del equilibrador de carga de la puerta de enlace (para admitir AWS Network Firewall o dispositivos de terceros). Estas subredes se utilizan para contener interfaces de red elásticas para estos servicios. Si utiliza AWS Transit Gateway y una puerta de enlace de equilibrador de carga, se crean dos subredes en cada zona de disponibilidad para la VPC. Debido a la forma en que VPCs están diseñadas, estas subredes adicionales no pueden ser más pequeñas que una máscara /28 y pueden consumir un valioso espacio IP enrutable que, de otro modo, podría usarse para cargas de trabajo enrutables. Este patrón muestra cómo se puede utilizar un rango de enrutamiento entre dominios sin clase (CIDR) secundario y no enrutable para estas subredes dedicadas a fin de ayudar a preservar el espacio IP enrutable.

Requisitos previos y limitaciones

Requisitos previos

- Estrategia de múltiples VPC para un espacio IP enrutable
- Un rango de CIDR no enrutable para los servicios que está utilizando (conexión de puerta de enlace de tránsito y conexiones al equilibrador de carga de la puerta de enlace o puntos de conexión de Network Firewall)

Arquitectura

Arquitectura de destino

Este patrón incluye dos arquitecturas de referencia: una arquitectura tiene subredes para los adjuntos de la pasarela de tránsito (TGW) y un punto final de Gateway Load Balancer (GWLBe), y la segunda arquitectura tiene subredes solo para los adjuntos de la TGW.

Arquitectura 1: VPC conectada a TGW-con enrutamiento de entrada a un dispositivo

El siguiente diagrama representa una arquitectura de referencia para una VPC que abarca dos zonas de disponibilidad. Al entrar, la VPC utiliza un patrón de enrutamiento de entrada para dirigir el tráfico destinado a la subred pública a bump-in-the-wire un dispositivo para inspeccionar el firewall. Un adjunto de TGW admite la salida de las subredes privadas a una VPC independiente.

Este patrón utiliza un rango CIDR no enrutable para la subred adjunta del TGW y la subred. GWLBe En la tabla de enrutamiento de TGW, este CIDR no enrutable se configura con una ruta de agujero negro (estática) mediante un conjunto de rutas más específicas. Si las rutas se propagaran a la tabla de enrutamiento de TGW, se aplicarían estas rutas de agujero negro más específicas.

En este ejemplo, el CIDR enrutable /23 se divide y se asigna completamente a las subredes enrutables.

Arquitectura 2: VPC adjunta a TGW

El siguiente diagrama representa otra arquitectura de referencia para una VPC que abarca dos zonas de disponibilidad. Una conexión de TGW admite el tráfico de salida (egreso) de las subredes privadas a una VPC independiente. Utiliza un rango CIDR no enrutable solo para la subred de conexión de TGW. En la tabla de enrutamiento de TGW, este CIDR no enrutable se configura con una ruta de agujero negro mediante un conjunto de rutas más específicas. Si las rutas se propagaran a la tabla de enrutamiento de TGW, se aplicarían estas rutas de agujero negro más específicas.

En este ejemplo, el CIDR enrutable /23 se divide y se asigna completamente a las subredes enrutables.

Tools (Herramientas)

Servicios y recursos de AWS

- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS. En este patrón, las VPC secundarias CIDRs se utilizan para conservar el espacio IP enrutable en la carga de trabajo. CIDRs
- El enrutamiento de ingreso de la puerta de enlace de Internet (asociaciones de periferia) se puede utilizar junto con los puntos de conexión del equilibrador de carga de la puerta de enlace para subredes dedicadas no enrutables.

- AWS Transit Gateway es un centro central que conecta VPCs las redes locales. Según este patrón, VPCs están conectados centralmente a una puerta de enlace de tránsito y los adjuntos a la puerta de enlace de tránsito están en una subred dedicada no enrutable.
- Los equilibradores de carga de la puerta de enlace permiten implementar, escalar y administrar dispositivos virtuales, como firewalls, sistemas de prevención y detección de intrusiones así como sistemas de inspección profunda de paquetes. La puerta de enlace sirve como punto único de entrada y salida para todo el tráfico. En este patrón, los puntos de conexión de un equilibrador de carga de puerta de enlace se pueden usar en una subred dedicada no enrutable.
- AWS Network Firewall es un servicio de detección y prevención de intrusiones y firewall de red gestionado y con estado para la VPCs nube de AWS. En este patrón, los puntos de conexión de un firewall se pueden usar en una subred dedicada no enrutable.

Repositorio de código

En el repositorio de patrones CIDR secundarios GitHub no enrutables hay un manual y CloudFormation plantillas de AWS para este patrón. Puede usar los archivos de muestra para configurar un laboratorio de trabajo en su entorno.

Prácticas recomendadas

AWS Transit Gateway

- Utilice una subred independiente para cada archivo asociado a la VPC de la puerta de enlace de tránsito.
- Asigne una subred /28 del rango CIDR secundario no enrutable para las subredes de conexión de puerta de enlace de tránsito.
- En cada tabla de enrutamiento de la puerta de enlace de tránsito, añada una ruta estática más específica para el rango CIDR no enrutable como agujero negro.

Equilibrador de carga de puerta de enlace y enrutamiento de ingreso

- Utilice el enrutamiento de ingreso para dirigir el tráfico de Internet a los puntos de conexión del equilibrador de carga de puerta de enlace.
- Utilice una subred independiente para cada punto de conexión del equilibrador de carga de puerta de enlace.
- Asigne una subred /28 del rango CIDR secundario no enrutable para las subredes de punto de conexión de puerta de enlace del equilibrador de carga.

Epics

Crear VPCs

Tarea	Descripción	Habilidades requeridas
Determine el rango CIDR no enrutable.	Determine un rango CIDR no enrutable que se utilizará para la subred de conexión de puerta de enlace de tránsito y (opcionalmente) para cualquier subred de punto de conexión de equilibrador de carga de puerta de enlace o Network Firewall. Este rango de CIDR se utilizará como CIDR secundario para la VPC. No debe poder enrutarse desde el rango CIDR principal de la VPC ni desde la red más amplia.	Arquitecto de la nube
Determine los rangos de CIDR enrutables para. VPCs	Determine un conjunto de rangos de CIDR enrutable s que se utilizarán para su. VPCs Este rango de CIDR se utilizará como el CIDR principal de su. VPCs	Arquitecto de la nube
Crear. VPCs	Crea las tuyas VPCs y adjúntalas a la pasarela de transporte. Cada VPC debe tener un rango CIDR principal que se pueda enrutar y un rango CIDR secundari o que no se pueda enrutar, según los rangos que haya	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	determinado en los dos pasos anteriores.	

Configuración de las rutas de agujeros negros de puerta de enlace de tránsito

Tarea	Descripción	Habilidades requeridas
Crea agujeros negros más específicos que no se puedan enrutar CIDRs .	Cada tabla de enrutamiento de las pasarelas de tránsito debe tener un conjunto de rutas negras creadas para las que no se pueden enrutar. CIDRs Están configurados para garantizar que el tráfico del CIDR de la VPC secundaria no se pueda enrutar y no se filtre a la red más amplia. Estas rutas deben ser más específicas que el CIDR no enrutable que se establece como el CIDR secundario en la VPC. Por ejemplo, si el CIDR secundario no enrutable es 100.64.0.0/26, las rutas de agujero negro de la tabla de enrutamiento de la puerta de enlace de tránsito deberían ser 100.64.0.0/27 y 100.64.0.32/27.	Arquitecto de la nube

Recursos relacionados

- Prácticas recomendadas para implementar el Equilibrador de carga de puerta de enlace
- Arquitecturas de inspección distribuida con el Equilibrador de carga de puerta de enlace

- Día de inmersión en redes: laboratorio de firewall de Internet a VPC
- Prácticas recomendadas de diseño de una puerta de enlace de tránsito

Información adicional

El rango CIDR secundario no enrutable también puede resultar útil cuando se trabaja con implementaciones de contenedores de mayor escala que requieren un gran conjunto de direcciones IP. Puede utilizar este patrón con una puerta de enlace NAT privada para utilizar una subred no enrutable para alojar las implementaciones de contenedores. Para obtener más información, consulte la entrada de blog sobre cómo resolver el agotamiento de la IP privada con una solución de NAT privada.

Aprovisione un producto de Terraform AWS Service Catalog mediante un repositorio de código

Dr. Rahul Sharad Gaikwad y Tamilselvan P, Amazon Web Services

Resumen

AWS Service Catalog admite el aprovisionamiento de autoservicio con gobernanza para sus configuraciones de Terraform. HashiCorp Si usa Terraform, puede usar Service Catalog como la única herramienta para organizar, gobernar y distribuir sus configuraciones de Terraform AWS a escala. Puede acceder a las funciones clave de Service Catalog, como la catalogación de plantillas de infraestructura como código (IaC) estandarizadas y previamente aprobadas, el control de acceso, el aprovisionamiento de recursos en la nube con el menor acceso privilegiado, el control de versiones, el uso compartido con miles de personas y el etiquetado. Cuentas de AWS Los usuarios finales, como ingenieros, administradores de bases de datos y científicos de datos, ven una lista de productos y versiones a los que tienen acceso y, a continuación, pueden implementarlos con una sola acción.

Este patrón le ayuda a implementar AWS recursos mediante el código de Terraform. Se accede al código de Terraform del GitHub repositorio a través de Service Catalog. Con este enfoque, puede integrar los productos con los flujos de trabajo de Terraform existentes. Los administradores pueden crear carteras de Service Catalog y añadirles AWS Launch Wizard productos mediante Terraform.

Los siguientes son beneficios de esta solución:

- Gracias a la característica de reversión de Service Catalog, si se produce algún problema durante la implementación, puede revertir el producto a una versión anterior.
- Puede identificar fácilmente las diferencias entre las versiones del producto. Esto le permite resolver los problemas durante la implementación.
- Puede configurar una conexión al repositorio en Service Catalog, por ejemplo, a GitHub o GitLab. Puede realizar cambios en los productos directamente a través del repositorio.

Para obtener información sobre las ventajas generales de AWS Service Catalog, consulte Qué es Service Catalog.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.
- Un GitHub repositorio u otro que contenga archivos de configuración de Terraform en formato ZIP. BitBucket
- AWS Serverless Application Model Interfaz de línea de comandos (AWS SAM CLI), instalada.
- AWS Command Line Interface (AWS CLI), instalado y configurado.
- Go instalado.
- Versión 3.9 de Python, instalada. AWS SAM La CLI requiere esta versión de Python.
- Permisos para escribir y ejecutar AWS Lambda funciones y permisos para acceder a los productos y carteras de Service Catalog y administrarlos.

Arquitectura

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Cuando la configuración de Terraform está lista, un desarrollador crea un archivo .zip que contiene todo el código de Terraform. El desarrollador carga el archivo .zip en el repositorio de código que está conectado a Service Catalog.
2. Un administrador asocia el producto de Terraform a una cartera de Service Catalog. El administrador también crea una restricción de lanzamiento que permite a los usuarios finales aprovisionar el producto.
3. En Service Catalog, los usuarios finales lanzan AWS recursos mediante la configuración de Terraform. Pueden elegir qué versión de producto se debe implementar.

Tools (Herramientas)

Servicios de AWS

- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Service Catalogle ayuda a gestionar de forma centralizada los catálogos de servicios de TI aprobados. AWS Los usuarios finales pueden implementar rápidamente solo los servicios de TI aprobados que necesitan, de acuerdo con las limitaciones establecidas por su organización.

Otros servicios

- Go es un lenguaje de programación de código abierto compatible con Google.
- Python es un lenguaje de programación informático de uso general.

Repositorio de código

Si necesita ejemplos de configuraciones de Terraform que pueda implementar a través de Service Catalog, puede usar las configuraciones del repositorio GitHub Amazon Macie Organization Setup Using Terraform. No es necesario usar los ejemplos de código de este repositorio.

Prácticas recomendadas

- En lugar de proporcionar los valores de las variables en el archivo de configuración de Terraform (`terraform.tfvars`), configure los valores de las variables al lanzar el producto a través de Service Catalog.
- Conceda acceso a la cartera solo a usuarios o administradores específicos.
- Cumpla con el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte las mejores prácticas de seguridad y concesión de privilegios mínimos en la documentación AWS Identity and Access Management (IAM).

Epics

Configure su equipo de trabajo local

Tarea	Descripción	Habilidades requeridas
(Opcional) Instale Docker.	Si desea ejecutar las AWS Lambda funciones en su entorno de desarrollo, instale Docker. Para ver instrucciones, consulte Install Docker Engine (Instalar motor de Docker) en la documentación de Docker.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Instale el AWS Service Catalog motor para Terraform.	1. Ingrese el siguiente comando para clonar el repositorio AWS Service Catalog Engine for Terraform.
	`git clone https://github.com/aws-samples/service-catalog-engine-for-terraform-os.git`
	2. Vaya al directorio raíz que contiene el repositorio clonado.
	3. Escriba el siguiente comando. Esto instala el motor.
	`run ./bin/bash/deploy-tre.sh -r`
	El Región de AWS conjunto de su perfil predeterminado no se utiliza durante la instalación automática. En su lugar, tiene que proporcionar la región cuando use este comando.
		DevOps ingeniero, administrador de AWS

Conectar el GitHub repositorio

Tarea	Descripción	Habilidades requeridas
Cree una conexión con el GitHub repositorio.	1. Inicie sesión en la consola de Herramientas para desarrolladores y Consola de administración de AWS, a continuación, ábrala. Para acceder a la consola de herramientas para desarrolladores, elija un servicio como AWS CodePipeline o AWS CodeDeploy. 2. En el panel de navegación izquierdo, elija Configuración y, a continuación, Conexiones. 3. Elija Crear conexión. 4. Seleccione el repositorio en el que guarde el código fuente de Terraform. Por ejemplo, puedes elegir Bitbucket o GitHub Enterprise Server. GitHub 5. Ingrese un nombre paralaconexión y, a continuación, elija Conectar. 6. Cuando se le solicite, autentique el repositorio. Una vez completada la autenticación, se crea la conexión y el estado cambia a activo.	Administrador de AWS

Creación de un producto de Terraform en Service Catalog

Tarea	Descripción	Habilidades requeridas
Cree el producto de Service Catalog.	1. Abra la consola de AWS Service Catalog. 2. Vaya a la sección Administración y, a continuación, seleccione Lista de productos. 3. Seleccione Crear producto. 4. En la página Crear producto, en la sección Detalles del producto, seleccione el tipo de producto Externo. Service Catalog utiliza este tipo de producto para respaldar los productos de Terraform Community Edition. 5. Ingrese un nombre y un propietario para el producto de Service Catalog. 6. Selecciona Especificar tu repositorio de código mediante un CodeStar proveedor. 7. Ingrese la siguiente información del repositorio: • Conéctese a su proveedor mediante AWS CodeConnections: seleccione la conexión que creó anteriormente.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	• Repositorio: seleccione el repositorio. • Rama: seleccione la rama. • Ruta del archivo de plantilla: elija la ruta donde se almacena el archivo de plantilla de código. El nombre debe terminar con `tar.gz`. 8. En Nombre y descripción de la versión, proporcione información sobre la versión del producto. 9. Seleccione Crear producto.	

Tarea	Descripción	Habilidades requeridas
Cree una cartera.	1. Abra la consola de AWS Service Catalog. 2. Vaya a la sección Administración y, a continuación, seleccione Carteras. 3. Seleccione Crear cartera. 4. Escriba los siguientes valores: • Portfolio name: `Sample terraform` • Descripción de la cartera: `Sample portfolio for Terraform configurations` • Propietario: su información de contacto, como una dirección de correo electrónico. 5. Seleccione Crear.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Agregue el producto de Terraform a la cartera.	1. Abra la consola de AWS Service Catalog. 2. Vaya a la sección Administración y, a continuación, seleccione Lista de productos. 3. Seleccione el producto de Terraform que ha creado previamente. 4. Seleccione Acciones y, a continuación, elija Agregar un producto a la cartera. 5. Seleccione la cartera `Sample terraform` . 6. Seleccione Añadir producto a la cartera.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Cree la política de acceso.	1. Abra la consola de AWS Identity and Access Management (IAM). 2. En el panel de navegación, seleccione Políticas. 3. En el panel de contenido , elija Create policy (Crear política). 4. Elija la opción JSON. 5. Ingrese la política de JSON de ejemplo en Política de acceso, en la sección Información adicional de este patrón. 6. Elija Siguiente. 7. En la página Revisar y crear, en el recuadro Nombre de la política, ingrese `TerraformResourceCreationAndArtifactAccessPolicy` . 8. Elija Crear política.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Cree una política de confianza personalizada.	1. Abra la consola de IAM. 2. Seleccione Roles en el panel de navegación. 3. Elija Crear rol. 4. En Tipo de entidad de confianza, seleccione Política de confianza personalizada. 5. En el editor de políticas de JSON, ingrese la política de JSON de ejemplo en Política de confianza, en la sección Información adicional de este patrón. 6. Elija Siguiente. 7. En Políticas de permisos, elija la `TerraformResourceCreationAndArtifactAccessPolicy` que haya creado anteriormente. 8. Elija Siguiente. 9. En Detalles del rol, ingrese `SCLaunch-product` en el recuadro Nombre del rol. **Important** El nombre del rol debe empezar por `SCLaunch`. 10. Seleccione Crear rol.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Agregue una restricción de lanzamiento al producto de Service Catalog.	1. Inicie sesión Consola de administración de AWS como usuario con permisos administrativos. 2. Abra la consola de AWS Service Catalog. 3. En el menú de navegación, seleccione Carteras. 4. Elija la cartera que creó previamente. 5. En la página Detalles de la cartera, elija la pestaña Restricciones y, a continuación, elija Crear restricción. 6. En Producto, seleccione el producto de Terraform que ha creado anteriormente. 7. En Restricción de lanzamiento, en Método, elija Escriba el nombre del rol. 8. En el recuadro Nombre del rol, ingrese `SCLaunch-product` . 9. Seleccione Crear.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Conceda acceso al producto.	1. Abra la consola de AWS Service Catalog. 2. En el menú de navegación, seleccione Carteras. 3. Elija la cartera que creó previamente. 4. Seleccione la pestaña Acceso y, a continuac ión, seleccione Conceder acceso. 5. Elija la pestaña Roles y, a continuación, seleccione el rol que deba tener acceso para implementar este producto. 6. Elija Grant access (Conceder acceso).	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Lance el producto.	1. Inicie sesión Consola de administración de AWS como usuario con permisos para implementar el producto Service Catalog. 2. Abra la consola de AWS Service Catalog. 3. En el panel de navegación, elija Productos. 4. Elija el producto que creó anteriormente y, a continuación, elija Lanzar producto. 5. Ingrese un nombre de producto y defina los parámetros necesarios. 6. Seleccione Lanzar producto.	DevOps ingeniero

Verifique la implementación

Tarea	Descripción	Habilidades requeridas
Valide la implementación.	Hay dos máquinas de AWS Step Functions estado para el flujo de trabajo de aprovisio namiento de Service Catalog: • `ManageProvisionedProductStateMachine` : Service Catalog invoca esta máquina de estados al aprovisionar un nuevo	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	producto de Terraform y al actualizar un producto aprovisionado por Terraform existente. • `TerminateProvisionedProductStateMachine` : Service Catalog invoca esta máquina de estados al finalizar un producto aprovisionado por Terraform existente. Debe comprobar los registros de la máquina de estados `ManageProvisionedProductStateMachine` para confirmar que el producto se ha aprovisionado. 1. Inicie sesión en la AWS Step Functions consola y Consola de administración de AWS, a continuación, ábrala. 2. En el panel de navegación izquierdo, elija Máquinas de estado. 3. Elija `ManageProvisionedProductStateMachine` . 4. En la lista Ejecuciones, ingrese el ID del producto aprovisionado para localizar la ejecución.	

Tarea	Descripción	Habilidades requeridas
	Note Los nombres de los buckets del backend del archivo de estados comienzan por `sc-terraform-engine-state-` . 5. Valide que se hayan creado todos los recursos necesarios en la cuenta.	

Limpieza de la infraestructura

Tarea	Descripción	Habilidades requeridas
Elimine los productos aprovisionados.	1. Inicie sesión Consola de administración de AWS como usuario con permisos para implementar el producto Service Catalog. 2. Abra la consola de AWS Service Catalog. 3. Elija Productos aprovisionados en el menú de navegación izquierdo. 4. Seleccione el producto que ha creado. 5. En la lista Acciones, seleccione Terminar.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	6. En el recuadro de texto de confirmación, ingrese `terminate` y, a continuación, seleccione Terminar el producto aprovisionado. 7. Repita estos pasos para terminar todos los productos aprovisionados.	

Tarea	Descripción	Habilidades requeridas
Retire el AWS Service Catalog motor de Terraform.	1. Inicie sesión Consola de administración de AWS como usuario con permisos administrativos. 2. Abra la consola de Amazon Simple Storage Serv 3. En el panel de navegación, elija Buckets. 4. Seleccione el bucket `sc-terraform-engine-logging-XXXX` . 5. Elija Vaciar. 6. Repita los pasos del 4 al 5 para los siguientes buckets: • `sc-terraform-engine-state-XXXX` • `terraform-engine-bootstrap-XXXX` 7. Abre la AWS CloudFormation consola y, a continuación, comprueba que estás en la dirección correcta Región de AWS. 8. En el panel de navegación izquierdo, seleccione Pilas. 9. Seleccione `SAM-TRE` y, a continuación, elija Eliminar. Espere a que se elimine la pila. 10. Seleccione `Bootstrap-TRE` y, a continuación, elija	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	Eliminar. Espere a que se elimine la pila.	

Recursos relacionados

AWS documentación

- Cómo empezar con un producto de Terraform

Documentación de Terraform

- Instalación de Terraform
- Terraform backend configuration
- Documentación de Terraform Provider AWS

Información adicional

Política de acceso

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
                }
            }
        },
        {
            "Action": [
                "s3:CreateBucket*",
                "s3:DeleteBucket*",
```

```
                "s3:Get*",
                "s3:List*",
                "s3:PutBucketTagging"
            ],
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:ListGroupResources",
                "resource-groups:DeleteGroup",
                "resource-groups:Tag"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "tag:GetResources",
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Política de confianza

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GivePermissionsToServiceCatalog",
            "Effect": "Allow",
            "Principal": {
                "Service": "servicecatalog.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
```

```
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account_id:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
TerraformExecutionRole*",
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
ServiceCatalogExternalParameterParserRole*",
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
ServiceCatalogTerraformOSParameterParserRole*"
                    ]
                }
            }
        }
    ]
}
```

Registre varios Cuentas de AWS con una sola dirección de correo electrónico mediante Amazon SES

Joe Wozniak y Shubhangi Vishwakarma, Amazon Web Services

Resumen

Este patrón describe cómo puede desvincular las direcciones de correo electrónico reales de la dirección de correo electrónico asociada a una. Cuenta de AWS Cuentas de AWS requieren que se proporcione una dirección de correo electrónico única al momento de crear la cuenta. En algunas organizaciones, el equipo que lo administra Cuentas de AWS debe asumir la carga de administrar muchas direcciones de correo electrónico únicas con su equipo de mensajería. Esto puede resultar difícil para las grandes organizaciones que administran muchas Cuentas de AWS. Además, si su sistema de correo electrónico no permite usar el símbolo + en direcciones ni usar subdirecciones, tal como se define en Sieve Email Filtering: Subaddress Extension (RFC 5233) (agregando un signo más [+] y un identificador al final de la parte local del correo, como `admin+123456789123@example.com`) este patrón permite sortear dicha limitación.

Este patrón proporciona una solución única de venta de direcciones de correo electrónico que permite a Cuenta de AWS los propietarios asociar una dirección de correo electrónico con varias Cuentas de AWS. Luego, las direcciones de correo electrónico reales de Cuenta de AWS los propietarios se asocian a estas direcciones de correo electrónico generadas en una tabla. La solución gestiona todo el correo entrante de las cuentas de correo electrónico únicas, busca al propietario de cada cuenta y, a continuación, reenvía los mensajes recibidos al propietario.

Requisitos previos y limitaciones

Requisitos previos

- Acceso administrativo a un Cuenta de AWS.
- Acceso a un entorno de desarrollo.
- (Opcional) Estar familiarizado con los AWS Cloud Development Kit (AWS CDK) flujos de trabajo y el lenguaje de programación Python le ayudará a solucionar cualquier problema o a realizar modificaciones.

Limitaciones

- La longitud total de la dirección de correo electrónico vendida es de 64 caracteres. Para obtener más información, consulta la CreateAccountreferencia de la AWS Organizations API.

Versiones de producto

- Node.js, versión 22.x o posterior
- Python 3.13 o posterior
- Paquetes de Python pip y virtualenv
- AWS CDK CLI versión 2.1019.2 o posterior
- Docker, versión 20.10x o posterior

Arquitectura

Pila de tecnología de destino

- CloudFormation pila
- AWS Lambda funciones
- Reglas y conjunto de reglas de Amazon Simple Email Service (Amazon SES)
- AWS Identity and Access Management funciones y políticas (IAM)
- Un bucket de Amazon Simple Storage Service (Amazon S3) y política de bucket
- AWS Key Management Service (AWS KMS) política clave y clave
- Tema de Amazon Simple Notification Service (Amazon SNS) y política de temas
- Tabla de Amazon DynamoDB

Arquitectura de destino

En este diagrama se muestran dos flujos:

- Flujo de venta de direcciones de correo electrónico: en el diagrama, el flujo de venta de direcciones de correo electrónico (sección inferior) comienza normalmente con una solución de venta de cuentas o con una automatización externa, o se invoca manualmente. En la solicitud, se llama a una función de Lambda con una carga útil que contiene los metadatos necesarios. La función utiliza esta información para generar un nombre de cuenta y una dirección de correo electrónico únicos, los almacena en una base de datos de DynamoDB y devuelve los valores a la

persona que llama. Luego, estos valores se pueden usar para crear una nueva Cuenta de AWS (normalmente mediante AWS Organizations).

- Flujo de reenvío de correo electrónico: este flujo se ilustra en la sección superior del diagrama anterior. Cuando Cuenta de AWS se crea una con el correo electrónico de la cuenta generado a partir del flujo de venta de direcciones de correo electrónico, AWS envía varios correos electrónicos, como la confirmación de registro de la cuenta y las notificaciones periódicas, a esa dirección de correo electrónico. Siguiendo los pasos de este patrón, configuras tu cuenta Cuenta de AWS con Amazon SES para recibir correos electrónicos de todo el dominio. Esta solución configura reglas de reenvío que permiten a Lambda procesar todos los correos electrónicos entrantes, comprobar si la dirección T0 está en la tabla de DynamoDB y, en su lugar, reenviar el mensaje a la dirección de correo electrónico del propietario de la cuenta. El uso de este proceso permite a los propietarios de las cuentas asociar varias cuentas a una sola dirección de correo electrónico.

Automatización y escala

Este patrón lo utiliza AWS CDK para automatizar completamente la implementación. La solución utiliza servicios AWS gestionados que se escalarán automáticamente (o se pueden configurar) para adaptarse a sus necesidades. Es posible que las funciones de Lambda requieran una configuración adicional para satisfacer sus necesidades de escalado. Para obtener más información, consulte Comprender el escalado de la función de Lambda en la documentación de Lambda.

Tools (Herramientas)

Servicios de AWS

- CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y administrarlos a lo largo de su ciclo de vida en todas Cuentas de AWS las regiones.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.

- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Email Service (Amazon SES) facilita poder enviar y recibir correos electrónicos a través de los dominios y direcciones de correo electrónico propios.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Herramientas necesarias para la implementación

- Entorno de desarrollo con acceso AWS CLI de IAM a su. Cuenta de AWS Para obtener más información, consulte los enlaces de la sección de recursos relacionados.
- En su sistema de desarrollo, instale lo siguiente:
  - Herramienta de línea de comandos de Git, disponible en el sitio web de descargas de Git.
  - AWS CLI Para configurar las credenciales de acceso para AWS CDK. Para obtener más información, consulte la Documentación de AWS CLI.
  - La versión 3.13 o posterior de Python, disponible en el sitio web de descargas de Python.
  - UV para la administración de paquetes de Python. Para ver instrucciones de instalación, consulte UV installation guide.
  - La versión 22.x o posterior de Node.js. Consulte la documentación de Node.js para ver las instrucciones de instalación.
  - AWS CDK CLI versión 2.1019.2 o posterior. Consulte la documentación de AWS CDK para ver las instrucciones de instalación.
  - La versión 20.10.x o posterior de Docker. Consulte la documentación de Docker para ver las instrucciones de instalación.

Código

El código de este patrón está disponible en el repositorio de correo electrónico de GitHub Cuenta de AWS fábrica.

Epics

Asigne un entorno de implementación objetivo

Tarea	Descripción	Habilidades requeridas
Identifique o cree un Cuenta de AWS.	Identifique uno existente o nuevo Cuenta de AWS al que tenga acceso administrativo completo para implementar la solución de correo electrónico.	Administrador de la nube, administrador de AWS
Configure un entorno de implementación.	Configure un entorno de implementación fácil de usar y configure las dependencias siguiendo estos pasos: 1. Configure su entorno de desarrollo con las herramientas enumeradas en la sección Herramientas. 2. Clone la base de código del repositorio de correo electrónico de GitHub Cuenta de AWS fábrica en su entorno de desarrollo mediante el comando: `git clone https://github.com/aws-samples/aws-account-factory-email` 3. En el archivo `requirements.in` (en la raíz del repositorio), actualice la línea que comienza con `aws-cdk-lib==` para	AWS DevOps, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	que coincida con la versión de AWS CDK más reciente. Para identificar cuál es la versión más reciente, use `npm view aws-cdk-lib` y busque la palabra clave “latest:”. 4. Si actualizó a la versión en `requirements.in`, use el siguiente comando para actualizar el archivo `requirements.txt` mediante UV: `uv pip compile requirements.in -o requirements.txt --python-version 3.13`	

Configuración de un dominio verificado

Tarea	Descripción	Habilidades requeridas
Identifique y asigne un dominio.	La funcionalidad de reenvío de correo electrónico requiere un dominio dedicado. Identifique y asigne un dominio o subdominio que pueda verificar con Amazon SES. Este dominio debe estar disponible para recibir el correo electrónico entrante en el Cuenta de AWS lugar donde esté implementada la	Administrador de la nube, administrador de redes, administrador de DNS

Tarea	Descripción	Habilidades requeridas
	solución de reenvío de correo electrónico. Requisitos del dominio: • El dominio debe ser un dominio o subdominio estándar. • El dominio debe poder resolverse mediante DNS de forma externa, ya que se utilizará para recibir correos electrónicos de personas ajenas a la organización.	
Compruebe el dominio.	Compruebe que el dominio identificado se puede utilizar para aceptar el correo entrante. Complete las instrucciones de Verificación de su dominio para la recepción de correos electrónicos de Amazon SES en la documentación de Amazon SES. Esto requerirá la coordinación con la persona o el equipo responsable de los registros de DNS del dominio.	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Configure los registros MX.	Configure su dominio con registros MX que apunten a los puntos de enlace de Amazon SES de su Cuenta de AWS región. Para obtener más información, consulte Publicar un registro MX para la recepción de correos electrónicos de Amazon SES en la documentación de Amazon SES.	Administrador de la nube, administrador de redes, administrador de DNS

Implemente la solución de venta y reenvío de correo electrónico

Tarea	Descripción	Habilidades requeridas
Modifique los valores predeterminados en `cdk.json`.	Edite algunos de los valores predeterminados del archivo `cdk.json` (en la raíz del repositorio) para que la solución funcione correctam ente una vez implementada. 1. Modifique el valor `SES_DOMAIN_NAME` para que coincida con el nombre de dominio que verificó anteriormente. 2. Modifique el valor `ADDRESS_FROM` para incluir el mismo dominio en el que se encuentra `SES_DOMAIN_NAME` . Su equipo de nube debe	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	determinar la parte local de la dirección. Esta dirección se convierte en la dirección `FROM` de todos los correos electrónicos que se reenvían a través de la solución. 3. Modifique el valor `ADDRESS_ADMIN` para que coincida con la dirección de correo electrónico a la que se reenviarán los mensajes entrantes que no coincidan . Este valor debe ser una dirección de correo electrónico válida y operativa.	

Tarea	Descripción	Habilidades requeridas

Implemente la solución de venta y reenvío de correo electrónico.	1. Cree un entorno virtual Python:
	`uv venv --python 3.13`
	2. Active el entorno virtual Python:
	`source .venv/bin/activate`
	O bien, en la plataforma Windows, utilice:
	`% .venv\Scripts\activate.bat`
	3. Instale todos los requisitos de Python sin errores:
	`uv pip install -r requirements.txt`
	4. Sintetice la CloudFormation plantilla:
	`cdk synth`
	Confirme que no hay errores y que la CloudFormation plantilla completa contiene el resultado esperado.
	5. (Opcional) Si va a implementar el AWS CDK código en la región Cuenta
		Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas

	de AWS o en la actual por primera vez, inicie el entorno. Para obtener más información, consulte AWS CDK Bootstrapping en la documentación. AWS CDK
	`cdk bootstrap aws://AWS-ACCOUNT-NUMBER/REGION`
	Sustituya `AWS-ACCOUNT-NUMBER` y `REGION` por valores reales.
	6. Implemente la solución:
	`cdk bootstrap`
	`cdk deploy`
	Los comandos deberían completarse sin errores.	

Tarea	Descripción	Habilidades requeridas
Compruebe que la solución se haya implementado.	Compruebe que la solución se ha implementado correctam ente antes de comenzar las pruebas: 1. Abra la CloudForm ation consola y busque una CloudFormation pila que contenga el nombre `AwsMailFw dStack` . 2. Confirme que esta pila `AwsMailFwdStack` tenga los siguientes recursos: • Funciones de Lambda • Regla y conjunto de reglas de Amazon SES • Roles y políticas de IAM • Política de bucket y bucket de Amazon S3 • AWS KMS clave y política clave • Tema y política de Amazon SNS • Tabla de DynamoDB	Desarrollador de aplicaciones, AWS DevOps

Compruebe que la venta y el reenvío de correo electrónico funcionan según lo previsto

Tarea	Descripción	Habilidades requeridas
Verifique que la API está en funcionamiento.	En este paso, debe enviar los datos de prueba a la API de la solución y confirmar	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	que la solución produce el resultado esperado y que las operaciones de backend se han realizado según lo previsto. Ejecute manualmente la función Vend Email de la función de Lambda mediante una entrada de prueba. (Para ver un ejemplo, consulte el archivo sample_vend_request.json). Para `OwnerAddress` , utilice una dirección de correo electrónico válida. La API debería devolver el nombre de la cuenta y el correo electrónico de la cuenta con los valores esperados.	

Tarea	Descripción	Habilidades requeridas
Compruebe que el correo electrónico se está reenviando.	En este paso, envía un correo electrónico de prueba a través del sistema y comprueba que el correo electrónico se ha reenviado al destinatario previsto. 1. Obtenga el correo electrónico de la cuenta del último paso. 2. Envíe un correo electrónico a esta dirección con el tema de la prueba y el cuerpo del texto. 3. Confirme que recibió el correo electrónico en la dirección de correo electrónico del propietario de la cuenta. 4. Confirme que el correo electrónico que ha recibido tiene una dirección `FROM` que coincide con la configuración `ADDRESS_FROM` indicada en `cdk.json`. 5. Confirme que el asunto y el cuerpo del correo electrónico recibido son los mismos que los del mensaje enviado originalmente.	Desarrollador de aplicaciones, AWS DevOps

Resolución de problemas

Problema	Solución
El sistema no reenvía el correo electrónico como se esperaba.	Compruebe que la configuración es correcta: 1. Debería haber completado el proceso de verificación de Amazon SES para su dominio. 2. Su dominio debe estar configurado correctamente con registros MX que apunten a los puntos de enlace de Amazon SES de su Cuenta de AWS región. Para obtener más información, consulte Publicar un registro MX para la recepción de correos electrónicos de Amazon SES en la documentación de Amazon SES. Después de verificar la configuración de dominio, siga estos pasos: 1. Abra la CloudWatch consola de Amazon de la cuenta y la región en las que implement ó la solución y navegue hasta los grupos de CloudWatch registros en el panel de navegación. 2. Busque en la lista de los grupos de registros para `SesMailForwardLogGroup` . 3. Investigue los registros de este grupo para ver si se ha generado algún error durante el proceso de venta y reenvío de correo electrónico.
Cuando intenta implementar la AWS CDK pila, recibe un error similar al siguiente:	En la mayoría de las instancias, este mensaje de error significa que la región a la que se dirige no tiene todos los servicios de AWS

Problema	Solución
“Template format error: Unrecognized resource types”	disponibles. Si utilizas una EC2 instancia de Amazon para implementar la solución, es posible que te dirijas a una región diferente de la región en la que se ejecuta la instancia. **Note** De forma predeterminada, se AWS CDK despliega en la región y la cuenta que configuraste en. AWS CLI Posibles soluciones: 1. Revise los servicios de AWS por región para comprobar si todos los servicios necesarios para esta solución (consulte la sección sobre el conjunto de tecnologías de TargetRegión de AWS que aparece anteriormente en este patrón) están incluidos en la lista de destinatarios. 2. Si utiliza una EC2 instancia y se orienta a una región distinta de la región en la que se ejecuta la instancia, asegúrese de configura r la variable de `AWS_DEFAULT_REGION` entorno o establecer una región con ella AWS CLI antes de implementar la solución. Para obtener más información, consulte la sección Configuración de variables de entorno que se AWS CLI encuentra en la AWS CLI documentación. Como alternativa, puede modificar el archivo `app.py` en la raíz del repositorio para incluir un ID y región de cuenta de codificación rígida y una región

Problema	Solución
	siguiendo las instrucciones de la documentación de AWS CDK sobre entornos.
Al implementar la solución, recibirá el siguiente mensaje de error: «Fallo en la implementación: Error AwsMailFwdStack: no se encontró el parámetro bootstrap /hnb659fds/version /cdk- de SSM. ¿Arrancó el entorno? Please run 'cdk bootstrap'"	Si nunca has desplegado ningún AWS CDK recurso en la región a la que te diriges, primero tendrás que ejecutar el `cdk bootstrap` comando, tal Cuenta de AWS y como indica el error. Si sigue recibiendo este error después de usar el comando de arranque, es posible que esté intentando implementar la solución en una región distinta de la región del entorno de desarrollo. Para resolver este problema, defina la variable de `AWS_DEFAULT_REGION` entorno o defina una región con la AWS CLI antes de implementar la solución. Como alternativa, puede modificar el archivo `app.py` en la raíz del repositorio para incluir un ID y región de cuenta de codificación rígida y una región siguiendo las instrucciones de la documentación de AWS CDK sobre entornos.

Recursos relacionados

- Para obtener ayuda con la instalación AWS CLI, consulte Instalación o actualización a la versión más reciente de AWS CLI.
- Para obtener ayuda para configurar el AWS CLI con credenciales de acceso de IAM, consulte Configurar los ajustes del AWS CLI.
- Para obtener ayuda con el AWS CDK, consulte Primeros pasos con. AWS CDK

Información adicional

Costos

Al implementar esta solución, el Cuenta de AWS propietario puede incurrir en costos asociados con el uso de los siguientes servicios. Es importante que comprenda cómo se facturan estos servicios para estar al tanto de los posibles cargos. Para obtener información sobre precios, consulte las siguientes páginas:

- Precios de Amazon SES
- Precios de Amazon S3
- AWS KMS precios
- AWS Lambda precios
- Precios de Amazon DynamoDB

Configure la resolución de DNS para redes híbridas en un entorno de AWS de una sola cuenta

Abdullahi Olaoye, Amazon Web Services

Resumen

Este patrón describe cómo configurar una arquitectura de sistema de nombres de dominio (DNS) totalmente híbrida que permita la resolución end-to-end mediante DNS de recursos locales, recursos de AWS y consultas de DNS de Internet, sin sobrecargas administrativas. El patrón describe cómo configurar las reglas de reenvío de Amazon Route 53 Resolver que determinan dónde debe enviarse una consulta de DNS que se origina en AWS, en función del nombre de dominio. Las consultas de DNS para los recursos en las instalaciones se reenvían a los solucionadores de DNS en las instalaciones. Route 53 Resolver resuelve las consultas de DNS para los recursos de AWS y las consultas de DNS de Internet.

Este patrón cubre la resolución de DNS híbrido en un entorno de cuenta única de AWS. Para obtener información sobre la configuración de consultas de DNS salientes en un entorno de varias cuentas de AWS, consulte el patrón Configurar la resolución de DNS para redes híbridas en un entorno de AWS de varias cuentas.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS
- Crear una nube privada virtual (VPC) en la cuenta de AWS.
- Conectividad de red entre el entorno en las instalaciones y VPC a través de los servicios de AWS Virtual Private Network (AWS VPN) o AWS Direct Connect
- Direcciones IP de sus resolutores de DNS en las instalaciones (accesibles desde su VPC)
- Nombre de dominio o subdominio para reenviar a los solucionadores en las instalaciones (por ejemplo, onprem.mydc.com)
- Nombre de dominio/subdominio de la zona alojada privada de AWS (por ejemplo, myvpc.cloud.com)

Arquitectura

Pila de tecnología de destino

- Zona alojada privada de Amazon Route 53
- Amazon Route 53 Resolver
- Amazon VPC
- AWS VPN o Direct Connect

Arquitectura de destino

Tools (Herramientas)

- Amazon Route 53 Resolver facilita la nube híbrida a los clientes empresariales al permitir una resolución de consultas de DNS perfecta en toda la nube híbrida. Puede crear puntos de enlace de DNS y reglas de reenvío condicional para resolver los espacios de nombres de DNS entre su centro de datos local y el suyo. VPCs
- La zona alojada privada de Amazon Route 53 es un contenedor que contiene información sobre cómo desea que Route 53 responda a las consultas de DNS de un dominio y sus subdominios dentro de uno o varios VPCs que cree con el servicio Amazon VPC.

Epics

Configure una zona alojada privada

Tarea	Descripción	Habilidades requeridas
Cree una zona alojada privada de Route 53 para un nombre de dominio reservado de AWS, como myvpc.cloud.com.	Esta zona contiene los registros de DNS de los recursos de AWS que deben resolverse desde el entorno en las instalaci ones. Para obtener instrucci ones, consulte Crear una zona alojada privada en la documentación de Route 53.	Administrador de red, administrador del sistema
Asocie esta zona alojada privada con la VPC de la VPC.	Para permitir que los recursos de la VPC resuelvan los	Administrador de red, administrador del sistema

Tarea	Descripción	Habilidades requeridas
	registros DNS en esta zona alojada privada, debe asociar la VPC a la zona alojada. Para obtener instrucciones, consulte Crear una zona alojada privada en la documentación de Route 53.	

Configure los puntos de conexión de Route 53 Resolver

Tarea	Descripción	Habilidades requeridas
Crear un punto de conexión de entrada	Route 53 Resolver utiliza un punto de conexión de entrada para recibir las consultas de DNS de los solucionadores en las instalaciones. Para obtener instrucciones, consulte Reenviar consultas DNS entrantes a su cuenta VPCs en la documentación de Route 53. Anote la dirección IP del punto de conexión entrante.	Administrador de red, administrador del sistema
Crear un punto de conexión de salida	Route 53 Resolver utiliza un punto de conexión de salida para enviar las consultas de DNS de los solucionadores en las instalaciones. Para obtener instrucciones, consulte Reenvío de consultas de DNS de salida a su red en la documentación de Route	Administrador de red, administrador del sistema

Tarea	Descripción	Habilidades requeridas
	53. Anote el ID del punto de conexión de salida.	

Configure una regla de reenvío y asóciela a su VPC

Tarea	Descripción	Habilidades requeridas
Crear una regla de reenvío para un dominio en las instalaciones	Esta regla indicará a Route 53 Resolver que reenvíe cualquier consulta de DNS para los dominios en las instalaciones (como onprem.mydc.com) a los solucionadores de DNS en las instalaciones. Para crear esta regla, necesitará las direccion es IP de los resolutores de DNS en las instalaciones y el ID del punto de conexión de salida de Route 53 Resolver. Para obtener instrucciones, consulte Administración de reglas de reenvío en la documentación de Route 53.	Administrador de red, administrador del sistema
Asocie la regla de reenvío a su VPC.	Para que la regla de reenvío entre en vigor, debe asociarla a su VPC. Luego, Route 53 Resolver tiene en cuenta la regla al resolver un dominio. Para obtener instrucciones, consulte Administración de reglas de reenvío en la documentación de Route 53.	Administrador de red, administrador del sistema

Configuración de solucionadores DNS en las instalaciones

Tarea	Descripción	Habilidades requeridas
Configure el reenvío condicional en los solucionadores de DNS en las instalaciones.	Para que las consultas de DNS se envíen a la zona alojada privada de Route 53 desde el entorno en las instalaciones, debe configurar el reenvío condicional en los solucionadores de DNS en las instalaciones. Esto indica a los solucionadores de DNS que reenvíen todas las consultas de DNS del dominio de AWS (por ejemplo, para myvpc.cloud.com) a la dirección IP del punto de conexión entrante de Route 53 Resolver.	Administrador de red, administrador del sistema

Pruebe la resolución de DNS end-to-end

Tarea	Descripción	Habilidades requeridas
Probar la resolución DNS desde AWS en el entorno en las instalaciones.	Desde un servidor de la VPC, realice una consulta de DNS para un dominio en las instalaciones (como server1.onprem.mydc.com).	Administrador de red, administrador del sistema
Probar la resolución DNS desde AWS en el entorno en las instalaciones.	Desde un servidor en las instalaciones, realice la resolución de DNS para un dominio de AWS (como server1.myvpc.cloud.com).	Administrador de red, administrador del sistema

Recursos relacionados

- Administración centralizada de DNS de la nube híbrida con Amazon Route 53 y AWS Transit Gateway (AWS Transit Gateway (AWS Transit Gateway (Blog de AWS Networking y Content Delivery)
- Simplifique la administración de DNS en un entorno multicuenta con Route 53 Resolver (publicación del blog de AWS Security)
- Trabajar con zonas alojadas privadas (documentación de Route 53)
- Introducción a Route 53 Resolver (documentación de Route 53)

Configure automáticamente los bots de UiPath RPA en Amazon EC2 mediante AWS CloudFormation

Dr. Rahul Sharad Gaikwad y Tamilselvan P, Amazon Web Services

Resumen

Este patrón explica cómo puede implementar bots de automatización robótica de procesos (RPA) en instancias de Amazon Elastic Compute Cloud (Amazon EC2). Utiliza una canalización de EC2 Image Builder para crear una Amazon Machine Image (AMI) personalizada. Una AMI es una imagen de máquina virtual (VM) preconfigurada que contiene el sistema operativo (SO) y el software preinstalado para implementar EC2 instancias. Este patrón utiliza CloudFormation plantillas de AWS para instalar la edición UiPath Studio Community en la AMI personalizada. UiPath es una herramienta de RPA que le ayuda a configurar robots para automatizar sus tareas.

Como parte de esta solución, las instancias de EC2 Windows se lanzan mediante la AMI base y la aplicación UiPath Studio se instala en las instancias. El patrón utiliza la herramienta Microsoft System Preparation (Sysprep) para duplicar la instalación personalizada de Windows. Después, elimina la información del host y crea una AMI final de la instancia. A continuación, puede lanzar las instancias bajo demanda mediante la AMI final con sus propias convenciones de nomenclatura y configuración de supervisión.

Nota: Este patrón no proporciona ninguna información sobre el uso de bots de RPA. Para obtener esa información, consulte la UiPath documentación. También puede usar este patrón para configurar otras aplicaciones de bots de RPA personalizando los pasos de instalación en función de sus necesidades.

Este patrón proporciona las siguientes automatizaciones y ventajas:

- Implementación y uso compartido de aplicaciones: puede crear Amazon EC2 AMIs para el despliegue de aplicaciones y compartirlas en varias cuentas a través de una canalización de EC2 Image Builder, que utiliza CloudFormation plantillas de AWS como scripts de infraestructura como código (IaC).
- EC2 Aprovisionamiento y escalado de Amazon: las plantillas de CloudFormation IaC proporcionan secuencias de nombres de ordenadores personalizadas y automatizan las uniones de Active Directory.

- Observabilidad y supervisión: el patrón configura los CloudWatch paneles de Amazon para ayudarte a monitorear las EC2 métricas de Amazon (como el uso de CPU y disco).
- Ventajas de la RPA para su empresa: la RPA mejora la precisión porque los robots pueden realizar las tareas asignadas de forma automática y coherente. La RPA también aumenta la velocidad y la productividad porque elimina las operaciones que no añaden valor y gestiona las actividades repetitivas.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Permisos de AWS Identity and Access Management (IAM) para implementar plantillas CloudFormation
- Políticas de IAM para configurar la distribución de AMI entre cuentas con Image Builder EC2

Arquitectura

1. El administrador proporciona la AMI de Windows básica en el `ec2-image-builder.yaml` archivo e implementa la pila en la CloudFormation consola.
2. La CloudFormation pila implementa la canalización EC2 Image Builder, que incluye los siguientes recursos:
   - `Ec2ImageInfraConfiguration`
   - `Ec2ImageComponent`
   - `Ec2ImageRecipe`
   - `Ec2AMI`
3. La canalización de EC2 Image Builder lanza una EC2 instancia temporal de Windows mediante la AMI base e instala los componentes necesarios (en este caso, UiPath Studio).
4. EC2 Image Builder elimina toda la información del host y crea una AMI desde Windows Server.
5. Actualiza el `ec2-provisioning yaml` archivo con la AMI personalizada y lanza varias EC2 instancias en función de sus requisitos.

6. La macro Count se implementa mediante una CloudFormation plantilla. Esta macro proporciona una propiedad Count para CloudFormation los recursos, de modo que puede especificar fácilmente varios recursos del mismo tipo.
7. Actualiza el nombre de la macro en el CloudFormation `ec2-provisioning.yaml` archivo y despliega la pila.
8. El administrador actualiza el archivo `ec2-provisioning.yaml` en función de los requisitos y lanza la pila.
9. La plantilla implementa EC2 instancias con la aplicación UiPath Studio.

Tools (Herramientas)

Servicios de AWS

- AWS le CloudFormation ayuda a modelar y gestionar los recursos de infraestructura de forma automatizada y segura.
- Amazon le CloudWatch ayuda a observar y supervisar los recursos y las aplicaciones en AWS, en las instalaciones y en otras nubes.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática segura y de tamaño variable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- EC2 Image Builder simplifica la creación, las pruebas y el despliegue de máquinas virtuales e imágenes de contenedores para su uso en AWS o de forma local.
- Amazon le EventBridge ayuda a crear aplicaciones basadas en eventos a escala en AWS, sistemas existentes o aplicaciones de software como servicio (SaaS).
- AWS Identity and Access Management (IAM) le ayuda a controlar de forma segura el acceso a los recursos de AWS. Con IAM, puede administrar de forma centralizada los permisos que controlan a qué recursos de AWS pueden acceder los usuarios. Utilice IAM para controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos.
- AWS Lambda es un servicio de computación controlado por eventos sin servidor que permite ejecutar código para prácticamente cualquier tipo de aplicación o servicio backend, sin aprovisionar ni administrar servidores. Puede utilizar funciones de Lambda desde más de 200 servicios de AWS y aplicaciones SaaS y pagar solo por el consumo realizado.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

- AWS Systems Manager Agent (SSM Agent) ayuda a Systems Manager a actualizar, gestionar y configurar EC2 instancias, dispositivos periféricos, servidores locales y máquinas virtuales ()VMs.

Repositorios de código

El código de este patrón está disponible en la configuración del bot de GitHub UiPath RPA mediante el repositorio. CloudFormation El patrón también usa una macro que está disponible en el repositorio de CloudFormation macros de AWS.

Prácticas recomendadas

- AWS lanza nuevas versiones de Windows AMIs cada mes. Contienen los últimos parches del sistema operativo, controladores y agentes de lanzamiento. Le recomendamos que aproveche las AMI más recientes al lanzar nuevas instancias o al crear sus propias imágenes personalizadas.
- Aplique todos los parches de seguridad disponibles para Windows o Linux durante la creación de imágenes.

Epics

Implemente una canalización de imágenes para la imagen base

Tarea	Descripción	Habilidades requeridas
Configure una canalización EC2 de Image Builder.	1. Clone la configuración del bot de UiPath RPA mediante el CloudFormation repositorio o descargue la `ec2-image-builder.yaml` plantilla del repositorio. 2. Inicie sesión en la consola de administración de AWS y abra la CloudFormation consola de AWS. 3. Seleccione Crear pila. 4. En la sección Specify template (Especificar	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	plantilla) seleccione Upload a template file (Cargar un archivo de plantilla). 5. Busque y cargue la plantilla `ec2-image-builder.yaml` desde su computadora y, a continuación, seleccione Siguiente. 6. Proporcione parámetros de entrada para su pila o acepte los valores predeterminados. Elija Siguiente. **Note** El número y los valores de los parámetros pueden variar en función de los valores de entrada. 7. Si lo desea, configure las opciones de pila y luego elija Siguiente. 8. Revise los detalles de la pila. 9. Al final de la pantalla, seleccione la casilla de verificación para confirmar las capacidades y, a continuación, seleccione Enviar.	

Tarea	Descripción	Habilidades requeridas
	10. Supervise el progreso de la pila. Cuando el estado sea `CREATE_COMPLETE` , la implementación estará lista.	
Vea EC2 la configuración de Image Builder.	La configuración EC2 de Image Builder incluye la configuración de la infraestructura, la configuración de distribución y la configuración de escaneo de seguridad. Para ver la configuración: 1. Abra la consola EC2 de Image Builder. 2. En el panel de navegación, vaya a varios ajustes de Generador de imágenes. **Note** Como práctica recomendada, las actualizaciones de EC2 Image Builder se deben realizar únicamente a través de la CloudFormation plantilla.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Puede ver la canalización de imágenes.	Para ver la canalización de imágenes desplegada: 1. En la consola EC2 de Image Builder, elija Image Pipelines en el panel de navegación. 2. Seleccione la canalización de imágenes que ha creado. 3. Vea los detalles de configuración de las imágenes de salida, la receta de la imagen, la configuración de la infraestructura, los ajustes de distribución, EventBridge las reglas de Amazon y las etiquetas.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Ver los registros de Generador de imágenes.	EC2 Los registros de Image Builder se agrupan en grupos de CloudWatch registros. Para ver los registros en CloudWatch: 1. Abra la consola de CloudWatch . 2. En el panel de navegación, elija Logs (Registros), Log groups (Grupos de registro) . 3. Elija el nombre del grupo de registros. EC2 Los registros de Image Builder se agregan al grupo de registros `/aws/imagebuilder/XXX` . 4. Compruebe los registros más recientes del flujo de registro correspondiente para ver si se ha producido algún error al ejecutar la canalización de imágenes. EC2 Los registros de Image Builder también se almacenan en un bucket de S3. Para consultar los registros en el bucket: 1. Abra la consola de Amazon S3.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	2. En la lista de Buckets, seleccione el nombre del bucket. Los registros se agregan en el bucket de S3 `<stack-name>-XXXXX X` .	
Cargue el UiPath archivo en un bucket de S3.	1. Descargue el `.msi` archivo de UiPath Studio desde la ubicación https://download.uipath.com UiPathStudioCommunity/.msi. 2. Cargue el archivo qen un bucket de S3. 3. Actualice el nombre del bucket y la clave de archivo en la plantilla `ec2-image -builder.yaml` , en la sección de datos de usuario, línea 310.	AWS DevOps

Implementación y pruebas de la macro Count

Tarea	Descripción	Habilidades requeridas
Implemente la macro Count.	1. Clona o descarga la CloudFormation macro Count. 2. Vaya a la carpeta `Count`. 3. Necesitará un depósito S3 para almacenar los CloudFormation artefactos. Si aún no tiene un bucket	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	de S3 en, cree uno con el nombre `aws s3 mb s3://<bucket name>` .
	4. Package la plantilla de la macro Count. La plantilla utiliza el modelo de aplicaciones sin servidor (SAM) de AWS, por lo que debe transformarse antes de poder implementarla.
	`aws cloudformation package \ --template-file template.yaml \ --s3-bucket <your bucket name here> \ --output-template-file packaged.yaml`
	Por ejemplo:
	`aws cloudformation package \ --template-file template.yaml \ --s3-bucket count-macro-ec2 \ --output-template-file packaged.yaml`
	5. Implemente la plantilla empaquetada para crear una CloudFormation pila.	

Tarea	Descripción	Habilidades requeridas
	`aws cloudformation deploy \ --stack-name Count-macro \ --template-file packaged.yaml \ --capabilities CAPABILITY_IAM` Si quieres usar la consola, sigue las instrucciones de la epopeya anterior o de la CloudFormation documentación.	
Pruebe la macro Count.	Para probar las capacidades de la macro, intente iniciar la plantilla de ejemplo que se proporciona con la macro. `aws cloudformation deploy \ --stack-name Count-test \ --template-file test.yaml \ --capabilities CAPABILITY_IAM`	DevOps ingeniero

Implemente la CloudFormation pila para aprovisionar instancias con la imagen personalizada

Tarea	Descripción	Habilidades requeridas
Implemente la plantilla de EC2 aprovisionamiento de Amazon.	Para implementar EC2 Image Pipeline mediante CloudFormation: 1. Descargue la `ec2-provisioning.yaml` plantilla del GitHub repositorio o ubíquela en su ordenador si ha clonado el repositorio. 2. Abra la consola de CloudFormation . 3. Repite los pasos de la primera epopeya (o sigue las instrucciones de la CloudFormation documentación) para realizar la implementación`ec2-provisioning.yaml` .	AWS DevOps
Consulta la EC2 configuración de Amazon.	La EC2 configuración de Amazon incluye configuraciones de seguridad, redes, almacenamiento, comprobaciones de estado, monitoreo y etiquetas. Para ver estas configuraciones: 1. Abre la EC2 consola de Amazon. 2. En el panel de navegación, elige Instances y, a continuación, selecciona la EC2 instancia que creó la	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	plantilla de EC2 aprovisio namiento de Amazon. 3. En el resumen de la instancia, selecciona las pestañas para ver la EC2 configuración de Amazon correspondiente.	
Vea el CloudWatch panel de control.	1. Abra la consola de CloudWatch . 2. En el panel de navegación, seleccione Paneles. 3. Elija el panel de control que tiene el nombre de su pila. **Note** Después de aprovisio nar la pila, se tarda un tiempo en rellenar el panel con las métricas. El panel proporciona las siguientes métricas: `CPUUtilization` , `DiskUtilization` , `MemoryUtilization` , `NetworkIn` , `NetworkOut` , `StatusCheckFailed` .	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Vea las métricas personalizadas del uso de memoria y disco.	1. En la CloudWatch consola, elija Dashboards. 2. En el panel de navegación, seleccione Métricas y, a continuación, Todas las métricas. 3. Elija Espacios de nombres personalizados,. CWAgent	AWS DevOps
Vea las alarmas de uso de memoria y disco.	1. En la CloudWatch consola, en el panel de navegación, elija Dashboards. 2. Seleccione All alarms (Todas las alarmas).	AWS DevOps
Verifique la regla del ciclo de vida de las instantáneas.	1. Abre la EC2 consola de Amazon. 2. En el panel de navegación, seleccione Lifecycle Manager (Administrador de ciclo de vida). 3. Verifique la configuración del ciclo de vida de la AMI.	AWS DevOps

Eliminar el entorno (opcional)

Tarea	Descripción	Habilidades requeridas
Elimine las pilas.	Cuando haya completado su PoC o su proyecto piloto, le recomendamos que elimine las pilas que ha creado para asegurarse de que no se le cobre por estos recursos.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	1. Abra la CloudFormation consola de AWS. 2. En el panel de navegación, seleccione Pilas y, a continuación, seleccione una o las dos pilas que creó anteriormente y que desee eliminar. La pila se debe estar ejecutando en este momento. 3. En el panel de detalles de la pila, seleccione Eliminar. 4. Cuando se le solicite, seleccione Delete stack (Eliminar pila). **Important** La operación de eliminación de la pila no se puede detener una vez que comienza. La pila avanza al estado `DELETE_IN_PROGRESS` . Si la eliminación ha fallado, la pila tendrá el estado `DELETE_FAILED` . Para obtener soluciones, consulte Fallos al eliminar una pila en la documentación de	

Tarea	Descripción	Habilidades requeridas
	CloudFormation solución de problemas de AWS. Para obtener información sobre cómo proteger las pilas para que no se eliminen accidentalmente, consulte Cómo proteger una pila para que no se elimine en la CloudFormation documenta ción de AWS.	

Resolución de problemas

Problema	Solución
Al implementar la plantilla de EC2 aprovisio namiento de Amazon, aparece el error: Se ha recibido una respuesta con formato incorrecto de transform 123xxxx: :Count.	Se trata de un problema conocido. (Consulte la solución personalizada y las relaciones públicas en el repositorio de CloudFormation macros de AWS). Para solucionar este problema, abra la consola de AWS Lambda y actualice `index.py` con el contenido del GitHub repositorio.

Recursos relacionados

GitHub repositorios

- UiPath Configuración del bot RPA mediante CloudFormation
- Count Macro CloudFormation

Referencias de AWS

- Creación de una pila en la CloudFormation consola de AWS (CloudFormation documentación)
- Solución de problemas CloudFormation (CloudFormation documentación)
- Supervise las métricas de memoria y disco de las EC2 instancias de Amazon (EC2 documentación de Amazon)
- ¿Cómo puedo usar el CloudWatch agente para ver las métricas del monitor de rendimiento en un servidor Windows? (artículo de AWS Re:post)

Referencias adicionales

- UiPath documentación
- Configuración del nombre de host en una SysPreped AMI (entrada de blog de Brian Beach)
- ¿Cómo hago para que Cloudformation reprocese una plantilla mediante una macro cuando cambian los parámetros? (Desbordamiento de pila)

Configure una PeopleSoft arquitectura de alta disponibilidad en AWS

Ramanathan Muralidhar, Amazon Web Services

Resumen

Cuando migra sus PeopleSoft cargas de trabajo a AWS, la resiliencia es un objetivo importante. Garantiza que su PeopleSoft aplicación siempre tenga una alta disponibilidad y pueda recuperarse rápidamente de los errores.

Este patrón proporciona una arquitectura para sus PeopleSoft aplicaciones en AWS a fin de garantizar la alta disponibilidad (HA) en los niveles de red, aplicación y base de datos. Emplea una base de datos Amazon Relational Database Service (Amazon RDS) para Oracle o Amazon RDS para SQL Server en el nivel de base de datos. Esta arquitectura escalable también incluye servicios de AWS como Amazon Route 53, instancias de Linux en Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Storage (Amazon EBS), Amazon Elastic File System (Amazon EFS) y un equilibrador de carga de aplicación.

Oracle PeopleSoft proporciona un conjunto de herramientas y aplicaciones para la administración de la fuerza laboral y otras operaciones empresariales.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un PeopleSoft entorno con las licencias necesarias para configurarlo en AWS
- Una nube privada virtual (VPC) configurada en su cuenta de AWS con los siguientes recursos:
  - Al menos dos zonas de disponibilidad
  - Una subred pública y tres subredes privadas en cada zona de disponibilidad
  - Una puerta de enlace NAT y una puerta de enlace de Internet
  - Tablas de enrutamiento en cada subred para enrutar el tráfico
  - Listas de control de acceso a la red (red ACLs) y grupos de seguridad definidos para garantizar la seguridad de la PeopleSoft aplicación de acuerdo con los estándares de su organización

Limitaciones

- Este patrón proporciona una solución de alta disponibilidad (HA). No es compatible con escenarios de recuperación de desastres (DR). En el infrecuente caso de que toda la región de AWS para la implementación de alta disponibilidad dejase de estar disponible, la aplicación dejaría de estar disponible.

Versiones de producto

- PeopleSoft aplicaciones que ejecutan la versión PeopleTools 8.52 y versiones posteriores

Arquitectura

Arquitectura de destino

El tiempo de inactividad o la interrupción de PeopleSoft la aplicación de producción afectan a la disponibilidad de la aplicación y provocan importantes interrupciones en su negocio.

Le recomendamos que diseñe su aplicación de PeopleSoft producción de manera que siempre tenga una alta disponibilidad. Para ello, puede eliminar los puntos únicos de fallo, añadir puntos de cruce o conmutación por error fiables y detectar los fallos. El siguiente diagrama ilustra una arquitectura de alta disponibilidad para PeopleSoft AWS.

Esta implementación de arquitectura utiliza Amazon RDS for Oracle como PeopleSoft base de datos e instancias EC2 que se ejecutan en Red Hat Enterprise Linux (RHEL). También puede usar Amazon RDS para SQL Server como base de datos de Peoplesoft.

Esta arquitectura contiene los siguientes componentes:

- Amazon Route 53 se utiliza como servidor de nombres de dominio (DNS) para enrutar las solicitudes de Internet a la PeopleSoft aplicación.
- AWS WAF le ayuda a protegerse contra exploits y bots web comunes que pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos. AWS Shield Avanzado (no se ilustra) proporciona una protección mucho más amplia.
- El Equilibrador de carga de aplicación equilibra la carga del tráfico HTTP y HTTPS con un enrutamiento de solicitudes avanzado dirigido a los servidores web.
- Los servidores web, los servidores de aplicaciones, los servidores del programador de procesos y los servidores Elasticsearch que admiten la PeopleSoft aplicación se ejecutan en varias zonas de disponibilidad y utilizan Amazon EC2 Auto Scaling.

- La base de datos utilizada por la PeopleSoft aplicación se ejecuta en Amazon RDS en una configuración Multi-AZ.
- El recurso compartido de archivos que utiliza la PeopleSoft aplicación está configurado en Amazon EFS y se utiliza para acceder a los archivos de todas las instancias.
- Amazon EC2 Auto Scaling utiliza Amazon Machine Images (AMI) para garantizar PeopleSoft que los componentes se clonen rápidamente cuando sea necesario.
- Las puertas de enlace NAT conectan las instancias de una subred privada a servicios externos a su VPC y garantizan que los servicios externos no puedan iniciar una conexión con dichas instancias.
- La puerta de enlace de internet es un componente de la VPC de escalado horizontal, redundante y de alta disponibilidad que permite la comunicación entre su VPC e internet.
- Los host bastión de la subred pública proporcionan acceso a los servidores de la subred privada desde una red externa, como Internet o una red en las instalaciones. Los host bastión proporcionan un acceso controlado y seguro a los servidores de las subredes privadas.

Detalles de la arquitectura

La PeopleSoft base de datos está alojada en una base de datos Amazon RDS for Oracle (o Amazon RDS for SQL Server) en una configuración Multi-AZ. La función Amazon RDS Multi-AZ replica las actualizaciones de la base de datos en dos zonas de disponibilidad para aumentar la durabilidad y la disponibilidad. Amazon RDS conmuta automáticamente a la base de datos en espera en caso de mantenimiento planificado e interrupciones imprevistas.

La PeopleSoft web y el nivel medio se instalan en las instancias EC2. Estas instancias se distribuyen en varias zonas de disponibilidad, y están vinculadas a un grupo de escalado automático. Esto garantiza que estos componentes estén siempre altamente disponibles. Se mantiene el número mínimo de instancias necesarias para garantizar que la aplicación esté siempre disponible y pueda escalarse cuando sea necesario.

Recomendamos usar un tipo de instancia EC2 de la generación actual para las instancias EC2 OEM. Los tipos de instancias de la generación actual, como las instancias creadas en el sistema Nitro de AWS, admiten máquinas virtuales de hardware (HVMs). Las HVM AMIs son necesarias para aprovechar las ventajas de las redes mejoradas y, además, ofrecen una mayor seguridad. Las instancias de EC2 que forman parte de cada grupo de escalado automático usan su propia AMI al reemplazar o escalar verticalmente las instancias. Le recomendamos que seleccione los tipos de instancias EC2 en función de la carga que desee que PeopleSoft gestione su aplicación y de los valores mínimos recomendados por Oracle para su PeopleSoft aplicación y PeopleTools versión.

Para obtener más información sobre los requisitos de hardware y software, consulte el sitio web de soporte de Oracle.

La PeopleSoft web y el nivel medio comparten una montura de Amazon EFS para compartir informes, archivos de datos y (si es necesario) el `PS_HOME` directorio. Amazon EFS se configura con objetivos de montaje en cada zona de disponibilidad por motivos de rendimiento y costo.

Se aprovisiona un Application Load Balancer para soportar el tráfico que accede a la PeopleSoft aplicación y equilibra la carga del tráfico entre los servidores web de las diferentes zonas de disponibilidad. Un equilibrador de carga de aplicación es un dispositivo de red que proporciona alta disponibilidad en, al menos, dos zonas de disponibilidad. Los servidores web distribuyen el tráfico a diferentes servidores de aplicaciones mediante una configuración de equilibrio de carga. El equilibrador de carga entre el servidor web y el servidor de aplicaciones garantiza que la carga se distribuya de manera uniforme entre las instancias, ayudando a evitar los cuellos de botella y las interrupciones del servicio debido a la sobrecarga de las instancias.

Amazon Route 53 se emplea como servicio de DNS para enrutar el tráfico desde Internet al equilibrador de carga de aplicación. Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.

Detalles de HA

- Bases de datos: la función Multi-AZ de Amazon RDS opera dos bases de datos en varias zonas de disponibilidad con replicación sincrónica. Esto crea un entorno de alta disponibilidad con conmutación por error automática. Amazon RDS cuenta con una función de detección de eventos de conmutación por error, e inicia una conmutación por error automática cuando se producen dichos eventos. También puede iniciar una conmutación por error manual a través de la API de Amazon RDS. Para obtener una explicación detallada, consulte la entrada del blog Amazon RDS entre bastidores: Multi-AZ. La conmutación por error es fluida, y la aplicación se vuelve a conectar automáticamente a la base de datos cuando se produce. Sin embargo, cualquier trabajo del programador de procesos durante la conmutación por error genera errores y debe volver a enviarse.
- PeopleSoft servidores de aplicaciones: los servidores de aplicaciones están distribuidos en múltiples zonas de disponibilidad y tienen un grupo de Auto Scaling definido para ellos. Si una instancia falla, el grupo de escalado automático la reemplaza inmediatamente por una instancia en buen estado que se clona desde la AMI de la plantilla del servidor de aplicaciones. Se habilita la agrupación por descargas de modo que, cuando una instancia del servidor de aplicaciones deja de funcionar, las sesiones se conmutan automáticamente por error a otro servidor de aplicaciones,

y el grupo de escalado automático activa automáticamente otra instancia, abre el servidor de aplicaciones y la registra en el montaje de Amazon EFS. El servidor de aplicaciones recién creado se añade automáticamente a los servidores web mediante el script `PSSTRSETUP.SH` de los servidores web. Esto garantiza que el servidor de la aplicación esté siempre altamente disponible y se recupere de los errores con rapidez.

- Programadores de procesos: los servidores de los programadores de procesos están distribuidos en varias zonas de disponibilidad, y tienen un grupo de escalado automático definido para ellos. Si falla una instancia, el grupo de escalado automático la sustituye inmediatamente por una instancia sana clonada a partir de la AMI de la plantilla de servidor del programador de procesos. Cuando una instancia del programador de procesos deja de funcionar, el grupo de escalado automático activa automáticamente otra instancia y abre el programador de procesos. Todos los trabajos que estaban en ejecución cuando la instancia falló deben volver a enviarse. Esto garantiza que el programador de procesos esté disponible en todo momento y se recupere rápidamente de los errores.
- Servidores Elasticsearch: Los servidores Elasticsearch tienen un grupo de escalado automático definido para ellos. Si falla una instancia, el grupo de escalado automático la sustituye inmediatamente por una instancia sana clonada a partir de la AMI de la plantilla del servidor de Elasticsearch. Cuando una instancia de Elasticsearch deja de funcionar, el equilibrador de carga de aplicación que le envía las solicitudes detecta el error y deja de enviarle tráfico. El grupo de escalado automático activa automáticamente otra instancia y abre la instancia de Elasticsearch. Cuando la instancia de Elasticsearch se recupera, el equilibrador de carga de aplicación detecta que está en buen estado y vuelve a enviarle solicitudes. Esto garantiza que el servidor de Elasticsearch esté siempre altamente disponible y se recupere de los errores con rapidez.
- Servidores web: Los servidores web tienen un grupo de escalado automático definido para ellos. Si falla una instancia, el grupo de escalado automático la sustituye inmediatamente por una instancia sana clonada a partir de la AMI de la plantilla del servidor web. En concreto, cuando una instancia de servidor web se cae, el Equilibrador de carga de aplicación que le sirve las peticiones detecta el fallo y deja de enviarle tráfico. El grupo de escalado automático pone en marcha automáticamente otra instancia y pone en marcha la instancia del servidor web. Cuando la instancia del servidor web vuelve a funcionar, el Equilibrador de carga de aplicación detecta que está en buen estado y comienza a enviarle peticiones de nuevo. Esto garantiza que el servidor web esté siempre altamente disponible y se recupere de los errores con rapidez.

Tools (Herramientas)

Servicios de AWS

- Los Equilibradores de carga de aplicación distribuyen el tráfico entrante de aplicaciones entre varios destinos, tales como instancias EC2, en varias zonas de disponibilidad.
- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento por bloques para su uso con instancias de Amazon Elastic Compute Cloud (Amazon EC2).
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Elastic File System (Amazon EFS) le ayuda a crear y configurar sistemas de archivos compartidos en la nube de AWS.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.

Prácticas recomendadas

Prácticas operativas recomendadas

- Cuando utilice AWS, utilice Route 53 para enrutar el tráfico desde Internet y de forma local. PeopleSoft Use la opción de conmutación por error para redirigir el tráfico al sitio de recuperación de desastres (DR) si la instancia de base de datos principal no está disponible.
- Utilice siempre un Application Load Balancer delante del PeopleSoft entorno. Esto garantiza que la carga del tráfico se equilibre en los servidores web de forma segura.
- En la configuración del grupo de destino del equilibrador de carga de aplicación, asegúrese de que la adherencia esté activada con una cookie generada por el equilibrador de carga.

> **Note**
>
> Es posible que tenga que utilizar una cookie basada en aplicación si utiliza un inicio de sesión único (SSO) externo. Esto garantiza que las conexiones sean consistentes entre los servidores web y los servidores de aplicaciones.

- En el caso de una aplicación de PeopleSoft producción, el tiempo de espera de inactividad de Application Load Balancer debe coincidir con el establecido en el perfil web que utilice. Esto evita que las sesiones de usuario caduquen en la capa del equilibrador de carga.

- Para una aplicación PeopleSoft de producción, establezca el recuento de reciclaje del servidor de aplicaciones en un valor que minimice las pérdidas de memoria.
- Si utiliza una base de datos de Amazon RDS para su aplicación de PeopleSoft producción, tal y como se describe en este patrón, ejecútela en formato Multi-AZ para obtener una alta disponibilidad.
- Si la base de datos se ejecuta en una instancia EC2 para la aplicación de PeopleSoft producción, asegúrese de que la base de datos en espera se ejecute en otra zona de disponibilidad para garantizar una alta disponibilidad.
- Para la DR, asegúrese de que la base de datos de Amazon RDS o la instancia de EC2 tengan un modo de espera configurado en una región de AWS independiente de la base de datos de producción. Esto garantiza que, en caso de que se produzca un desastre en la región, pueda cambiar la aplicación a otra región.
- En cuanto a la RD, use Amazon Elastic Disaster Recovery para configurar los componentes de nivel de aplicación en una región distinta de los componentes de producción. Esto garantiza que, en caso de que se produzca un desastre en la región, pueda cambiar la aplicación a otra región.
- Utilice Amazon EFS (para I/O requisitos moderados) o Amazon FSx (para I/O requisitos altos) para almacenar sus PeopleSoft informes, archivos adjuntos y archivos de datos. Esto garantiza que el contenido se almacene en una ubicación central y accesible desde cualquier lugar de la infraestructura.
- Utilice Amazon CloudWatch (básico y detallado) para supervisar los recursos de la nube de AWS que utiliza su PeopleSoft aplicación prácticamente en tiempo real. Esto garantiza que reciba alertas de los problemas al instante y pueda solucionarlos rápidamente antes de que afecten a la disponibilidad del entorno.
- Si utiliza una base de datos de Amazon RDS como base de datos, utilice Enhanced Monitoring. PeopleSoft Esta función proporciona acceso a más de 50 métricas, incluidas la CPU, la memoria y el sistema I/O, and disk I/O de archivos.
- Utilice AWS CloudTrail para supervisar las llamadas a la API en los recursos de AWS que utiliza su PeopleSoft aplicación. Esto permite realizar análisis de seguridad, seguimiento de los cambios en los recursos y auditorías de conformidad.

Prácticas recomendadas de seguridad

- Para proteger su PeopleSoft aplicación de vulnerabilidades habituales, como la inyección de SQL o el cross-site scripting (XSS), utilice AWS WAF. Considere la posibilidad de usar AWS Shield Avanzado para obtener servicios de detección y mitigación personalizados.

- Agrega una regla al Application Load Balancer para redirigir el tráfico de HTTP a HTTPS automáticamente y así proteger tu PeopleSoft aplicación.
- Configure un grupo de seguridad independiente para el equilibrador de carga de aplicación. Este grupo de seguridad debe permitir solo el tráfico HTTPS/HTTP entrante y no el saliente. Esto garantiza que solo se permita el tráfico previsto y ayuda a proteger la aplicación.
- Use subredes privadas para los servidores de aplicaciones, los servidores web y la base de datos, y use puertas de enlace NAT para el tráfico de Internet saliente. Esto garantiza que no se pueda acceder públicamente a los servidores que respaldan la aplicación y, al mismo tiempo, proporciona acceso público solo a los servidores que lo necesitan.
- Utilice diferentes VPCs para ejecutar sus entornos de PeopleSoft producción y de no producción. Utilice AWS Transit Gateway, la interconexión de VPC, la red ACLs y los grupos de seguridad para controlar el flujo de tráfico entre las VPC y, si es necesario, su centro de datos local.
- Siga el principio de privilegio mínimo Conceda acceso a los recursos de AWS que utiliza la PeopleSoft aplicación solo a los usuarios que lo necesiten absolutamente. Otorgue únicamente los privilegios mínimos obligatorios para realizar una tarea. Para obtener más información, consulte el pilar de seguridad del Marco de AWS Well-Architected.
- Siempre que sea posible, utilice AWS Systems Manager para acceder a las instancias EC2 que utiliza la PeopleSoft aplicación.

Prácticas recomendadas de fiabilidad

- Cuando utilice un equilibrador de carga de aplicación, registre un único destino para cada zona de disponibilidad habilitada. Esto aumenta la efectividad del equilibrador de carga.
- Le recomendamos que tenga tres direcciones distintas URLs para cada entorno de PeopleSoft producción: una URL para acceder a la aplicación, otra para servir al agente de integración y otra para ver los informes. Si es posible, cada URL debe tener sus propios servidores web y servidores de aplicaciones dedicados. Este diseño ayuda a que PeopleSoft la aplicación sea más segura, ya que cada URL tiene una funcionalidad distinta y un acceso controlado. También minimiza el alcance del impacto en caso de que los servicios subyacentes fallen.
- Te recomendamos que configures las comprobaciones de estado de los grupos objetivo del balanceador de cargas de tu PeopleSoft aplicación. Las comprobaciones de estado deben realizarse en los servidores web, y no en las instancias EC2 que ejecutan esos servidores. Esto garantiza que si el servidor web se bloquea o la instancia EC2 que aloja el servidor web deja de funcionar, el equilibrador de carga de aplicación refleje esa información con precisión.

- En el caso PeopleSoft de una aplicación de producción, le recomendamos que distribuya los servidores web en al menos tres zonas de disponibilidad. Esto garantiza que la PeopleSoft aplicación siempre tenga una alta disponibilidad, incluso si una de las zonas de disponibilidad deja de funcionar.
- Para una aplicación PeopleSoft de producción, habilite la agrupación de sacudidas ()`joltPooling=true`. Esto garantiza que su aplicación se conmute por error a otro servidor de aplicaciones si un servidor está inactivo por motivos de aplicación de parches o debido a un fallo de la máquina virtual.
- Para una aplicación de PeopleSoft producción, establézcalo en `1DynamicConfigReload` . Esta configuración se admite en la PeopleTools versión 8.52 y versiones posteriores. Añade nuevos servidores de aplicaciones al servidor web de forma dinámica, sin necesidad de reiniciar los servidores.
- Para minimizar el tiempo de inactividad al aplicar PeopleTools parches, utilice el método de blue/green despliegue para las configuraciones de lanzamiento grupal de Auto Scaling para los servidores web y de aplicaciones. Para obtener más información, consulte el documento técnico Descripción general de las opciones de implementación en AWS.
- Utilice AWS Backup para hacer copias de seguridad de su PeopleSoft aplicación en AWS. AWS Backup es un servicio rentable, totalmente gestionado y basado en políticas que simplifica la protección de datos a escala.

Prácticas recomendadas de rendimiento

- Termine el SSL en el Application Load Balancer para obtener un rendimiento óptimo del PeopleSoft entorno, a menos que su empresa requiera tráfico cifrado en todo el entorno.
- Cree puntos de enlace de VPC de interfaz para los servicios de AWS, como Amazon Simple Notification Service (Amazon SNS) CloudWatch, de forma que el tráfico sea siempre interno. Esto es rentable y ayuda a mantener la aplicación segura.

Prácticas recomendadas de optimización de costos

- Etiquete todos los recursos que utiliza su PeopleSoft entorno y active las etiquetas de asignación de costes. Estas etiquetas le ayudan a ver y gestionar los costos de sus recursos.
- Para una aplicación PeopleSoft de producción, configure grupos de Auto Scaling para los servidores web y los servidores de aplicaciones. De este modo, mantiene el número mínimo de

servidores web y de aplicaciones para dar soporte a su aplicación. Puede usar políticas de grupo de escalado automático para ampliar o reducir los servidores según sea necesario.

- Use alarmas de facturación para recibir alertas cuando los costos superen el umbral presupuestario que especifique.

Prácticas recomendadas de sostenibilidad

- Utilice la infraestructura como código (IaC) para mantener sus PeopleSoft entornos. Esto permite crear entornos coherentes y a mantener el control de los cambios.

Epics

Migre su PeopleSoft base de datos a Amazon RDS

Tarea	Descripción	Habilidades requeridas
Creación de un grupo de subredes de base de datos.	En la consola de Amazon RDS, en el panel de navegación, elija Grupos de subred y, a continuación, cree un grupo de subredes de base de datos de Amazon RDS con subredes en varias zonas de disponibilidad. Esto es necesario para que la base de datos de Amazon RDS se ejecute en una configuración Multi-AZ.	Administrador de la nube
Crear la base de datos de Amazon RDS.	Cree una base de datos de Amazon RDS en una zona de disponibilidad de la región de AWS que haya seleccionado para el entorno de PeopleSoft alta disponibilidad. Al crear la base de datos de Amazon RDS, asegúrese de seleccion	Administrador de la nube, administrador de bases de datos de Oracle

Tarea	Descripción	Habilidades requeridas
	ar la opción Multi-AZ (crear una instancia en espera) y el grupo de subredes de la base de datos que creó en el paso anterior. Para obtener más información, consulte la documentación de Amazon RDS.	
Migre su PeopleSoft base de datos a Amazon RDS.	Migre su PeopleSoft base de datos existente a la base de datos de Amazon RDS mediante AWS Database Migration Service (AWS DMS). Para más información, consulte la documentación de AWS DMS y la publicación del blog de AWS Migración de bases de datos de Oracle con un tiempo de inactividad casi nulo mediante AWS DMS.	Administrador de nube, administrador de bases de datos PeopleSoft

Configure su sistema de archivos Amazon EFS

Tarea	Descripción	Habilidades requeridas
Cree un sistema de archivos.	En la consola de Amazon EFS, cree un sistema de archivos y monte los destinos para cada zona de disponibi lidad. Para obtener instrucci ones, consulte la documenta ción de Amazon EFS. Cuando haya creado el sistema de archivos, anote su nombre de	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	DNS. Usará esta información cuando monte el sistema de archivos.	

Configure su PeopleSoft aplicación y su sistema de archivos

Tarea	Descripción	Habilidades requeridas
Lanzar una instancia EC2.	Lance una instancia EC2 para su PeopleSoft aplicación. Para obtener instrucciones, consulte la documentación de Amazon EC2. • En Nombre, escriba `APP_TEMPLATE` . • En imágenes de SO, seleccione Red Hat. • En Tipo de instancia, elija el tipo de instancia adecuado para su PeopleSoft aplicación. Para obtener más información, consulte los Detalles de arquitectura en la sección Arquitectura.	Administrador de nube, PeopleSoft administrador
Instálelo PeopleSoft en la instancia.	Instale PeopleSoft la aplicación y PeopleTools en la instancia EC2 que creó. Para obtener instrucciones, consulte la documentación de Oracle.	Administrador de nube, PeopleSoft administrador
Crear el servidor de la aplicación.	Cree el servidor de aplicaciones para la plantilla de AMI y	Administrador de la nube, PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas
	asegúrese de que se conecta correctamente a la base de datos de Amazon RDS.	

Monte el sistema de archivos de Amazon EFS.	Inicie sesión en la instancia EC2 como usuario raíz y ejecute los siguientes comandos para montar el sistema de archivos de Amazon EFS en una carpeta llamada PSFTMNT en el servidor.
	`sudo su -`
	`mkdir /psftmnt`
	`cat /etc/fstab`
	Añada la línea siguiente al archivo `/etc/fstab` . Use el nombre de DNS que anotó al crear el sistema de archivos.
	`fs-09e064308f11453 88.efs.us-east-1.a mazonaws.com:/ / psftmnt nfs4 nfsvers=4 .1,rsize=1048576,w size=1048576,hard, timeo=600,retrans= 2,noresvport,_netdev 0 0`
	`mount -a`
		Administrador de la nube, PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas
Comprobar permisos.	Asegúrese de que la `PSFTMNT` carpeta tenga los permisos adecuados para que el PeopleSoft usuario pueda acceder a ella correctamente.	Administrador de la nube, PeopleSoft administrador
Cree instancias adicionales.	Repita los pasos anteriores de esta épica para crear instancias de plantilla para el programador de procesos, el servidor web y el servidor Elasticsearch. Nombre estas instancias como `PRCS_TEMPLATE` , `WEB_TEMPLATE` y `SRCH_TEMPLATE` . En el servidor web, defina `joltPooling=true` y `DynamicConfigReload=1` .	Administrador de la nube, PeopleSoft administrador

Cree scripts para configurar los servidores

Tarea	Descripción	Habilidades requeridas
Cree un script para instalar el servidor de aplicaciones.	En la `APP_TEMPLATE` instancia de Amazon EC2, cree el siguiente script como PeopleSoft usuario. Asígnele el nombre `appstart.sh` y colóquelo en el directorio `PS_HOME`. Usará este script para abrir el servidor de aplicaciones y también para registrar el nombre del	PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas

	servidor en el soporte de Amazon EFS.
	
	`#!/bin/ksh`
	`. /usr/homes/hcmdemo/.profile.`
	`psadmin -c configure -d HCMDEMO`
	`psadmin -c parallelboot -d HCMDEMO`
	`touch /psftmnt/`echo $HOSTNAME`	

Tarea	Descripción	Habilidades requeridas

Cree un script para instalar el servidor de programador de procesos.	En la `PRCS_TEMPLATE` instancia de Amazon EC2, cree el siguiente script como PeopleSoft usuario. Asígnele el nombre `prcsstart.sh` y colóquelo en el directorio `PS_HOME`. Usará este script para abrir el servidor de programador de procesos.
	`#!/bin/ksh`
	`. /usr/homes/hcmdemo/. profile`
	`/* The following line ensures that the process scheduler always has a unique name during replaceme nt or scaling activity. */`
	`sed -i "s/.*Prcs ServerName.*/`host name -I | awk -F. '{print "PrcsServ erName=PSUNX"$3$4} '`/" $HOME/appserv/ prcs/*/psprcs.cfg`
	`psadmin -p configure -d HCMDEMO`
	`psadmin -p start -d HCMDEMO`
		PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas

Cree un script para instalar el servidor Elasticsearch.	En la instancia `SRCH_TEMPLATE` de Amazon EC2, como usuario de Elasticsearch, cree el siguiente script. Asígnele el nombre `srchstart.sh` y colóquelo en el directorio `HOME`.
	
	`#!/bin/ksh`
	`/* The following line ensures that the correct IP is indicated in the elasticsearch.yaml file. */`
	`sed -i "s/.*network.host.*/`hostname -I
		awk '{print "host:"$0}'`/" $ES_HOME_DIR/config/elasticsearch.yaml`
		`nohup $ES_HOME_DIR/bin/elasticsearch &`
			PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas
Cree un script para instalar el servidor web.	En la instancia `WEB_TEMPLATE` de Amazon EC2, como usuario del servidor web, cree los siguientes scripts en el directorio `HOME`. `renip.sh`: este script garantiza que el servidor web tenga la IP correcta cuando se clone desde la AMI. `#!/bin/ksh` `hn=`hostname`` `/* On the following line, change the IP with the hostname with the hostname of the web template. */` `for text_file in `find * -type f -exec grep -l '<hostname-of-the-web-template>' {} \;` `do` `sed -e 's/<hostname-of-the-web-template>/'$hn'/g' $text_file > temp` `mv -f temp $text_file` `done`  `psstrsetup.sh` : Este script garantiza que el servidor web utilice el servidor de aplicaciones correcto IPs que se está ejecutando actualmente. Intenta conectarse a cada servidor de aplicaciones en el	PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas

	puerto de descarga y lo añade al archivo de configuración.
	
	`#!/bin/ksh`
	`c2=""`
	`for ctr in `ls -1 /psftmnt/*.internal`do`
	`c1=`echo $ctr | awk -F "/" '{print $3}'`/* In the following lines, 9000 is the jolt port. Change it if necessary. */`
	`if nc -z $c1 9000 2> /dev/null; then`
	`if [[ $c2 = "" ]]; then`
	`c2="psserver="`echo $c1`":9000"`
	`else`
	`c2=`echo $c2`","`echo $c1`":9000"`
	`fi`
	`fi`
	`done`
	
	`webstart.sh` : este script ejecuta los dos scripts anteriores e inicia los servidores web.
	
	`#!/bin/ksh`
	`/* Change the path in the following if necessary. */`
	`cd /usr/homes/hcmdemo`
	`./renip.sh`
	`./psstrsetup.sh`	

Tarea	Descripción	Habilidades requeridas
	`webserv/peoplesoft/bin/startPIA.sh`	
Añada una entrada de crontab.	En la instancia de Amazon EC2 `WEB_TEMPLATE` , como usuario del servidor web, añada la siguiente línea a crontab. Cambie la hora y la ruta para reflejar los valores que necesita. Esta entrada garantiza que su servidor web siempre tenga las entradas correctas del servidor de aplicaciones en el archivo `configuration.properties` . `* * * * * /usr/homes/hcmdemo/psstrsetup.sh`	PeopleSoft administrador

Plantillas de grupos de Creación AMIs y Auto Scaling

Tarea	Descripción	Habilidades requeridas
Cree una AMI para la plantilla del servidor de aplicaciones.	En la consola de Amazon EC2, cree una imagen de AMI de la instancia `APP_TEMPLATE` de Amazon EC2. Ponga el nombre `PSAPPSRV-SCG-VER1` a la AMI. Para obtener instrucciones, consulte la documentación de Amazon EC2.	Administrador de la nube, PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas
Crea AMIs para los demás servidores.	Repita el paso anterior AMIs para crear el programador de procesos, el servidor Elasticsearch y el servidor web.	Administrador de la nube, administrador PeopleSoft

Tarea	Descripción	Habilidades requeridas

Cree una plantilla de lanzamiento para el grupo de escalado automático del servidor de aplicaciones.	Cree una plantilla de lanzamiento para el grupo de escalado automático del servidor de aplicaciones. Asigne el nombre `PSAPPSRV_TEMPLATE.` a la plantilla. En la plantilla, elija la AMI que creó para la instancia `APP_TEMPLATE` . Para obtener instrucciones, consulte la documentación de Amazon EC2.
	• En la plantilla de lanzamiento, seleccione el tipo de instancia según sus requisitos.
	• En el campo Datos de usuario de la sección Detalles avanzados, añada las siguientes entradas. Asegúrese de que la ruta y la información del usuario sean correctas. Ha creado el script `appstart.sh` en un paso anterior.
	`#! /bin/ksh`
	`su -c "/usr/homes/hcmdemo/appstart.sh" - hcmdemo`
		Administrador de la nube, PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas

Cree una plantilla de lanzamiento para el grupo de escalado automático del servidor de programación de procesos.	Repita el paso anterior para crear una plantilla de lanzamiento para el grupo de escalado automático del servidor programador de procesos. Asigne un nombre a la plantilla `PSPRCS_TEMPLATE` . En la plantilla, elija la AMI que creó para el programador de procesos.
	• En el campo Datos de usuario de la sección Detalles avanzados, añada las siguientes entradas. Asegúrese de que la ruta y la información del usuario sean correctas. Ha creado el script `prcsstart.sh` en un paso anterior.
	`#! /bin/ksh`
	`su -c "/usr/homes/hcmdemo/prcsstart.sh" - hcmdemo`
		Administrador de la nube, PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas

Cree una plantilla de lanzamiento para el grupo de escalado automático del servidor de Elasticsearch.	Repita los pasos anteriores para crear una plantilla de lanzamiento para el grupo de escalado automático del servidor Elasticsearch. Asigne un nombre a la plantilla `SRCH_TEMPLATE` . En la plantilla, elija la AMI que creó para el servidor de búsqueda.
	• En el campo Datos de usuario de la sección Detalles avanzados, añada las siguientes entradas. Asegúrese de que la ruta y la información del usuario sean correctas. Ha creado el script `srchstart.sh` en un paso anterior.
	`#! /bin/ksh`
	`su -c "/usr/hom`
	`es/essearch/srchst`
	`art.sh" - essearch`
		Administrador de la nube, PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas

Cree una plantilla de lanzamiento para el grupo de escalado automático del servidor web.	Repita los pasos anteriores para crear una plantilla de lanzamiento para el grupo de escalado automático del servidor web. Asigne un nombre a la plantilla `WEB_TEMPLATE` . En la plantilla, elija la AMI que creó para el servidor web.
	• En el campo Datos de usuario de la sección Detalles avanzados, añada las siguientes entradas. Asegúrese de que la ruta y la información del usuario sean correctas. Ha creado el script `webstart.sh` en un paso anterior.
	`#! /bin/ksh`
	`su -c "/usr/homes/hcmdemo/webstart.sh" - hcmdemo`
		Administrador de la nube, PeopleSoft administrador

Crear grupos de escalado automático

Tarea	Descripción	Habilidades requeridas
Cree un grupo de escalado automático para el servidor de aplicaciones.	En la consola de Amazon EC2, cree un grupo de escalado automático llamado `PSAPPSRV_ASG` para el servidor de aplicaciones	Administrador de la nube, PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas
	usando la plantilla `PSAPPSRV_TEMPLATE` . Para obtener instrucciones, consulte la documentación de Amazon EC2. • En la página Elegir opciones de lanzamiento de instancias, seleccione la VPC correcta y, a continuación, seleccione varias subredes de distintas zonas de disponibilidad. • En la página Configurar opciones avanzadas, no seleccione ningún equilibrador de carga. • En la página Configurar tamaño de grupo y políticas de escalado, seleccione los ajustes en función de la carga para la que desee diseñar el sistema y de si desea utilizar una política de escalado. Le recomendamos que establezca la capacidad mínima deseada en 2, como mínimo, para que haya al menos una instancia disponible para atender el tráfico en cualquier momento. Para más información sobre las políticas de escalado automático, consulte la	

Tarea	Descripción	Habilidades requeridas
	documentación de Amazon EC2.	
Cree grupos de escalado automático en el resto de servidores.	Repita el paso anterior para crear grupos de escalado automático para el programador de procesos, el servidor Elasticsearch y el servidor web.	Administrador de la nube, PeopleSoft administrador

Cree y configure grupos de destino

Tarea	Descripción	Habilidades requeridas
Cree un grupo de destino para el servidor web.	En la consola de Amazon EC2, cree un grupo de destino para el servidor web. Para obtener más instrucciones, consulte la documentación de Elastic Load Balancing. Establezca el puerto en el que escucha el servidor web.	Administrador de la nube
Configurar comprobaciones de estado.	Confirme que las comprobaciones de estado tengan los valores correctos según los requisitos de su empresa. Para obtener más información, consulte la Documentación de Elastic Load Balancing.	Administrador de la nube
Cree un grupo de destino para el servidor Elasticsearch.	Repita los pasos anteriores para crear un grupo de destino llamado PSFTSRCH para el servidor de Elasticse	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	arch, y configure el puerto de Elasticsearch correcto.	
Añada grupos de destino a los grupos de escalado automático.	Abra el grupo de escalado automático `PSPIA_ASG` que creó anteriormente. En la pestaña Equilibrador de carga, elija Editar y, a continuación, añada el grupo de destino `PSFTWEB` al grupo de escalado automático. Repite este paso para el grupo de escalado automático de Elasticsearch `PSSRCH_ASG` y añada el grupo objetivo `PSFTSRCH` que creó anteriormente.	Administrador de la nube
Establezca la adherencia de la sesión.	En el grupo de destino `PSFTWEB`, seleccione la pestaña Atributos, elija Editar y defina la adherencia de la sesión. En el tipo de adherencia, seleccione Cookie generada por el equilibrador de carga, y establezca la duración en 1. Para obtener más información, consulte la Documentación de Elastic Load Balancing. Repita este paso para el grupo de destino `PSFTSRCH`.	Administrador de la nube

Crear y configurar equilibradores de carga de aplicaciones

Tarea	Descripción	Habilidades requeridas
Crear un equilibrador de carga para los servidores web.	Cree un equilibrador de carga de aplicación con el nombre `PSFTLB` para equilibrar la carga del tráfico a los servidores web. Para obtener más instrucciones, consulte la documentación de Elastic Load Balancing. • Proporcione el nombre del equilibrador de carga. • En Scheme, elija Internet-facing. • En la sección Mapeo de redes, seleccione la VPC correcta y, al menos, dos subredes públicas de distintas zonas de disponibilidad. • En la sección de Escucha y enrutamiento, seleccione el grupo de destino `PSFTWEB` y especifique el protocolo y el número de puerto.	Administrador de la nube
Cree un equilibrador de carga para los servidores de Elasticsearch.	Cree un equilibrador de carga de aplicación con el nombre `PSFTSCH` para equilibrar la carga del tráfico a los servidores de Elasticsearch. • Proporcione el nombre del equilibrador de carga.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	• En Esquema, seleccione Interno. • En la sección Mapeo de redes, seleccione la VPC y las subredes privadas correctas. • En la sección de Escucha y enrutamiento, seleccione el grupo de destino `PSFTSRCH` y especifique el protocolo y el número de puerto.	
Configure Route 53.	En la consola Amazon Route 53, cree un registro en la zona alojada que servirá a la PeopleSoft aplicación. Para obtener instrucciones, consulte la documentación de Amazon Route 53. Esto garantiza que todo el tráfico pase por el equilibrador de carga `PSFTLB`.	Administrador de la nube

Recursos relacionados

- PeopleSoft Sitio web de Oracle
- Documentación de AWS

Configure la recuperación ante desastres para Oracle JD Edwards EnterpriseOne con AWS Elastic Disaster Recovery

Thanigaivel Thirumalai, Amazon Web Services

Resumen

Los desastres provocados por catástrofes naturales, fallos en las aplicaciones o interrupciones de servicios son perjudiciales para los ingresos y provocan tiempo de inactividad en las aplicaciones corporativas. Para reducir las repercusiones de este tipo de eventos, la planificación de la recuperación ante desastres (DR) es fundamental para las empresas que adoptan los sistemas de planificación de recursos EnterpriseOne empresariales (ERP) de JD Edwards y otros programas de software esenciales y empresariales de JD Edwards.

Este patrón explica cómo las empresas pueden utilizar AWS Elastic Disaster Recovery como una opción de recuperación ante desastres para sus EnterpriseOne aplicaciones de JD Edwards. También describe los pasos para utilizar la conmutación por error y la recuperación ante fallos de Elastic Disaster Recovery a fin de crear una estrategia de recuperación ante desastres entre regiones para las bases de datos alojadas en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) en la nube de AWS.

> **Note**
>
> Este patrón requiere que las regiones principal y secundaria para que la implementación de DR entre regiones se hospede en AWS.

Oracle JD Edwards EnterpriseOne es una solución de software ERP integrada para empresas medianas y grandes de una amplia gama de sectores.

AWS Elastic Disaster Recovery minimiza el tiempo de inactividad y la pérdida de datos con una recuperación rápida y fiable de aplicaciones locales y basadas en la nube mediante el uso de un almacenamiento asequible, un cálculo y point-in-time una recuperación mínimos.

AWS proporciona cuatro patrones de arquitectura de DR principales. Este documento se centra en la instalación, configuración y optimización mediante una estrategia de prueba piloto. Esta estrategia le ayuda a crear un entorno de DR de costo reducido, en el que inicialmente se aprovisiona un servidor de replicación para replicar los datos de la base de datos de origen. El servidor de base de datos

propiamente dicho se aprovisiona solo cuando se inicia un proceso de recuperación de desastres. Esta estrategia elimina los gastos de mantenimiento de un servidor de base de datos en la región de DR. En su lugar, usted paga por una instancia EC2 más pequeña que actúa como servidor de replicación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una EnterpriseOne aplicación de JD Edwards que se ejecuta en Oracle Database o Microsoft SQL Server con una base de datos compatible en estado de ejecución en una instancia EC2 gestionada. Esta aplicación debe incluir todos los componentes EnterpriseOne básicos de JD Edwards (Enterprise Server, HTML Server y Database Server) instalados en una región de AWS.
- Un rol de AWS Identity and Access Management (IAM) para configurar el servicio Elastic Disaster Recovery.
- Una red para ejecutar Elastic Disaster Recovery, configurada de acuerdo con los ajustes de conectividad requeridos.

Limitaciones

- Puede usar este patrón para replicar todos los niveles, a menos que la base de datos esté alojada en Amazon Relational Database Service (Amazon RDS). En este caso, le recomendamos que use la funcionalidad de copia entre regiones de Amazon RDS.
- Elastic Disaster Recovery no es compatible con CloudEndure Disaster Recovery, pero puede actualizarse desde CloudEndure Disaster Recovery. Para obtener más información, consulte las preguntas frecuentes en la documentación de Elastic Disaster Recovery.
- Amazon Elastic Block Store (Amazon EBS) limita la velocidad a la que puede tomar instantáneas. Puede replicar un número máximo de 300 servidores en una única cuenta de AWS mediante Elastic Disaster Recovery. Para replicar más servidores, puede usar varias cuentas de AWS o varias regiones de AWS de destino. (Deberá configurar Elastic Disaster Recovery por separado en cada cuenta y región). Para más información, consulte las Prácticas recomendadas en la documentación de Elastic Disaster Recovery.
- Las cargas de trabajo de origen (la EnterpriseOne aplicación y la base de datos de JD Edwards) deben alojarse en instancias EC2. Este patrón no admite cargas de trabajo en las instalaciones o en otros entornos de nube.

- Este patrón se centra en los componentes de JD Edwards EnterpriseOne . Un plan completo de DR y continuidad empresarial (BCP) debe incluir otros servicios básicos, como:
  - Redes (nube privada virtual, subredes y grupos de seguridad)
  - Active Directory
  - Amazon WorkSpaces
  - Elastic Load Balancing
  - Un servicio de base de datos administrado como Amazon Relational Database Service (Amazon RDS).

Para obtener información adicional sobre los requisitos previos, configuraciones y limitaciones, consulte la documentación de Elastic Disaster Recovery.

Versiones de producto

- Oracle JD Edwards EnterpriseOne (versiones compatibles con Oracle y SQL Server basadas en los requisitos técnicos mínimos de Oracle)

Arquitectura

Pila de tecnología de destino

- Una sola región y una sola nube privada virtual (VPC) para producción y no producción, y una segunda región para DR
- Zonas de disponibilidad únicas para asegurar una baja latencia entre los servidores
- Un equilibrador de carga de aplicación que distribuya el tráfico de red para mejorar la escalabilidad y la disponibilidad de las aplicaciones en varias zonas de disponibilidad
- Amazon Route 53, para proporcionar configuración de sistema de nombres de dominio (DNS)
- Amazon proporcionará WorkSpaces a los usuarios una experiencia de escritorio en la nube
- Amazon Simple Storage Service (Amazon S3) para almacenar copias de seguridad, archivos y objetos
- Amazon CloudWatch para el registro, la supervisión y las alarmas de aplicaciones
- Amazon Elastic Disaster Recovery, para la recuperación de desastres

Arquitectura de destino

El siguiente diagrama muestra la arquitectura de recuperación ante desastres interregional de JD Edwards EnterpriseOne mediante Elastic Disaster Recovery.

Procedimiento

A continuación puede ver un resumen de alto nivel del proceso. Para más información, consulte la sección Epics.

- La replicación de Elastic Disaster Recovery comienza con una sincronización inicial. Durante esta sincronización inicial, el agente de replicación de AWS replica todos los datos de los discos de origen en el recurso correspondiente de la subred del área transitoria.
- La replicación continua sigue realizándose indefinidamente una vez finalizada la sincronización inicial.
- Debe revisar los parámetros de lanzamiento, que incluyen las configuraciones específicas del servicio y una plantilla de lanzamiento de Amazon EC2, una vez que se haya instalado el agente y se haya iniciado la replicación. Cuando se indique que el servidor de origen está listo para la recuperación, podrá iniciar las instancias.
- Cuando Elastic Disaster Recovery emite una serie de llamadas a la API para iniciar la operación de lanzamiento, la instancia de recuperación se lanza inmediatamente en AWS según la configuración de lanzamiento. El servicio activa automáticamente un servidor de conversión durante el inicio.
- La nueva instancia se activa en AWS una vez finalizada la conversión y está lista para usarse. El estado del servidor de origen en el momento del lanzamiento se representa mediante los volúmenes asociados a la instancia lanzada. El proceso de conversión implica cambios en los controladores, la red y la licencia del sistema operativo para asegurar que la instancia se inicie de forma nativa en AWS.
- Tras el lanzamiento, los volúmenes recién creados ya no se mantienen sincronizados con los servidores de origen. El agente de replicación de AWS sigue replicando de forma rutinaria los cambios realizados en los servidores de origen de los volúmenes del área transitoria, pero las instancias lanzadas no reflejan dichos cambios.
- Al iniciar una nueva instancia de simulacro o recuperación, los datos siempre se reflejan en el estado más reciente que se ha replicado desde el servidor de origen a la subred del área transitoria.
- Cuando el servidor de origen esté marcado como preparado para la recuperación, podrá iniciar las instancias.

> **Note**
>
> El proceso funciona en ambos sentidos: para la conmutación por error de una región de AWS principal a una región de DR, y también para la conmutación por recuperación al sitio principal una vez que se ha recuperado. Puede preparar la conmutación por recuperación invirtiendo la dirección de replicación de los datos desde el equipo de destino al equipo de origen de forma totalmente orquestada.

Entre las ventajas del proceso descrito en este patrón se incluyen las siguientes:

- Flexibilidad: los servidores de replicación escalan horizontal y verticalmente en función del conjunto de datos y del tiempo de replicación, por lo que puede realizar pruebas de DR sin interrumpir las cargas de trabajo de origen ni la replicación.
- Fiabilidad: la replicación es sólida, no disruptiva y continua.
- Automatización: esta solución proporciona un proceso unificado y automatizado para las pruebas, la recuperación y la conmutación por recuperación.
- Optimización de costos: puede replicar y pagar solo por los volúmenes necesarios, y pagar por los recursos de cómputo en el sitio de DR solo cuando esos recursos estén activados. Puede usar una instancia de replicación con costos optimizados (le recomendamos que emplee un tipo de instancia optimizada para la computación) para varias fuentes o una sola fuente con un gran volumen de EBS.

Automatización y escala

Al realizar una recuperación ante desastres a escala, los EnterpriseOne servidores de JD Edwards dependerán de otros servidores del entorno. Por ejemplo:

- Los servidores de EnterpriseOne aplicaciones de JD Edwards que se conectan a una base de datos EnterpriseOne compatible con JD Edwards durante el arranque dependen de esa base de datos.
- EnterpriseOne Los servidores de JD Edwards que requieren autenticación y necesitan conectarse a un controlador de dominio durante el arranque para iniciar los servicios dependen del controlador de dominio.

Por este motivo, le recomendamos que automatice las tareas de conmutación por error. Por ejemplo, puede usar AWS Lambda o AWS Step Functions para automatizar los scripts de EnterpriseOne inicio de JD Edwards y los cambios en el balanceador de carga para automatizar el end-to-end proceso de conmutación por error. Para obtener más información, consulte la publicación del blog Crear un plan de recuperación de desastres escalable con AWS Elastic Disaster Recovery.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Block Store (Amazon EBS) brinda volúmenes de almacenamiento por bloques para su uso con instancias de EC2.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- AWS Elastic Disaster Recovery minimiza el tiempo de inactividad y la pérdida de datos con una recuperación rápida y fiable de aplicaciones locales y basadas en la nube mediante un almacenamiento asequible, un cálculo y point-in-time una recuperación mínimos.
- Amazon Virtual Private Cloud (Amazon VPC) le ofrece un control total sobre su entorno de redes virtuales, incluida la ubicación de los recursos, la conectividad y la seguridad.

Prácticas recomendadas

Prácticas recomendadas generales

- Elabore con antelación un plan de acción en caso de que se produzca un evento de recuperación real.
- Después de configurar Elastic Disaster Recovery correctamente, cree una CloudFormation plantilla de AWS que pueda crear la configuración bajo demanda, en caso de que sea necesario. Determine el orden en el que deben lanzarse los servidores y las aplicaciones, y regístrelo en el plan de recuperación.
- Realice un simulacro regular (se aplican las tarifas estándar de Amazon EC2).
- Supervise el estado de la replicación en curso mediante la consola de Elastic Disaster Recovery o mediante programación.
- Proteja las point-in-time instantáneas y confirme antes de finalizar las instancias.
- Cree un rol de IAM para la instalación del agente de replicación de AWS.

- Habilite la protección de finalización de las instancias de recuperación en un escenario real de DR.
- No use la acción Desconectar de AWS en la consola de Elastic Disaster Recovery en los servidores para los que lanzó instancias de recuperación, incluso en el caso de un evento de recuperación real. Al realizar una desconexión, se cancelan todos los recursos de replicación relacionados con estos servidores de origen, incluidos los puntos de recuperación point-in-time (PIT).
- Modifique la política de PIT para cambiar el número de días de retención de las instantáneas.
- Edite la plantilla de lanzamiento, en la configuración de lanzamiento de Elastic Disaster Recovery, para configurar la subred, el grupo de seguridad y el tipo de instancia correctos para su servidor de destino.
- Automatice el proceso de end-to-end conmutación por error mediante Lambda o Step Functions para automatizar los scripts de inicio de JD EnterpriseOne Edwards y los cambios en el balanceador de carga.

Optimización y consideraciones de JD Edwards EnterpriseOne

- Vaya PrintQueuea la base de datos.
- Vaya MediaObjectsa la base de datos.
- Excluya los registros y la carpeta temporal de los servidores lógicos y por lotes.
- Excluya la carpeta temporal de Oracle WebLogic.
- Cree scripts para el inicio después de la conmutación por error.
- Excluya la tempdb de SQL Server.
- Excluya el archivo temporal de Oracle.

Epics

Realice las tareas y configuración iniciales

Tarea	Descripción	Habilidades requeridas
Configure la red de replicación.	Implemente su EnterpriseOne sistema JD Edwards en la región principal de AWS e identifique la región de AWS	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	para DR. Siga los pasos de la sección de requisitos de red de replicación de la documentación de Elastic Disaster Recovery para planificar y configurar su red de replicación y DR.	
Determine el RPO y el RTO.	Identifique el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO) para los servidores de aplicaciones y la base de datos.	Arquitecto de la nube, arquitecto de DR
Habilite la replicación para Amazon EFS.	Si procede, habilite la replicación desde la región principal de AWS a la región DR para sistemas de archivos compartidos como Amazon Elastic File System (Amazon EFS) mediante AWS DataSync, rsync u otra herramienta adecuada.	Administrador de la nube
Administre el DNS de DR.	Identifique el proceso para actualizar el sistema de nombres de dominio (DNS) durante el simulacro de DR o la recuperación real	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Crear un rol de IAM para la configuración.	Siga las instrucciones de la sección Inicialización y permisos de Elastic Disaster Recovery, de la documentación de Elastic Disaster Recovery, para crear un rol de IAM para inicializar y administrar el servicio de AWS.	Administrador de la nube
Configure las interconexiones con VPC.	Asegúrese de que el origen y el destino VPCs estén sincronizados y sean accesibles entre sí. Para obtener instrucciones sobre la configuración, consulte la documentación de Amazon VPC.	Administrador de AWS

Configure los parámetros de replicación de Elastic Disaster Recovery

Tarea	Descripción	Habilidades requeridas
Inicialice Elastic Disaster Recovery.	Abra la consola de Elastic Disaster Recovery, seleccione la región de AWS de destino (donde replicará los datos y lanzará las instancias de recuperación) y, a continuación, elija Cómo establecer la configuración de replicación predeterminada.	Administrador de AWS
Configure los servidores de replicación	1. En el panel Configurar servidores de replicación, introduzca la subred del	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	área transitoria y el tipo de instancia del servidor de replicación. La opción predeterminada es el tipo de instancia `t3.small`. Ajuste esta configuración en función de sus requisitos y recuerde tener en cuenta los precios de las instancias. Para obtener más información, consulte Precios de Amazon EC2. 2. En la sección Acceso al servicio, seleccione Ver detalles para revisar el rol vinculado al servicio y las políticas adicionales creadas durante la inicialización del servicio. 3. Elija Siguiente.	

Tarea	Descripción	Habilidades requeridas
Configure los volúmenes y los grupos de seguridad.	1. En el panel Volúmenes y grupos de seguridad , seleccione el tipo de volumen de EBS para el servidor de replicación y establezca el cifrado de Amazon EBS como Predeterminado. 2. Seleccione Usar siempre grupo de seguridad de AWS Elastic Disaster Recovery para que Elastic Disaster Recovery pueda adjuntar y supervisar automáticamente el grupo de seguridad predeterm inado. 3. Elija Siguiente.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure los ajustes adicionales.	1. En el panel Configuración adicional, configure el enrutamiento y la limitación de datos, la política de PIT y las etiquetas. • El enrutamiento y la limitación de datos controlan la forma en que los datos fluyen desde el servidor externo a los servidores de replicación. Seleccione Usar IP privada para la replicación de datos. De lo contrario, a los servidores de replicación se les asignará automáticamente una IP pública y los datos fluirán a través de la internet pública. • En la sección Políticas de tiempo (PIT), configure una política de retención que determine el tiempo después del cual no es necesario conservar las instantáneas. El periodo de retención predeterminado es de siete días. • En la sección Etiquetas, añada etiquetas personalizadas a los recursos creados por Elastic	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	Disaster Recovery en su cuenta de AWS. 2. Seleccione Siguiente, revise la configuración en el panel y, a continuación, elija Crear predeterminado para crear la plantilla predeterminada.	

Instale el agente de replicación de AWS

Tarea	Descripción	Habilidades requeridas
Crear un rol de IAM.	Cree un rol de IAM que contenga la política `AWSElasticDisasterRecoveryAgentInstallationPolicy` . En la sección Seleccionar tipo de acceso de AWS, habilite el acceso programático. Apunte el ID de clave de acceso y la clave de acceso secreta. Necesitará esta información durante la instalación del agente de replicación de AWS.	Administrador de AWS
Compruebe los requisitos.	Compruebe y complete los requisitos previos de la documentación de Elastic Disaster Recovery para instalar el agente de replicación de AWS.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

Instale el agente de replicación de AWS.	Siga las instrucciones de instalación de su sistema operativo e instale el agente de replicación de AWS.
	• Para Microsoft Windows: descargue los archivos de configuración y ejecute el archivo .exe como administrador. Siga las indicaciones para completar la instalación.
	• Para Linux: copie los siguientes comandos (en el orden en que aparecen) y péguelos en su sesión de Secure Shell (SSH). El primer comando descarga el instalador y el segundo lo ejecuta.
	`wget -O ./aws-replication-installer-init.py https://aws-elastic-disaster-recovery-us-west-2.s3.amazonaws.com/latest/linux/aws-replication-installer-init.py`
	`sudo python3 aws-replication-installer-init.py`
		Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	Siga las indicaciones para completar la instalación. **Note** Cambie la URL para que refleje su región. Repita estos pasos en el servidor restante.	
Supervisar la replicación	Regrese al panel Servidores de origen de Elastic Disaster Recovery para supervisar el estado de la replicación. La sincronización inicial tardará algún tiempo en función del tamaño de la transferencia de datos. Cuando el servidor de origen esté completamente sincronizado, el estado del servidor se actualizará a Listo. Esto significa que se ha creado un servidor de replicación en el área transitoria, y que los volúmenes de EBS se han replicado desde el servidor de origen al área de almacenamiento transitorio.	Administrador de AWS

Configure los ajustes de lanzamiento

Tarea	Descripción	Habilidades requeridas
Edite la configuración de lanzamiento.	Para actualizar la configuración de lanzamiento de las instancias de simulacro y recuperación, en la consola de Elastic Disaster Recovery, seleccione el servidor de origen y, a continuación, seleccione Acciones y Editar configuración de lanzamiento. También puede elegir las máquinas de origen que se van a replicar en la página Servidores de origen y, a continuación, elegir la pestaña Configuración de lanzamiento. Esta pestaña tiene dos secciones: Configuración general de lanzamiento y plantilla de lanzamiento de EC2.	Administrador de AWS
Configure los ajustes generales de lanzamiento.	Revise la configuración general de lanzamiento según sus necesidades. • Tamaño correcto del tipo de instancia: si elige Básico, Elastic Disaster Recovery omite el tipo de instancia que seleccionó en la plantilla de lanzamiento de Amazon EC2 y elige automáticamente el tipo	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	de instancia en función del sistema operativo, la CPU y la RAM del servidor de origen. • Copiar IP privada: seleccione si desea que Elastic Disaster Recovery se asegure de que la IP privada usada por la instancia de simulacro o recuperación coincide con la IP privada usada por el servidor de origen. Si elige Sí, asegúrese de que el rango de IP de la subred que configuró en la plantilla de lanzamiento de Amazon EC2 incluya la dirección IP privada. Para obtener más información, consulte la Configuración general de lanzamiento en la documentación de Elastic Disaster Recovery.	

Tarea	Descripción	Habilidades requeridas
Configure la plantilla de lanzamiento de Amazon EC2.	Elastic Disaster Recovery emplea plantillas de lanzamiento de Amazon EC2 para lanzar instancias de simulacro y recuperación para cada servidor de origen. La plantilla de lanzamiento se crea automáticamente para cada servidor de origen que añada a Elastic Disaster Recovery tras instalar AWS Replication Agent. Debe configurar la plantilla de lanzamiento de Amazon EC2 como plantilla de lanzamiento predeterminada si desea usarla con Elastic Disaster Recovery. Para obtener más información, consulte la Plantilla de lanzamiento de EC2 en la documentación de Elastic Disaster Recovery.	Administrador de AWS

Inicie el simulacro y la conmutación por error de DR

Tarea	Descripción	Habilidades requeridas
Inicie el simulacro	1. En la consola de Elastic Disaster Recovery, abra la página Servidores de origen y compruebe que el estado	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	del servidor de origen es Listo. 2. Seleccione todos los servidores de origen en los que desee realizar el simulacro de recuperación de desastres. 3. En el menú Iniciar el trabajo de recuperac ión, seleccione Iniciar el análisis y seleccione la point-in-time instantán ea adecuada. Se iniciará un trabajo de recuperac ión en los servidores de origen seleccionados. Puede supervisar el estado del trabajo en la pestaña Historial de trabajos de recuperación. La instancia de simulacro lanzada aparecerá también en la página Instancias de recuperación. **Note** Los cambios que se realicen en el servidor de origen se sincronizarán con el servidor de replicación, no	

Tarea	Descripción	Habilidades requeridas
	con la instancia de simulacro. 4. Pruebe y verifique la instancia de simulacro de DR. 5. En la página Instancias de recuperación, seleccione la instancia de simulacro y, a continuación, elija Acciones, Desconectar de AWS. Se eliminará AWS Replication Agent de la instancia de recuperac ión y se eliminarán todos los recursos asociados a la instancia de recuperac ión de Elastic Disaster Recovery. 6. Seleccione Eliminar instancias de recuperación. Se eliminará la represent ación de la instancia de la consola de Elastic Disaster Recovery y se desvinculará completamente la instancia del servicio de Elastic Disaster Recovery. No se eliminará la instancia de EC2 subyacente. 7. Finalice la instancia de simulacro de DR desde la consola de Amazon EC2.	

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte las Preparación para la conmutación por error en la documentación de Elastic Disaster Recovery.	
Valide el simulacro.	En el paso anterior, lanzó nuevas instancias de destino en la región de DR. Las instancias de destino son réplicas de los servidore s de origen basadas en la instantánea realizada al iniciar el lanzamiento. En este procedimiento, se conectará a las máquinas de destino de Amazon EC2 para confirmar que funcionan según lo previsto. 1. Abra la consola de Amazon EC2. 2. Seleccione Instancias (en ejecución). 3. Seleccione la instancia de destino y anote su IPv4 dirección privada. 4. Asegúrese de poder conectarse a la instancia EC2 y de que el JD Edwards EnterpriseOne y los componentes relaciona dos se replican según lo previsto.	

Tarea	Descripción	Habilidades requeridas
Iniciar la conmutación por error.	La conmutación por error es la redirección del tráfico de un sistema principal a un sistema secundario. Elastic Disaster Recovery le ayuda a realizar una conmutación por error al lanzar instancias de recuperación en AWS. Cuando se lanzan las instancias de recuperación, el tráfico de sus sistemas principales se redirige a estas instancias. 1. En la consola de Elastic Disaster Recovery, abra la página Servidores de origen y compruebe que en la columna Listo para recuperación del servidor de origen aparezca Listo, y que en la columna Estado de replicación de datos aparezca Correcto. 2. Seleccione el servidor de origen. En el menú Iniciar trabajo de recuperación, seleccione Iniciar recuperación. 3. Seleccione la point-in-time instantánea desde la que desea lanzar la instancia de recuperación y, a continuación, elija Iniciar la recuperación.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	Se iniciará un trabajo de recuperación. Puede supervisar el estado del trabajo en la página Instancias de recuperación. 4. Pruebe y verifique la instancia de recuperación. Si es necesario, ajuste la configuración del DNS y conecte la EnterpriseOne aplicación JD Edwards a la base de datos. 5. Ahora puede desconectar y retirar el EnterpriseOne servidor JD Edwards de origen, ya que todos los cambios se han escrito en la nueva instancia de recuperación. 6. Registre la instancia de recuperación como servidor de origen en la región de DR siguiendo el proceso descrito en la épica Instale el agente de replicación de AWS. Para más información, consulte las Efectuar una conmutación por error en la documentación de Elastic Disaster Recovery.	

Tarea	Descripción	Habilidades requeridas
Inicie la conmutación por recuperación.	El proceso para iniciar una conmutación por recuperación es similar al proceso para iniciar una conmutación por error. 1. Abre la consola de Elastic Disaster Recovery en la región principal. Vaya a la página Instancias de recuperación, seleccione la instancia de perforación y, a continuación, elija Acciones, Desconectar de AWS, Eliminar instancias de recuperación. 2. Abre la consola de Elastic Disaster Recovery en la región de DR. Registre su nuevo EnterpriseOne servidor de JD Edwards como servidor de origen en la región de RD mediante la instalación del AWS Replication Agent. Los datos se sincronizarán con un nuevo servidor de replicación aprovisionado en la nueva subred transitoria. **Note** Cuando el nuevo EnterpriseOne	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	servidor de JD Edwards se registre como servidor de origen, es posible que vea dos servidores de origen en la consola de Elastic Disaster Recovery: un servidor que se creó a partir de la instancia de EC2 principal y el nuevo servidor que se creó a partir de la instancia de recuperación. Se recomiend a etiquetar los servidores correctamente para evitar confusion es y, preferibl emente, añadir el nuevo servidor a la plantilla de lanzamiento. 3. Para reiniciar la replicaci ón de DR desde la región principal, desasocie la instancia de recuperación lanzada de la consola de Elastic Disaster Recovery en la región de DR y	

Tarea	Descripción	Habilidades requeridas
	registre el host como servidor de origen en la región principal. Para más información, consulte las Efectuar una conmutación por recuperación en la documentación de Elastic Disaster Recovery.	

Tarea	Descripción	Habilidades requeridas
Inicie los EnterpriseOne componentes de JD Edwards.	1. Inicie la EnterpriseOne base de datos de JD Edwards iniciando sesión en el servidor de la base de datos. 2. Cuando la base de datos esté en ejecución, inicie los servidores EnterpriseOne lógicos y de lotes de JD Edwards. 3. Comience WebLogic en los servidores web e inicie una instancia JAS en los servidores JAS. 4. Comience WebLogic en el servidor de aprovisio namiento y en el servidor de la consola SM. 5. Inicie SM Agent en los servidores. 6. Confirme que el inicio de sesión en JD Edwards EnterpriseOne funciona correctamente. Deberá incorporar los cambios en Route 53 y Application Load Balancer para que funcione el EnterpriseOne enlace de JD Edwards. Puede automatizar estos pasos mediante Lambda, Step	JD Edwards CNC Enterpris eOne

Tarea	Descripción	Habilidades requeridas
	Functions y Systems Manager (Run Command). **Note** Elastic Disaster Recovery realiza la replicación en cada bloque de los volúmenes de EBS de la instancia de EC2 de origen que alojan el sistema operativo y los sistemas de archivos. Los sistemas de archivos compartidos creados con Amazon EFS no forman parte de esta replicación. Puede replicar los sistemas de archivos compartidos en la región de DR mediante AWS DataSync, como se indica en la primera epopeya, y luego montar estos sistemas de archivos replicados en el sistema de DR.	

Resolución de problemas

Problema	Solución
El estado de la replicación de los datos del servidor de origen es Estancado y la replicación se retrasa. Si comprueba los detalles, el estado de la replicación de datos muestra Agente no encontrado.	Compruebe que el servidor de origen estancado está en funcionamiento. **Note** Si el servidor de origen deja de funcionar, el servidor de replicación finaliza automáticamente. Para obtener más información sobre problemas de retardo, consulte Problemas de retardo en la replicación en la documentación de Elastic Disaster Recovery.
La instalación de AWS Replication Agent en la instancia de EC2 de origen falla en RHEL 8.2 después de escanear los discos. `aws_replication_agent_installer.log` indica que faltan los encabezados del kernel.	Antes de instalar AWS Replication Agent en RHEL 8, CentOS 8 u Oracle Linux 8, ejecute: `sudo yum install elfutils-libelf-devel` Para más información, consulte las Requisitos de instalación de Linux en la documentación de Elastic Disaster Recovery.
En la consola de Elastic Disaster Recovery, verá el servidor de origen como Listo con retardo, y el estado de replicación de datos como Estancado. En función del tiempo que AWS Replication Agent no esté disponible, el estado puede indicar un retardo elevado, pero el problema seguirá siendo el mismo.	Use un comando del sistema operativo para confirmar que AWS Replication Agent se está ejecutando en la instancia de EC2 de origen o confirme que la instancia se está ejecutando. Tras corregir los problemas, Elastic Disaster Recovery reiniciará el escaneo. Espere a que se hayan sincronizado todos los datos y el

Problema	Solución
	estado de la replicación sea Correcto antes de iniciar un simulacro de DR.
Replicación inicial con retardo elevado. En la consola de Elastic Disaster Recovery, puede ver que el estado de sincronización inicial es extremadamente lento para un servidor de origen.	Compruebe los problemas de retardo en la replicación documentados en la sección Problemas de retardo en la replicación de la documentación de Elastic Disaster Recovery. Es posible que el servidor de replicación no pueda gestionar la carga debido a las operaciones informáticas intrínsecas. En ese caso, intente actualizar el tipo de instancia tras consultar con el equipo de soporte técnico de AWS.

Recursos relacionados

- Guía del usuario de AWS Elastic Disaster Recovery
- Crear un plan de recuperación de desastres escalable con AWS Elastic Disaster Recovery (publicación del blog de AWS)
- AWS Elastic Disaster Recovery: introducción técnica (curso de AWS Skill Builder; requiere iniciar sesión)
- Guía de inicio rápido de AWS Elastic Disaster Recovery

Configure la detección de CloudFormation desviaciones en una organización multirregional y multicuenta

Ram Kandaswamy, Amazon Web Services

Resumen

Los usuarios de Amazon Web Services (AWS) suelen buscar una forma eficaz de detectar los desajustes en la configuración de los recursos, incluida la desviación en las AWS CloudFormation pilas, y solucionarlos lo antes posible. Este es especialmente el caso cuando se AWS Control Tower utiliza.

Este patrón proporciona una solución prescriptiva que resuelve el problema de manera eficiente mediante el uso de cambios consolidados en la configuración de los recursos y la adopción de medidas en función de esos cambios para generar resultados. La solución está diseñada para situaciones en las que se crean varias CloudFormation pilas en más de una Región de AWS, en más de una cuenta, o en una combinación de ambas. Los objetivos de la solución son los siguientes:

- Simplificar el proceso de detección de desviaciones
- Configurar las notificaciones y las alertas
- Configurar los informes consolidados

Requisitos previos y limitaciones

Requisitos previos

- AWS Config está habilitada en todas las regiones y cuentas que se deben monitorear

Limitaciones

- El informe generado solo admite valores separados por comas (CSV) y JSON.

Arquitectura

El siguiente diagrama muestra la AWS Organizations configuración con varias cuentas. AWS Config las reglas se comunican entre las cuentas.

En el flujo de trabajo se incluyen los pasos siguientes:

1. La AWS Config regla detecta la desviación.
2. Los resultados de la detección de desviaciones que se encuentran en otras cuentas se envían a la cuenta de administración.
3. La CloudWatch regla de Amazon llama a una AWS Lambda función.
4. La función Lambda consulta la AWS Config regla para obtener resultados agregados.
5. La función de Lambda notifica a Amazon Simple Notification Service (Amazon SNS), que notifica la desviación por correo electrónico.

Automatización y escala

La solución que se presenta aquí puede escalarse tanto para regiones como para cuentas adicionales.

Tools (Herramientas)

Servicios de AWS

- AWS Configproporciona una vista detallada de la configuración de AWS los recursos de su Cuenta de AWS. Esto incluye cómo se relacionan los recursos entre sí y cómo se han configurado en el pasado, para que pueda ver cómo las configuraciones y las relaciones cambian a lo largo del tiempo.
- Amazon le CloudWatch ayuda a supervisar las métricas de sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.

Epics

Automatice la detección de desviaciones para CloudFormation

Tarea	Descripción	Habilidades requeridas
Cree el agregador.	1. Inicie sesión en https://console.aws.amazon.com/config Consola de administración de AWS y abra la AWS Config consola. 2. Cree un agregador en la cuenta de administración. 3. Asegúrese de que la replicación de datos esté activada para AWS Config poder obtener datos de las cuentas de origen. 4. Seleccione todas las regiones y cuentas aplicables. Puede seleccionar las cuentas según AWS Organizations. Recomendamos este enfoque porque las cuentas nuevas de la organización forman parte automáticamente del agregador.	Arquitecto de la nube
Cree una regla AWS gestionada.	Añada la regla `cloudformation-stack-drift-detection-check` AWS gestionada. La regla necesita un valor de parámetro: `cloudformationArn` .	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Introduzca el nombre de recurso de Amazon (ARN) del rol de IAM que tiene los permisos de detectar la desviación de las pilas. El rol debe tener una política de confianza que AWS Config permita asumirlo.	
Cree la sección de consultas avanzadas del agregador.	Para buscar pilas desviadas de varias fuentes, cree la siguiente consulta: `SELECT resourceId, configuration.driftInformation.stackDriftStatus WHERE resourceType = 'AWS::CloudFormation::Stack' AND configuration.driftInformation.stackDriftStatus IN ('DRIFTED')`	Arquitecto de la nube, desarrollador
Automatice la ejecución de la consulta y la publicación.	1. Cree una función de Lambda con el código que se adjunta. Lambda publicará los resultados en un tema de SNS que se proporciona como variable de entorno en la función de Lambda. 2. Para recibir alertas, cree una suscripción por correo electrónico al tema de SNS.	Arquitecto de la nube, desarrollador

Tarea	Descripción	Habilidades requeridas
Cree una CloudWatch regla.	Cree una CloudWatch regla basada en la programac ión para llamar a la función Lambda, que es responsable de las alertas.	Arquitecto de la nube

Recursos relacionados

Recursos

- ¿Qué es? AWS Config
- Acumulación de datos de multicuentas y multiregiones
- Detección de cambios de configuración no administrados en pilas y recursos
- IAM: Transferir una función de IAM a una función específica Servicio de AWS
- ¿Qué es Amazon SNS?

Información adicional

Consideraciones

Recomendamos utilizar la solución presentada en este patrón en lugar de utilizar soluciones personalizadas que impliquen llamadas a la API en intervalos específicos para iniciar la detección de desviaciones en cada CloudFormation pila o conjunto de pilas. Las soluciones personalizadas que utilizan llamadas a la API en intervalos específicos pueden provocar un gran número de llamadas a la API y afectar al rendimiento. Debido a la cantidad de llamadas a la API, se pueden producir limitaciones. Otro posible problema es el retraso en la detección si los cambios en los recursos se identifican únicamente en función de la programación.

Dado que los conjuntos de pilas se componen de pilas, puede utilizar esta solución. Los detalles de las instancias de pilas también están disponibles como parte de la solución.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Importación correcta de un bucket de S3 como CloudFormation pila de AWS

Ram Kandaswamy, Amazon Web Services

Resumen

Si utiliza los recursos de Amazon Web Services (AWS), como los buckets de Amazon Simple Storage Service (Amazon S3), y desea utilizar un enfoque de infraestructura como código (IaC), puede importar sus recursos a CloudFormation AWS y gestionarlos como una pila.

Este patrón proporciona los pasos para importar correctamente un bucket de S3 como una CloudFormation pila de AWS. Al utilizar este enfoque de patrón, puede evitar los posibles errores que podrían producirse si importa su bucket de S3 en una sola acción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un bucket de S3 y una política de bucket de S3 existentes. Para obtener más información al respecto, consulte Qué política de bucket de S3 debo usar para cumplir con la regla s3- de AWS Config bucket-ssl-requests-only en el Centro de conocimiento de AWS.
- Una clave de AWS Key Management Service (AWS KMS) existente y su alias. Para obtener más información, consulte Trabajar con alias en la documentación de AWS KMS.
- La CloudFormation plantilla de `CloudFormation-template-S3-bucket` AWS de muestra (adjunta), descargada en su ordenador local.

Arquitectura

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El usuario crea una plantilla de AWS CloudFormation con formato JSON o YAML.
2. La plantilla crea una CloudFormation pila de AWS para importar el bucket de S3.
3. La CloudFormation pila de AWS administra el depósito de S3 que especificó en la plantilla.

Pila de tecnología

- AWS CloudFormation
- AWS Identity y Access Management (IAM)
- AWS KMS
- Amazon S3

Herramientas

- AWS CloudFormation: AWS le CloudFormation ayuda a crear y aprovisionar despliegues de infraestructura de AWS de forma predecible y repetitiva.
- AWS Identity and Access Management (IAM): IAM es un servicio web que le ayuda a controlar el acceso seguro a los servicios de AWS.
- AWS KMS: AWS Key Management Service (AWS KMS) es un servicio de cifrado y administración de claves adaptado a la nube.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet.

Epics

Importe un bucket de S3 con cifrado AWS KMS key basado en una CloudFormation pila de AWS

Tarea	Descripción	Habilidades requeridas

Cree una plantilla para importar el bucket de S3 y la clave de KMS.	En su equipo local, cree una plantilla para importar el bucket de S3 y la clave de KMS con la plantilla de muestra siguiente:
	`AWSTemplateFormatVersion: 2010-09-09`
	`Parameters:`
	`  bucketName:`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	<pre> Type: String
	
	Resources:
	
	  S3Bucket:
	
	    Type: 'AWS::S3:
	:Bucket'
	
	    DeletionPolicy:
	 Retain
	
	    Properties:
	
	      BucketName: !Ref
	 bucketName
	
	      BucketEncryption:
	
	        ServerSid
	eEncryptionConfigu
	ration:
	
	          - ServerSid
	eEncryptionByDefault:
	
	              SSEAlgori
	thm: 'aws:kms'
	
	              KMSMaster
	KeyID: !GetAtt
	
	                -
	 KMSS3Encryption
	
	                - Arn
	
	  KMSS3Encryption:
	
	    Type: 'AWS::KMS
	::Key'</pre>	

Tarea	Descripción	Habilidades requeridas

	<pre> DeletionPolicy: Retain
	   Properties:
	     Enabled: true
	     KeyPolicy: !Sub |-
	       {
	           "Id": "key-consolepolicy-3",
	           "Version": "2012-10-17",
	           "Statement": [
	               {
	"Sid": "Enable IAM User Permissions",
	"Effect": "Allow",
	"Principal": {
	"AWS": ["arn:aws:iam::${AWS::AccountId}:root"]
	                   },</pre>	

Tarea	Descripción	Habilidades requeridas

	<pre>"Action": "kms:*",
	
	"Resource": "*"
	}
	}
	]
	}
	
	EnableKey
	Rotation: true</pre>	

Tarea	Descripción	Habilidades requeridas
Cree la pila.	1. Inicie sesión en la consola de administración de AWS, abra la CloudFormation consola de AWS, elija Ver pila, elija Crear pila y, a continuación, elija Con recursos existentes (importar recursos). 2. Elija Upload a template file (Cargar un archivo de plantilla) y, a continuac ión, cargue el archivo de plantilla que creó anteriorm ente. 3. Introduzca un nombre para su pila y configure las opciones restantes según sus necesidades. 4. Seleccione Create stack (Crear pila) y espere a que el estado de la colección cambie a `IMPORT_CO MPLETE` .	AWS DevOps

Tarea	Descripción	Habilidades requeridas

Cree el alias de la clave KMS.	1. En la CloudFormation consola de AWS, elija Stacks, elija el nombre de la pila que creó anteriormente, elija el panel Template y, a continuación, elija View in Designer.
	2. Añada el siguiente fragmento a la sección `Resource` de la plantilla y, a continuación, elija Create stack (Crear pila) y complete el asistente:
	
	`KMSS3EncryptionAlias:`
	
	`  Type: 'AWS::KMS ::Alias'`
	
	`  DeletionPolicy: Retain`
	
	`  Properties:`
	
	`  AliasName: alias/S3BucketKey`
	
	`  TargetKeyId: !Ref KMSS3Encryption`
	
	Para obtener más información al respecto, consulte las actualizaciones de la CloudFormation pila de
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	AWS en la CloudFormation documentación de AWS.	

Tarea	Descripción	Habilidades requeridas

Actualice la pila para incluir la política de bucket de S3.	1. En la CloudFormation consola de AWS, elija Stacks, elija el nombre de la pila que creó anteriormente, elija el panel Template y, a continuación, elija View in Designer.
	2. Añada el siguiente fragmento a la sección `Resource` de la plantilla y, a continuación, elija Create stack (Crear pila) y complete el asistente:
	
	`S3BucketPolicy:`
	
	`  Type: 'AWS::S3::BucketPolicy'`
	
	`  Properties:`
	
	`    Bucket: !Ref S3Bucket`
	
	`    PolicyDocument: !Sub |-`
	
	`      {`
	
	`  "Version": "2008-10-17",`
	
	`  "Id": "restricthttp",`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	"Statement": [
	{
	"Sid": "denyhttp",
	"Effect": "Deny",
	"Principal": {
	"AWS": "*"
	},
	"Action": "s3:*",
	"Resource": ["arn:aws:s3:::${S3Bucket}","arn:aws:s3:::${S3Bucket}/*"],
	"Condition": {
	"Bool": {
	"aws:SecureTransport": "false"
	}	

Tarea	Descripción	Habilidades requeridas
	} }] } **Note** Esta política de bucket de S3 tiene una declaración de denegación que restringe las llamadas a la API que no son seguras.	

Tarea	Descripción	Habilidades requeridas
Actualice la política de claves.	1. En la CloudFormation consola de AWS, elija Stacks, elija el nombre de la pila que creó anteriormente, elija el panel Template y, a continuación, elija View in Designer. 2. Modifique el recurso KMS de la plantilla para incluir la política de claves que permite a los administr adores administrar la clave de KMS. 3. Elija Create stack (Crear pila), elija Next (Siguiente) y, a continuación, complete el asistente según sus necesidades. Para más información, consulte Políticas de claves en AWS KMS en la documenta ción de AWS KMS.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

Adición de etiquetas de nivel de recursos.	1. En la CloudFormation consola de AWS, elija Stacks, elija el nombre de la pila que creó anteriormente, elija el panel Template y, a continuación, elija View in Designer.
	2. Añada el siguiente fragmento a la sección `Properties` de recursos de Amazon S3 de la plantilla y, a continuación, elija Crear pila y complete el asistente:
	`Tags:`
	`- Key: createdBy`
	`Value: Cloudformation`
		AWS DevOps

Recursos relacionados

- Incorporar los recursos existentes a la CloudFormation administración de AWS
- AWS re:Invent 2017: información detallada sobre AWS CloudFormation (vídeo)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Sincronice los datos entre los sistemas de archivos de Amazon EFS en distintas regiones de AWS mediante AWS DataSync

Sarat Chandra Pothula y Aditya Ambati, Amazon Web Services

Resumen

Esta solución proporciona un marco sólido para una sincronización de datos eficiente y segura entre instancias de Amazon Elastic File System (Amazon EFS) en regiones de AWS distintas. Este enfoque es escalable y proporciona una replicación de datos controlada entre regiones. Esta solución puede mejorar sus estrategias de recuperación ante desastres y redundancia de datos.

Al utilizar AWS Cloud Development Kit (AWS CDK), este patrón utiliza un enfoque de infraestructura como código (IaC) para implementar los recursos de la solución. La aplicación AWS CDK implementa los recursos esenciales de AWS, DataSync Amazon EFS, Amazon Virtual Private Cloud (Amazon VPC) y Amazon Elastic Compute Cloud (Amazon). EC2 Esta IaC proporciona un proceso de implementación repetible y controlado por versiones que está totalmente alineado con las prácticas recomendadas de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- La versión 2.9.11 o posterior de la Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada
- La versión 2.114.1 o posterior de AWS CDK instalada y arrancada
- La versión 20.8.0 o posterior de NodeJS instalada

Limitaciones

- La solución hereda las limitaciones de DataSync Amazon EFS, como las tasas de transferencia de datos, las limitaciones de tamaño y la disponibilidad regional. Para obtener más información, consulte Cuotas de AWS y DataSync Cuotas de Amazon EFS.
- Esta solución solo es compatible con Amazon EFS. DataSync es compatible con otros servicios de AWS, como Amazon Simple Storage Service (Amazon S3) y FSx Amazon for Lustre. Sin embargo, esta solución requiere modificaciones para sincronizar los datos con estos otros servicios.

Arquitectura

Esta solución implementa las pilas siguientes de AWS CDK:

- Pila de Amazon VPC: esta pila configura los recursos de la nube privada virtual (VPC), tal como las subredes, una puerta de enlace de Internet y una puerta de enlace NAT en las regiones de AWS principal y secundaria.
- Pila de Amazon EFS: esta pila implementa los sistemas de archivos de Amazon EFS en las regiones principal y secundaria y los conecta a sus respectivas VPCs regiones.
- Amazon EC2 stack: esta pila lanza EC2 instancias en las regiones principal y secundaria. Estas instancias están configuradas para montar el sistema de archivos de Amazon EFS, lo que les permite acceder al almacenamiento compartido.
- DataSync pila de ubicaciones: esta pila utiliza una construcción personalizada llamada `DataSyncLocationConstruct` para crear recursos de DataSync ubicación en las regiones principal y secundaria. Estos recursos definen los puntos de conexión para la sincronización de datos.
- DataSync pila de tareas: esta pila utiliza una construcción personalizada llamada `DataSyncTaskConstruct` para crear una DataSync tarea en la región principal. Esta tarea está configurada para sincronizar los datos entre las regiones principal y secundaria mediante las ubicaciones de DataSync origen y destino.

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- AWS DataSync es un servicio de transferencia y descubrimiento de datos en línea que le ayuda a mover archivos o datos de objetos hacia, desde y entre los servicios de almacenamiento de AWS.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Elastic File System (Amazon EFS) le ayuda a crear y configurar sistemas de archivos compartidos en la nube de AWS.

- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Repositorio de código

El código de este patrón está disponible en el repositorio de DataSync proyectos multiregionales de GitHub Amazon EFS.

Prácticas recomendadas

Siga las prácticas recomendadas descritas en Prácticas recomendadas para usar la CDK de AWS TypeScript para crear proyectos de IaC.

Epics

Implementación de la aplicación de AWS CDK

Tarea	Descripción	Habilidades requeridas
Clone el repositorio del proyecto.	Introduzca el siguiente comando para clonar el repositorio del DataSync proyecto multiregional de Amazon EFS. `git clone https://github.com/aws-samples/aws-efs-crossregion-datasync.git`	AWS DevOps
Instale las dependencias de npm.	Escriba el siguiente comando. `npm ci`	AWS DevOps
Elija las regiones principal y secundaria.	En el repositorio clonado, vaya al directorio `src/infra`. En el archivo `Launcher.`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`ts` , actualice los valores de `PRIMARY_AWS_REGION` y `SECONDARY_AWS_REGION` . Utilice los códigos de región correspondientes. `const primaryRegion = { account: account, region: '<PRIMARY_AWS_REGION>' }; const secondaryRegion = { account: account, region: '<SECONDARY_AWS_REGION>' };`	
Arranque el entorno de .	Introduzca el comando siguiente para iniciar la cuenta de AWS y región de AWS que quiere utilizar. `cdk bootstrap <aws_account>/<aws_region>` Para obtener más información, consulte Proceso de arranque en la documentación de AWS CDK.	AWS DevOps
Enumere las pilas de CDK de AWS.	Introduzca el comando siguiente para ver una lista de las pilas de AWS CDK de la aplicación. `cdk ls`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Sincronice las pilas de AWS CDK.	Introduzca el siguiente comando para generar una CloudFormation plantilla de AWS para cada pila definida en la aplicación AWS CDK. `cdk synth`	AWS DevOps
Implemente la aplicación de AWS CDK.	Introduzca el comando siguiente para implementar todas las pilas en su cuenta de AWS, sin necesidad de aprobación manual para hacer cambios. `cdk deploy --all --require-approval never`	AWS DevOps

Validación de la implementación

Tarea	Descripción	Habilidades requeridas
Inicie sesión en la EC2 instancia de la región principal .	1. Con Session Manager, una función de AWS Systems Manager, inicie sesión en la EC2 instancia de la región principal. Para obtener instrucciones, consulte el tema sobre cómo conectarse a una instancia de Linux mediante Administrador de sesiones de AWS Systems Manager.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	2. Cambie los directorios a la ruta de montaje de Amazon EFS. `cd /mnt/efs`	

Cree un archivo temporal.	Introduzca el comando siguiente para crear un archivo temporal en la ruta de montaje de Amazon EFS.
	`sudo dd if=/dev/zero \`
	`of=tmptst.dat \`
	`bs=1G \`
	`seek=5 \`
	`count=0`
	
	`ls -lrt tmptst.dat`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

Inicie la DataSync tarea.	Introduzca el siguiente comando para replicar el archivo temporal de la región principal a la región secundaria, donde `<ARN-task>` se encuentra el nombre del recurso de Amazon (ARN) de la tarea. DataSync
	`aws datasync start-task-execution \`
	`--task-arn <ARN-task>`
	El comando devuelve el ARN de la ejecución de la tarea con el formato siguiente:
	`arn:aws:datasync:<region>:<account-ID>:task/task-execution/<exec-ID>`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
Compruebe el estado de la transferencia de datos.	Introduzca el siguiente comando para describir la tarea de DataSync ejecución , donde `<ARN-task-execution>` está el ARN de la ejecución de la tarea. `aws datasync describe-task-execution \ --task-execution-arn <ARN-task-execution>` La DataSync tarea está completa cuando `PrepareStatus` `TransferStatus` , y `VerifyStatus` todas tienen el valor`SUCCESS`.	AWS DevOps
Inicie sesión en la EC2 instancia de la región secundaria.	1. Con Session Manager, una función de AWS Systems Manager, inicie sesión en la EC2 instancia de la región secundaria. Para obtener instrucciones, consulte el tema sobre cómo conectarse a una instancia de Linux mediante Administrador de sesiones de AWS Systems Manager. 2. Cambie los directorios a la ruta de montaje de Amazon EFS. `cd /mnt/efs`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Valide la replicación.	Introduzca el comando siguiente para verificar que el archivo temporal existe en el sistema de archivos de Amazon EFS. `ls -lrt tmptst.dat`	AWS DevOps

Recursos relacionados

Documentación de AWS

- AWS CDK API Reference
- Configuración de las DataSync transferencias de AWS con Amazon EFS
- Solución de problemas con las DataSync transferencias de AWS

Otros recursos de AWS

- AWS DataSync FAQs

Pruebe AWS la infraestructura mediante LocalStack Terraform Tests

Ivan Girardi y Ioannis Kalyvas, Amazon Web Services

Resumen

Este patrón le ayuda a probar localmente la infraestructura como código (IaC) AWS en Terraform sin necesidad de aprovisionar la infraestructura en su entorno. AWS Integra el marco de pruebas de Terraform con. LocalStack El contenedor LocalStack Docker proporciona un entorno de desarrollo local que emula varios. Servicios de AWS Esto le permite probar e iterar las implementaciones de infraestructura sin generar costos en la Nube de AWS.

Esta solución proporciona los siguientes beneficios:

- Optimización de costos: la ejecución de pruebas LocalStack elimina la necesidad de usarlo. Servicios de AWS Esto evita que incurra en los costos asociados con la creación, el funcionamiento y la modificación de esos AWS recursos.
- Velocidad y eficiencia: las pruebas locales también suelen ser más rápidas que implementar los AWS recursos. Este rápido ciclo de retroalimentación acelera el desarrollo y la depuración. Como LocalStack se ejecuta de forma local, puede desarrollar y probar sus archivos de configuración de Terraform sin conexión a Internet. Puede depurar los archivos de configuración de Terraform de forma local y recibir comentarios de inmediato, lo que simplifica el proceso de desarrollo.
- Consistencia y reproducibilidad: LocalStack proporciona un entorno coherente para las pruebas. Esta coherencia ayuda a garantizar que las pruebas arrojen los mismos resultados, independientemente de los AWS cambios externos o los problemas de la red.
- Aislamiento: las pruebas permiten LocalStack evitar que se afecten accidentalmente a AWS los recursos activos o a los entornos de producción. Este aislamiento permite experimentar y probar varias configuraciones de manera segura.
- Automatización: la integración con una canalización de integración y entrega continuas (CI/CD) le permite probar automáticamente los archivos de configuración de Terraform. La canalización prueba minuciosamente la IaC antes de la implementación.
- Flexibilidad: puede simular diferentes Regiones de AWS configuraciones y configuraciones de servicio para que se adapten mejor a sus entornos de producción. Cuentas de AWS

Requisitos previos y limitaciones

Requisitos previos

- Instalar Docker
- Habilite el acceso al socket de Docker predeterminado (`/var/run/docker.sock`). Para obtener más información, consulte la Documentación de LocalStack .
- Instalación de Docker Compose
- Instalación de la versión 1.6.0 o posterior de Terraform
- Instalación de la CLI de Terraform
- Configure el proveedor de Terraform AWS
- (Opcional) Instale y configure el AWS Command Line Interface (AWS CLI). Para ver un ejemplo de cómo usar el AWS CLI with LocalStack, consulta el repositorio de GitHub pruebas de AWS infraestructura LocalStack y Terraform Tests.

Limitaciones

- Este patrón proporciona ejemplos explícitos para probar los recursos de Amazon Simple Storage Service (Amazon S3) AWS Lambda y AWS Step Functions Amazon DynamoDB. Sin embargo, puede ampliar esta solución para incluir recursos adicionales AWS .
- Este patrón proporciona instrucciones para ejecutar las pruebas de Terraform de forma local, pero ¿se pueden integrar las pruebas en cualquier CI/CD proceso?
- Este patrón proporciona instrucciones para usar la imagen de la LocalStack comunidad. Si utilizas la imagen LocalStack Pro, consulta la documentación de LocalStack Pro.
- LocalStack proporciona servicios de emulación para diferentes. AWS APIs Para una lista completa, consulte AWS Service Feature Coverage. Es posible que algunas funciones avanzadas requieran una suscripción a LocalStack Pro.

Arquitectura

En el siguiente diagrama se muestra la arquitectura para esta solución. Los componentes principales son un repositorio de código fuente, una CI/CD canalización y un contenedor de LocalStack Docker. El contenedor LocalStack Docker aloja lo siguiente de forma local: Servicios de AWS

- Un bucket de Amazon S3 para almacenar archivos
- Amazon CloudWatch para la supervisión y el registro
- Una AWS Lambda función para ejecutar código sin servidor
- Una máquina de AWS Step Functions estados para organizar flujos de trabajo de varios pasos

- Una tabla de Amazon DynamoDB para almacenar datos de NoSQL

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Agregue y confirme un archivo de configuración de Terraform en el repositorio de código fuente.
2. La CI/CD canalización detecta los cambios e inicia un proceso de compilación para el análisis estático del código de Terraform. La canalización crea y ejecuta el contenedor de LocalStack Docker. A continuación, la canalización inicia el proceso de prueba.
3. La canalización carga un objeto en un bucket de Amazon S3 que está alojado en el contenedor de LocalStack Docker.
4. Al cargar el objeto, se invoca una función. AWS Lambda
5. La función Lambda almacena la notificación de eventos de Amazon S3 en un CloudWatch registro.
6. La función Lambda inicia una máquina de AWS Step Functions estados.
7. La máquina de estados escribe el nombre del objeto de Amazon S3 en una tabla de DynamoDB.
8. El proceso de prueba de la CI/CD canalización comprueba que el nombre del objeto cargado coincide con la entrada de la tabla de DynamoDB. También verifica que el bucket de S3 se haya implementado con el nombre especificado y que la AWS Lambda función se haya implementado correctamente.

Tools (Herramientas)

Servicios de AWS

- Amazon le CloudWatch ayuda a supervisar las métricas de sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Step Functionses un servicio de organización sin servidor que le ayuda a combinar AWS Lambda funciones y otras Servicios de AWS para crear aplicaciones críticas para la empresa.

Otras herramientas

- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización a nivel del sistema operativo para entregar software en contenedores.
- Docker Compose es una herramienta para definir y ejecutar aplicaciones de varios contenedores.
- LocalStackes un emulador de servicios en la nube que se ejecuta en un único contenedor. Al usarlo LocalStack, puede ejecutar cargas de trabajo en la máquina local que utilice Servicios de AWS, sin necesidad de conectarse al Nube de AWS.
- Terraform es una herramienta de iAC HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.
- Terraform Tests le permite a validar las actualizaciones de configuración de los módulos de Terraform mediante pruebas análogas a las pruebas de integración o unitarias.

Repositorio de código

El código de este patrón está disponible en la AWS infraestructura de GitHub pruebas mediante el repositorio de Terraform LocalStack Tests.

Prácticas recomendadas

- Esta solución prueba la AWS infraestructura que se especifica en los archivos de configuración de Terraform y no implementa esos recursos en ellos. Nube de AWS Si quiere implementar los recursos, siga el principio del mínimo privilegio (documentación de IAM) y, de manera correcta, configure el backend de Terraform (documentación de Terraform).
- Al LocalStack integrarlo en una CI/CD canalización, le recomendamos que no ejecute el contenedor LocalStack Docker en modo privilegiado. Para obtener más información, consulte Privilegios de tiempo de ejecución y capacidades de Linux (documentación de Docker) y Seguridad para ejecutores autogestionados (GitLab documentación).

Epics

Implementar la solución

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	En un intérprete de comandos de bash, ingrese el siguiente comando. Esto clona la AWS infraestructura de pruebas mediante LocalStack un repositorio de Terraform Tests de: GitHub `git clone https://github.com/aws-samples/localstack-terraform-test.git`	DevOps ingeniero

Ejecute el LocalStack contenedor.	1. Introduzca el siguiente comando para ir al repositorio clonado:
	`cd localstack-terraform-test`
	2. Ingresa el siguiente comando para iniciar el contenedor de LocalStack Docker en modo separado:
	`docker-compose up -d`
	3. Espere a que el contenedor LocalStack Docker esté operativo.
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Inicialice Terraform.	Introduzca el comando siguiente para inicializar Terraform: `terraform init`	DevOps ingeniero

Ejecute Terraform Tests.	1. Introduzca el comando siguiente para ejecutar Terraform Tests:
	`terraform test`
	2. Verifique que las pruebas se hayan completado correctamente. El resultado debería ser similar al siguiente:
	`Success! 3 passed, 0 failed.`
		DevOps ingeniero

Eliminación de recursos.	Introduzca el siguiente comando para destruir el LocalStack contenedor: `docker-compose down`	DevOps ingeniero

Resolución de problemas

Problema	Solución
Resultado de `Error: reading DynamoDB Table Item (Files|README.md):`	1. Vuelva a introducir el comando `terraform test`.

Problema	Solución

`empty` al ejecutar el comando `terraform test`.	2. Si eso no resuelve el error, edite el archivo main.tf para aumentar el tiempo de espera de inactividad a un valor superior a 15 segundos:
	`resource "time_sleep" "wait" {`
	`  create_duration = "15s"`
	`  triggers = {`
	`  s3_object = local.key_json`
	`  }`
	`}`

Recursos relacionados

- Cómo empezar con Terraform: orientación para AWS CDKAWS CloudFormation expertos (orientación AWS prescriptiva)
- Mejores prácticas para usar el AWS proveedor de Terraform (guía prescriptiva)AWS
- Terraform CI/CD y sus pruebas AWS con el nuevo Terraform Test Framework (entrada del blog)AWS
- Acelerar la entrega de software con LocalStack Cloud Emulator desde AWS Marketplace (AWS entrada del blog)

Información adicional

Integración con GitHub acciones

Puedes integrar LocalStack y terraformar las pruebas en una CI/CD canalización mediante GitHub Actions. Para obtener más información, consulta la documentación de GitHub Actions. El siguiente es un ejemplo de archivo de configuración de GitHub Actions:

```
name: LocalStack Terraform Test

on:
  push:
    branches:
      - '**'
```

```
  workflow_dispatch: {}

jobs:
  localstack-terraform-test:
    runs-on: ubuntu-latest

    steps:
    - uses: actions/checkout@v4

    - name: Build and Start LocalStack Container
      run: |
        docker compose up -d

    - name: Setup Terraform
      uses: hashicorp/setup-terraform@v3
      with:
        terraform_version: latest

    - name: Run Terraform Init and Validation
      run: |
        terraform init
        terraform validate
        terraform fmt --recursive --check
        terraform plan
        terraform show

    - name: Run Terraform Test
      run: |
        terraform test

    - name: Stop and Delete LocalStack Container
      if: always()
      run: docker compose down
```

Actualice los clústeres de SAP Pacemaker de a ENSA1 ENSA2

Gergely Cserdi y Balazs Sandor Skublics, Amazon Web Services

Resumen

Este patrón explica los pasos y las consideraciones para actualizar un clúster de SAP Pacemaker basado en Standalone Enqueue Server () a. ENSA1 ENSA2 La información de este patrón se aplica a los sistemas operativos SUSE Linux Enterprise Server (SLES) y Red Hat Enterprise Linux (RHEL).

Los clústeres Pacemaker de SAP NetWeaver 7.52 o S/4HANA 1709 y versiones anteriores se ejecutan en una arquitectura y están configurados específicamente para ello. ENSA1 ENSA1 Si ejecuta sus cargas de trabajo de SAP en Amazon Web Services (AWS) y está interesado en pasarse a ellos ENSA2, es posible que la documentación de SAP, SUSE y RHEL no proporcione información completa. Este patrón describe los pasos técnicos necesarios para reconfigurar los parámetros de SAP y los clústeres de Pacemaker desde los que realizar la actualización. ENSA1 ENSA2 Proporciona ejemplos de sistemas SUSE, pero el concepto es el mismo para los clústeres RHEL.

> **Note**
>
> ENSA1 y ENSA2 son conceptos que se refieren únicamente a las aplicaciones de SAP, por lo que la información de este patrón no se aplica a SAP HANA ni a otros tipos de clústeres.

> **Note**
>
> Técnicamente, se ENSA2 puede utilizar con o sin Enqueue Replicator 2. Sin embargo, la alta disponibilidad (HA) y la automatización de la conmutación por error (mediante una solución de clúster) requieren Enqueue Replicator 2. Este patrón utiliza el término ENSA2 clústeres para referirse a los clústeres con Enqueue Server 2 y Enqueue Replicator 2 independientes.

Requisitos previos y limitaciones

Requisitos previos

- Clúster funcional que utiliza Pacemaker y Corosync ENSA1 en SLES o RHEL.

- Al menos dos instancias de Amazon Elastic Compute Cloud (Amazon EC2) en las que se estén ejecutando las instancias (ABAP) de SAP Central Services (ASCS/SCS) y Enqueue Replication Server (ERS).
- Conocimientos sobre la gestión de clústeres y aplicaciones de SAP.
- Acceso al entorno Linux como usuario raíz.

Limitaciones

- ENSA1los clústeres basados solo admiten una arquitectura de dos nodos.
- ENSA2los clústeres basados en SAP no se pueden implementar en NetWeaver versiones de SAP anteriores a la 7.52.
- EC2 las instancias de los clústeres deben estar en distintas zonas de disponibilidad de AWS.

Versiones de producto

- SAP NetWeaver versión 7.52 o posterior
- A partir de S/4HANA 2020, solo ENSA2 se admiten clústeres
- Kernel 7.53 o posterior, que admite Enqueue Replicator ENSA2 2
- SLES para aplicaciones SAP, versión 12 o posterior
- RHEL para SAP con alta disponibilidad (HA) versión 7.9 o posterior

Arquitectura

Pila de tecnología de origen

- SAP NetWeaver 7.52 con SAP Kernel 7.53 o posterior
- Sistema operativo SLES o RHEL

Pila de tecnología de destino

- SAP NetWeaver 7.52 con SAP Kernel 7.53 o posterior, incluido S/4HANA 2020 con plataforma ABAP
- Sistema operativo SLES o RHEL

Arquitectura de destino

El siguiente diagrama muestra una configuración de alta disponibilidad de ASCS/SCS instancias ERS basadas en un clúster. ENSA2

Comparación de ENSA2 clústeres ENSA1 y clústeres

Se presenta SAP ENSA2 como el sucesor de ENSA1. Un clúster ENSA1 basado admite una arquitectura de dos nodos en la que la ASCS/SCS instancia se conmuta por error al ERS cuando se produce un error. Esta limitación se debe a la forma en que la ASCS/SCS instancia recupera la información de la tabla de bloqueo de la memoria compartida del nodo ERS tras la conmutación por error. ENSA2Los clústeres basados en Enqueue Replicator 2 eliminan esta limitación, ya que la ASCS/SCS instancia puede recopilar la información de bloqueo de la instancia ERS a través de la red. ENSA2Los clústeres basados pueden tener más de dos nodos, ya que la ASCS/SCS instancia ya no es necesaria para realizar la conmutación por error al nodo ERS. (Sin embargo, en un entorno de ENSA2 clúster de dos nodos, la ASCS/SCS instancia seguirá realizando la conmutación por error al nodo ERS porque no hay otros nodos en el clúster a los que realizar la conmutación por error). ENSA2 se admite a partir del kernel 7.50 de SAP con algunas limitaciones. Para una configuración de alta disponibilidad compatible con Enqueue Replicator 2, el requisito mínimo es de NetWeaver 7.52 (consulte la nota 2630416 de SAP OSS). El S/4HANA 1809 viene con la ENSA2 arquitectura recomendada de forma predeterminada, mientras que S/4HANA solo es compatible a partir de la versión 2020. ENSA2

Automatizar y escalar

El clúster de alta disponibilidad de la arquitectura de destino hace que el ASCS realice automáticamente la conmutación por error a otros nodos.

Escenarios para pasar a clústeres basados en clústeres ENSA2

Existen dos escenarios principales para la actualización a clústeres ENSA2 basados:

- Escenario 1: elige realizar la actualización a SAP ENSA2 sin necesidad de realizar una actualización de SAP o una conversión a S/4HANA, suponiendo que su versión de SAP y su versión de kernel sean compatibles. ENSA2
- Escenario 2: ENSA2 como parte de una actualización o conversión (por ejemplo, a S/4HANA 1809 o posterior), utiliza SUM.

La sección Epics describe los pasos para estos dos escenarios. El primer escenario requiere que configure manualmente los parámetros relacionados con SAP antes de cambiar la configuración del clúster. ENSA2 En el segundo escenario, SUM implementa los binarios y los parámetros relacionados con SAP, y la única tarea restante es actualizar la configuración del clúster para HA. Aun así, le recomendamos que valide los parámetros de SAP después de usar SUM. En la mayoría de los casos, la conversión a S/4HANA es el motivo principal de la actualización de un clúster.

Tools (Herramientas)

- Para los administradores de paquetes de sistemas operativos, recomendamos las herramientas Zypper (para SLES) o YUM (para RHEL).
- Para la administración de clústeres, recomendamos los servidores crm (para SLES) o pcs (para RHEL).
- Herramientas de administración de instancias de SAP, como SAPControl.
- (Opcional) Herramienta SUM para la actualización de conversión a S/4HANA.

Prácticas recomendadas

- Para conocer las prácticas recomendadas sobre el uso de cargas de trabajo de SAP en AWS, consulte SAP Lens para el Marco de AWS Well-Architected
- Tenga en cuenta la cantidad de nodos del clúster (pares o impares) en su arquitectura de ENSA2 varios nodos.
- Configure el ENSA2 clúster para el SLES 15 de acuerdo con el estándar de certificación SAP S/4-HA-CLU 1.0.
- Guarde o haga una copia de seguridad del estado actual del clúster y de la aplicación antes de realizar la actualización a ellos. ENSA2

Epics

Configure los parámetros de SAP manualmente para ENSA2 (solo en el escenario 1)

Tarea	Descripción	Habilidades requeridas
Configure los parámetros en el perfil predeterminado.	Si desea actualizar a la misma versión de SAP ENSA2 mientras utiliza la misma	SAP

Tarea	Descripción	Habilidades requeridas

	versión o si la versión de destino es la predeterminada ENSA1, defina los parámetros del perfil predeterminado (archivo DEFAULT.PFL) en los siguientes valores.
	
	`enq/enable=TRUE`
	`enq/serverhost=sapascsvirt`
	`enq/serverinst=10`
	`(instance number of ASCS/SCS instance)`
	`enque/process_location=REMOTESA`
	`enq/replicatorhost=sapersvirt`
	`enq/replicatorinst=11`
	`(instance number of ERS instance)`
	
	donde `sapascsvirt` es el nombre de host virtual de las instancias de ASCS y es `sapersvirt` el nombre de host virtual de las instancias de ERS. Puede cambiarlos para adaptarlos a su entorno de destino.
	
	Note
	Para utilizar esta opción de actualización, la versión de SAP y la versión	

Tarea	Descripción	Habilidades requeridas
	del núcleo deben ser compatibles ENSA2 con Enqueue Replicator 2.	

Tarea	Descripción	Habilidades requeridas
Configure el perfil de la instancia ASCS/SCS .	Si desea actualizar a la misma versión de SAP sin ENSA2 dejar de utilizar o si la versión de destino es la predeterm inada ENSA1, defina los siguientes parámetros en el perfil de la ASCS/SCS instancia. La sección del perfil en la que ENSA1 se define tiene un aspecto similar al siguiente. `#------------------ ------------------ ------------------ --------- Start SAP enqueue server #------------------ ------------------ ------------------ ------- _EN = en.sap$(S APSYSTEMNAME)$(INS TANCE_NAME) Execute_04 = local rm - f $(_EN) Execute_05 = local ln - s -f $(DIR_EXECUTABLE)/ enserver$(FT_EXE) $(_EN) Start_Program_01 = local $(_EN) pf=$(_PF)` Para reconfigurar esta sección para ENSA2:	SAP

Tarea	Descripción	Habilidades requeridas

	1. Cambie el prefijo del programa _EN para que _ENQ se base en la información más reciente de SAP (OSS Note 2501860; requiere una cuenta de usuario de SAP ONE Support Launchpad).
	2. Cambie el binario para el servidor de puesta en cola de `enserver` a `enq_server` .
	3. Defina el parámetro `enq/server/replication/enable` como `TRUE`.
	4. Asegúrese de que `Autostart = 0`.
	
	Esta sección de perfil tendrá un aspecto similar al siguiente después de los cambios.
	
	`#------------------------------------------------------------`
	`Start SAP enqueue server`
	`#------------------------------------------------------------`
	`_ENQ = enq.sap$(SAPSYSTEMNAME)$(INSTANCE_NAME)`	

Tarea	Descripción	Habilidades requeridas

	`Execute_04 = local rm -f $(_ENQ)`
	`Execute_05 = local ln -s -f $(DIR_EXECUTABLE)/enq_server$(FT_EXE) $(_ENQ)`
	`Start_Program_01 = local $(_ENQ) pf=$(_PF)`
	`...`
	`enq/server/replication/enable = TRUE`
	`Autostart = 0`
	
	Important
	_ENQ no debe tener habilitada la opción de reinicio. Si `RestartProgram_01` está configurada para _ENQ, cámbiela a `StartProgram_01`. Esto evita que SAP reinicie el servicio o interfiera con los recursos gestionados por el clúster.	

Tarea	Descripción	Habilidades requeridas
Configurar el perfil ERS.	Si desea actualizar a la misma versión de SAP ENSA2 mientras utiliza la misma versión de SAP o si la versión de destino es la predeterm inada ENSA1, defina los siguientes parámetros en el perfil de la instancia de ERS. Busque la sección en la que está definido el replicador de puesta en cola. Será similar al siguiente. `#------------------ ------------------ ------------------- Start enqueue replicati on server #------------------- ------------------ ------------------ _ER = er.sap$(S APSYSTEMNAME)$(INS TANCE_NAME) Execute_03 = local rm - f $(_ER) Execute_04 = local ln - s -f $(DIR_EXECUTABLE)/ enrepserver$(FT_EXE) $(_ER) Start_Program_00 = local $(_ER) pf=$(_PF) NR=$(SCSID)`	SAP

Tarea	Descripción	Habilidades requeridas
	Para volver a configurar esta sección para el replicador de puesta en cola 2: 1. Cambie el prefijo del `_ER` programa para que `_ENQR` se base en las últimas notas de SAP (OSS Note 2501860; requiere una SAP ONE Support Launchpad user account). 2. Cambie el binario del replicador de colas a en lugar de `enq_replicator` a `enrepserver` . 3. Asegúrese de que `Autostart = 0`. Esta sección de perfil tendrá un aspecto similar al siguiente después de los cambios. `#------------------ ------------------ ------------------ Start enqueue replicati on server #------------------ ------------------ ------------------ _ENQR = enqr.sap$ (SAPSYSTEMNAME)$(I NSTANCE_NAME) Execute_01 = local rm - f $(_ENQR) Execute_02 = local ln - s -f $(DIR_EXECUTABLE)/`	

Tarea	Descripción	Habilidades requeridas

	`enq_replicator$(FT _EXE) $(_ENQR)`
	`Start_Program_00 =  local $(_ENQR) pf= $(_PF) NR=$(SCSID)`
	`…`
	`Autostart = 0`
	
	Important
	_ENQR no debe tener habilitada la opción de reinicio. Si `RestartProgram_01` está configurada para _ENQR, cámbiela a `StartProgram_01` . Esto evita que SAP reinicie el servicio o interfiera con los servicios gestionados por clústeres.	

Tarea	Descripción	Habilidades requeridas

Reinicie SAP Start Services.	Tras cambiar los perfiles descritos anteriormente en esta epopeya, reinicie SAP Start Services tanto para ERS como para ASCS/SCS él.
	
	`sapcontrol -nr 10 -function RestartService SCT`
	
	`sapcontrol -nr 11 -function RestartService SCT`
	
	donde `SCT` se refiere al ID del sistema SAP y suponiendo que 10 y 11 son los números de instancia de ASCS/SCS las instancias ERS, respectivamente.
		SAP

Reconfigure el clúster para ENSA2 (obligatorio en ambos escenarios)

Tarea	Descripción	Habilidades requeridas
Verifique los números de versión en los agentes de recursos de SAP.	Cuando utiliza SUM para actualizar SAP a S/4HANA 1809 o posterior, SUM gestiona los cambios de parámetros en los perfiles de SAP. Solo el clúster requiere un ajuste manual. Sin embargo, le recomendamos que compruebe la configuración de los parámetros antes	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	de realizar cualquier cambio en el clúster. **Note** En los ejemplos de esta epic, se supone que está utilizando el sistema operativo SUSE. Si está utilizando RHEL, necesitará utilizar herramientas como YUM y pcs shell en lugar de Zypper y crm. Compruebe ambos nodos de la arquitectura para confirmar que el paquete de `resource-agents` coincide con la versión mínima recomenda da por SAP. Para el SLES, consulte la nota 2641019 de SAP OSS. Para RHEL, consulte la nota 2641322 de SAP OSS. (SAP Notes requiere una cuenta de usuario de SAP ONE Support Launchpad). `sapers:sctadm 23> zypper search -s -i resource-agents Loading repository data...`	

Tarea	Descripción	Habilidades requeridas

	`Reading installed packages...`
	`S | Name | Type | Version | Arch | Repository`
	`--+-------------+---------+-----------------+---------------+------+-----------+-----------------`
	`i | resource-agents | package | 4.8.0+git30.d0077df0-150300.8.28.1 | x86_64 | SLE-Product-HA15-SP3-Updates`
	
	Actualice la versión `resource-agents` si es necesario.	

Realice una copia de seguridad de la configuración del clúster.	Realice una copia de seguridad de la configuración del clúster de CRM de la siguiente manera. `crm configure show > /tmp/cluster_config_backup.txt`	Administrador de sistemas de AWS
Establezca el modo de mantenimiento.	Configure el clúster en modo de mantenimiento. `crm configure property maintenance-mode="true"`	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas

Compruebe la configuración del clúster.	Compruebe la configuración actual del clúster.
	
	`crm configure show`
	
	He aquí un extracto del resultado completo:
	
	`node 1: sapascs`
	`node 2: sapers`
	`...`
	`primitive rsc_sap_S`
	`CT_ASCS10 SAPInstance`
	` \`
	`operations $id=rsc_s`
	`ap_SCT_ASCS10-oper`
	`ations \`
	`op monitor interval=120`
	` timeout=60 on-fail=r`
	`estart \`
	`params InstanceN`
	`ame=SCT_ASCS10_sap`
	`ascsvirt START_PRO`
	`FILE="/sapmnt/SCT/`
	`profile/SCT_ASCS10`
	`_sapascsvirt" \`
	`  AUTOMATIC_RECOVER=`
	`false \`
	`meta resource-stickines`
	`s=5000 failure-t`
	`imeout=60 migration-`
	`threshold=1 priority=`
	`10`
	`primitive rsc_sap_S`
	`CT_ERS11 SAPInstance \`
	`operations $id=rsc_s`
	`ap_SCT_ERS11-opera`
	`tions \`
	`op monitor interval=120`
	` timeout=60 on-fail=r`
	`estart \`
		Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	`params InstanceN ame=SCT_ERS11_sape rsvirt START_PRO FILE="/sapmnt/SCT/ profile/SCT_ERS11_ sapersvirt" \ AUTOMATIC_RECOVER= false IS_ERS=true \ meta priority=1000 ... colocation col_sap_S CT_no_both -5000: grp_SCT_ERS11 grp_SCT_ASCS10 location loc_sap_S CT_failover_to_ers rsc_sap_SCT_ASCS10 \ rule 2000: runs_ers_SCT eq 1 order ord_sap_S CT_first_start_asc s Optional: rsc_sap_S CT_ASCS10:start rsc_sap_SCT_ERS11: stop symmetrical=false ...`  donde `sapascsvirt` se refiere al nombre de host virtual de las instancias de ASCS, `sapersvirt` se refiere al nombre de host virtual de las instancias de ERS y SCT se refiere al ID del sistema SAP.	

Tarea	Descripción	Habilidades requeridas
Elimine la restricción de colocación de la conmutación por error.	En el ejemplo anterior, la restricción de ubicación `loc_sap_SCT_failover_to_ers` especifica que la ENSA1 función de ASCS siempre debe seguir la instancia del ERS en caso de conmutación por error. Con ENSA2, ASCS debería poder realizar la conmutación por error libremente a todos los nodos participantes, de modo que pueda eliminar esta restricción. `crm configure delete loc_sap_SCT_failover_to_ers`	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas

Ajuste las primitivas.	También necesitará realizar cambios menores en las primitivas de ASCS y ERS. SAPInstance
	
	A continuación, se muestra un ejemplo de una SAPInstance primitiva de ASCS que está configurada para. ENSA1
	
	`primitive rsc_sap_SCT_ASCS10 SAPInstance \`
	`operations $id=rsc_sap_SCT_ASCS10-operations \`
	`op monitor interval=120 timeout=60 on-fail=restart \`
	`params InstanceName=SCT_ASCS10_sapascsvirt START_PROFILE="/sapmnt/SCT/profile/SCT_ASCS10_sapascsvirt" \`
	`AUTOMATIC_RECOVER=false \`
	`meta resource-stickiness=5000 failure-timeout=60 migration-threshold=1 priority=10`
	
	Para actualizar a ENSA2, cambie esta configuración por la siguiente.
		Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	`primitive rsc_sap_S CT_ASCS10 SAPInstance \ operations $id=rsc_s ap_SCT_ASCS10-oper ations \ op monitor interval=120 timeout=60 on-fail=r estart \ params InstanceN ame=SCT_ASCS10_sap ascsvirt START_PRO FILE="/sapmnt/SCT/ profile/SCT_ASCS10 _sapascsvirt" \ AUTOMATIC_RECOVER= false \ meta resource-stickines s=3000`  Este es un ejemplo de una SAPInstance primitiva ERS configurada para ENSA1.  `primitive rsc_sap_S CT_ERS11 SAPInstance \ operations $id=rsc_s ap_SCT_ERS11-opera tions \ op monitor interval=120 timeout=60 on-fail=r estart \ params InstanceN ame=SCT_ERS11_sape rsvirt START_PRO FILE="/sapmnt/SCT/ profile/SCT_ERS11_ sapersvirt" \ AUTOMATIC_RECOVER= false IS_ERS=true \`	

Tarea	Descripción	Habilidades requeridas

	`meta priority=1000`
	
	Para realizar la actualización a ENSA2, cambie esta configuración por la siguiente.
	
	`primitive rsc_sap_SCT_ERS11 SAPInstance \ operations $id=rsc_sap_SCT_ERS11-operations \ op monitor interval=120 timeout=60 on-fail=restart \ params InstanceName=SCT_ERS11_sapersvirt START_PROFILE="/sapmnt/SCT/profile/SCT_ERS11_sapersvirt" \ AUTOMATIC_RECOVER=false IS_ERS=true`
	
	Puede cambiar las primitivas de varias formas. Por ejemplo, puede revisarlas en un editor como vi, como se muestra en el siguiente ejemplo.
	
	`crm configure edit rsc_sap_SCT_ERS11`	

Tarea	Descripción	Habilidades requeridas
Deshabilitar el modo de mantenimiento.	Deshabilitar el modo de mantenimiento en el clúster. `crm configure property maintenance-mode="false"` Cuando el clúster está fuera del modo de mantenimiento, intenta poner en línea las instancias de ASCS y ERS con la nueva ENSA2 configuración.	Administrador de sistemas de AWS

(Opcional) Añada nodos de clúster

Tarea	Descripción	Habilidades requeridas
Consulte las prácticas recomendadas.	Antes de añadir más nodos, asegúrese de comprender las prácticas recomendadas, como por ejemplo si debe utilizar un número par o impar de nodos.	Administrador de sistemas de AWS
Añada nodos.	Añadir más nodos implica una serie de tareas, como actualizar el sistema operativo, instalar paquetes de software que coincidan con los nodos existentes y hacer que los montajes estén disponibles. Puede utilizar la opción Preparación de un host adicional en el Administr	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	ador de aprovisionamiento de software de SAP (SWPM) para crear una línea base del host específica para SAP. Para obtener más información, consulte las guías de SAP que se muestran en la siguiente sección.	

Recursos relacionados

Referencias de SAP y SUSE

Para acceder a SAP Notes, debe tener una cuenta de usuario de SAP ONE Support Launchpad. Para obtener más información, consulte el sitio web de soporte de SAP.

- SAP Note 2501860 – Documentación del servidor de NetWeaver aplicaciones SAP para ABAP 7.52
- SAP Note 2641019 – Instalación ENSA2 y actualización desde o en un entorno de alta disponibilidad de SUSE ENSA1 ENSA2
- SAP Note 2641322 – Instalación ENSA2 y actualización desde y ENSA2 cuando se utilizan las soluciones HA de Red Hat ENSA1 para SAP
- Nota de SAP 2711036: Uso del servidor Enqueue 2 independiente en un entorno de alta disponibilidad
- Servidor Enqueue 2 independiente (documentación de SAP)
- SAP S/4 HANA: Clúster de alta disponibilidad de Enqueue Replication 2: guía de configuración (documentación de SUSE)

Referencias de AWS

- SAP HANA en AWS: guía de configuración de alta disponibilidad para SLES y RHEL
- SAP Lens: Marco de AWS Well-Architected

Utilice zonas de disponibilidad coherentes en VPCs diferentes cuentas de AWS

Adam Spicer, Amazon Web Services

Resumen

En la nube de Amazon Web Services (AWS), una zona de disponibilidad tiene un nombre que puede variar entre sus cuentas de AWS y un Identificador de zona de disponibilidad (AZ ID) que identifica su ubicación. Si utiliza AWS CloudFormation para crear nubes privadas virtuales (VPCs), debe especificar el nombre o el ID de la zona de disponibilidad al crear las subredes. Si crea VPCs en varias cuentas, el nombre de la zona de disponibilidad es aleatorio, lo que significa que las subredes utilizan distintas zonas de disponibilidad en cada cuenta.

Para usar la misma zona de disponibilidad en todas sus cuentas, debe asignar el nombre de la zona de disponibilidad de cada cuenta al mismo Identificador de zona de disponibilidad. Por ejemplo, en el siguiente diagrama se muestra que el Identificador AZ de `use1-az6` se llama `us-east-1a` en la cuenta A de AWS y `us-east-1c` en la cuenta Z de AWS.

Este patrón ayuda a garantizar la coherencia zonal al proporcionar una solución escalable y multicuenta para utilizar las mismas zonas de disponibilidad en sus subredes. La coherencia zonal garantiza que el tráfico de red entre cuentas evite las rutas de red entre zonas de disponibilidad, lo que ayuda a reducir los costos de transferencia de datos y a reducir la latencia de red entre las cargas de trabajo.

Este patrón es un enfoque alternativo a la CloudFormation AvailabilityZoneId propiedad de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Al menos dos cuentas de AWS activas en la misma región de AWS.
- Evalúe cuántas zonas de disponibilidad se necesitan para cumplir con los requisitos de VPC en la región.
- Identifique y registre el Identificador de zona de disponibilidad para cada zona de disponibilidad que necesite admitir. Para obtener más información al respecto, consulte Availability Zone IDs para sus recursos de AWS en la documentación de AWS Resource Access Manager.

- Una lista ordenada y separada por comas de su zona de disponibilidad. IDs Por ejemplo, la primera zona de disponibilidad de la lista se mapea como `az1`, la segunda zona de disponibilidad se mapea como `az2` y esta estructura de mapeo continúa hasta que la lista separada por comas esté completamente mapeada. No hay un número máximo de AZ IDs que se puedan mapear.
- El `az-mapping.yaml` archivo del repositorio de mapeo de zonas de disponibilidad de GitHub múltiples cuentas, copiado en su máquina local

Arquitectura

El siguiente diagrama muestra la arquitectura que se implementa en una cuenta y que crea los valores de Almacén de parámetros de AWS Systems Manager. Estos valores del almacén de parámetros se consumen al crear una VPC en la cuenta.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. La solución de este patrón se implementa en todas las cuentas que requieren coherencia zonal para una VPC.
2. La solución crea valores de almacén de parámetros para cada Identificador de zona de disponibilidad y almacena el nombre de la nueva zona de disponibilidad.
3. La CloudFormation plantilla de AWS utiliza el nombre de la zona de disponibilidad almacenado en cada valor del almacén de parámetros, lo que garantiza la coherencia zonal.

En el siguiente diagrama, se muestra el flujo de trabajo para crear una VPC con la solución de este patrón.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Envíe una plantilla para crear una VPC a AWS. CloudFormation
2. AWS CloudFormation resuelve los valores del almacén de parámetros de cada zona de disponibilidad y devuelve el nombre de la zona de disponibilidad de cada ID de zona de disponibilidad.
3. Se crea una VPC con la AZ correcta IDs necesaria para garantizar la coherencia zonal.

Tras implementar la solución de este patrón, puede crear subredes que hagan referencia a los valores del almacén de parámetros. Si usa AWS CloudFormation, puede hacer referencia a los valores de los parámetros de mapeo de zonas de disponibilidad del siguiente código de ejemplo con formato YAML:

```
Resources:
    PrivateSubnet1AZ1:
        Type: AWS::EC2::Subnet
        Properties:
            VpcId: !Ref VPC
            CidrBlock: !Ref PrivateSubnetAZ1CIDR
            AvailabilityZone:
                !Join
                    - ''
                    - - '{{resolve:ssm:/az-mapping/az1:1}}'
```

Este código de muestra se incluye en el `vpc-example.yaml` archivo del repositorio de mapeo de zonas de disponibilidad de GitHub varias cuentas. Le muestra cómo crear una VPC y subredes que se alineen con los valores del almacén de parámetros para garantizar la coherencia zonal.

Pila de tecnología

- AWS CloudFormation
- AWS Lambda
- Almacén de parámetros de AWS Systems Manager

Automatización y escala

Puede implementar este patrón en todas sus cuentas de AWS mediante AWS CloudFormation StackSets o la solución Customizations for AWS Control Tower. Para obtener más información, consulte Trabajar con AWS CloudFormation StackSets en la documentación de AWS Cloudformation y Personalizaciones para la Torre de Control de AWS en la biblioteca de soluciones de AWS.

Después de implementar la CloudFormation plantilla de AWS, puede actualizarla para usar los valores del almacén de parámetros e implementarla VPCs en canalizaciones o según sus requisitos.

Tools (Herramientas)

Servicios de AWS

- AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Puede administrar y aprovisionar pilas en varias cuentas y regiones de AWS.
- AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.
- Almacén de parámetros de AWS Systems Manager es una funcionalidad de AWS Systems Manager. Proporciona un almacenamiento seguro y jerárquico para administrar los datos de configuración y los secretos.

Código

El código de este patrón se proporciona en el repositorio de mapeo de zonas de disponibilidad de GitHub múltiples cuentas.

Epics

Implemente el archivo az-mapping.yaml

Tarea	Descripción	Habilidades requeridas
Determine las zonas de disponibilidad requeridas para la región.	1. Determine la zona de IDs disponibilidad que debe utilizarse de forma coherente en su región. 2. Registre estas AZ IDs en una lista separada por comas y en el orden en que desee aplicarlas. Por ejemplo, la primera zona de disponibilidad de la lista se mapea como `az1` y la	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	segunda se mapea como `az2`. No hay un número máximo de AZ IDs que se puedan mapear.	
Implemente el archivo az-mapping.yaml.	Utilice el `az-mapping.yaml` archivo para crear una CloudFormation pila de AWS en todas las cuentas de AWS necesarias. En el parámetro `AZIds`, utilice la lista separada por comas que creó anteriorm ente. Le recomendamos que utilice AWS CloudFormation StackSets o la solución Customizations for AWS Control Tower.	Arquitecto de la nube

Impleméntelo VPCs en sus cuentas

Tarea	Descripción	Habilidades requeridas
Personalice las CloudForm ation plantillas de AWS.	Cuando cree las subredes con AWS CloudFormation, personalice las plantillas para que usen los valores del almacén de parámetros que creó anteriormente. Para ver una plantilla de ejemplo, consulte el `vpc-example.yaml` archivo en el repositorio de mapeo de	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	zonas de disponibilidad de GitHub múltiples cuentas.	
Implemente el VPCs.	Implemente las CloudForm ation plantillas de AWS personalizadas en sus cuentas. Por lo tanto, cada VPC de la región tiene coherencia zonal en las zonas de disponibilidad utilizadas para las subredes	Arquitecto de la nube

Recursos relacionados

- Zona de disponibilidad IDs para sus recursos de AWS (documentación de AWS Resource Access Manager)
- AWS::EC2::Subnet(CloudFormation documentación de AWS)

Utilice el usuario IDs en las políticas de IAM para el control de acceso y la automatización

Srinivas Ananda Babu y Ram Kandaswamy, Amazon Web Services

Resumen

Este patrón explica los posibles inconvenientes de usar políticas basadas en nombres de usuario en AWS Identity and Access Management la IAM, las ventajas de usar políticas basadas en el nombre de usuario y cómo integrar este IDs enfoque para la automatización. AWS CloudFormation

En él Nube de AWS, el servicio de IAM le ayuda a gestionar las identidades de los usuarios y el control de acceso con precisión. Sin embargo, confiar en los nombres de usuario al crear las políticas de IAM puede provocar riesgos de seguridad imprevistos y problemas de control de acceso. Por ejemplo, considere este escenario: un empleado nuevo, John Doe, se une a su equipo y usted crea una cuenta de usuario de IAM con el nombre de usuario `j.doe`, lo que le concede permisos a través de las políticas de IAM que hacen referencia a los nombres de usuario. Cuando John deja la empresa, se elimina la cuenta. El problema comienza cuando una empleada nueva, Jane Doe, se une al equipo y se vuelve a crear el nombre de usuario `j.doe`. Las políticas existentes ahora conceden a Jane Doe los mismos permisos que a John Doe. Esto crea una pesadilla en materia de seguridad y cumplimiento.

La actualización manual de cada política para reflejar los detalles de los usuarios nuevos es un proceso lento y propenso a errores, especialmente a medida que la organización crece. La solución consiste en utilizar un ID de usuario único e inmutable. Al crear una cuenta de usuario de IAM, AWS asigna al usuario de IAM un ID de usuario único (o ID principal). Puede utilizar estos usuarios IDs en sus políticas de IAM para garantizar un control de acceso coherente y fiable que no se vea afectado por los cambios o la reutilización del nombre de usuario.

Por ejemplo, una política de IAM que utiliza un ID de usuario podría tener un aspecto similar al siguiente:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::example-bucket",
```

```
            "Principal": { "AWS": "arn:aws:iam::123456789012:user/abcdef01234567890" }
        }
      ]
}
```

Entre las ventajas de utilizar el usuario IDs en las políticas de IAM se incluyen las siguientes:

- Unicidad. IDs Los usuarios son únicos en todos los ámbitos Cuentas de AWS, por lo que proporcionan una solicitud de permisos correcta y coherente.
- Inmutabilidad. El usuario IDs no se puede cambiar, por lo que proporciona un identificador estable para hacer referencia a los usuarios en las políticas.
- Auditoría y conformidad. Servicios de AWS suelen incluir al usuario IDs en los registros y registros de auditoría, lo que facilita el seguimiento de las acciones hasta usuarios específicos.
- Automatización e integración. El uso de scripts IDs de AWS APIs automatización o de entrada de usuario garantiza que los procesos no se vean afectados por los cambios de nombre de usuario. SDKs
- Preparación para el futuro. Utilizar el usuario IDs en las políticas desde el principio puede evitar posibles problemas de control de acceso o actualizaciones exhaustivas de las políticas.

Automatización

Cuando se utilizan herramientas de infraestructura como código (IaC) AWS CloudFormation, las dificultades de las políticas de IAM basadas en nombres de usuario pueden seguir causando problemas. El recurso de usuario de IAM devuelve el nombre de usuario cuando se llama a la función intrínseca `Ref`. A medida que la infraestructura de su organización evoluciona, el ciclo de creación y eliminación de recursos, tal como las cuentas de usuario de IAM, puede provocar problemas de control de acceso no deseados si se reutilizan los nombres de usuario.

Para solucionar este problema, te recomendamos que incorpores el usuario en tus plantillas. IDs CloudFormation Sin embargo, obtener IDs un usuario para este propósito puede resultar difícil. Aquí es donde los recursos personalizados pueden resultar útiles. Puede utilizar recursos CloudFormation personalizados para ampliar la funcionalidad del servicio mediante la integración con servicios externos AWS APIs o con otros. Al crear un recurso personalizado que obtenga el ID de usuario de un usuario de IAM determinado, puede hacer que el ID de usuario esté disponible en sus CloudFormation plantillas. Este enfoque agiliza el proceso de referencia al usuario IDs y garantiza que sus flujos de trabajo de automatización sigan siendo sólidos y estén preparados para el futuro.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Una función de IAM para que un administrador de la nube ejecute la plantilla CloudFormation

Limitaciones

- Algunas Servicios de AWS no están disponibles en todas Regiones de AWS. Para conocer la disponibilidad de las regiones, consulte Servicios de AWS by Region. Para los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

Arquitectura de destino

En el siguiente diagrama se muestra cómo se CloudFormation utiliza un recurso personalizado respaldado por AWS Lambda para recuperar el ID de usuario de IAM.

Automatización y escala

Puedes usar la CloudFormation plantilla varias veces para diferentes Regiones de AWS cuentas. Debe ejecutarla solo una vez en cada región o cuenta.

Tools (Herramientas)

Servicios de AWS

- IAM: AWS Identity and Access Management (IAM) es un servicio web que le ayuda a controlar de forma segura el acceso a los AWS recursos. Utilice IAM para controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos.
- AWS CloudFormation— le AWS CloudFormation ayuda a modelar y configurar sus AWS recursos para que pueda dedicar menos tiempo a gestionarlos y más tiempo a centrarse en las aplicaciones en las que se ejecutan. AWS Crea una plantilla que describe los AWS recursos que desea y CloudFormation se encarga de aprovisionar y configurar esos recursos por usted.

- AWS Lambda— AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.

Prácticas recomendadas

Si está empezando desde cero o tiene prevista una implementación totalmente nueva, le recomendamos que utilice AWS IAM Identity Center para la administración centralizada de usuarios. El Centro de Identidad de IAM se integra con sus proveedores de identidad existentes (como Active Directory u Okta) para federar las identidades de los usuarios AWS, lo que elimina la necesidad de crear y administrar los usuarios de IAM directamente. Este enfoque no solo garantiza un control de acceso uniforme, sino que también simplifica la administración del ciclo de vida de los usuarios y ayuda a mejorar la seguridad y el cumplimiento en todo el entorno. AWS

Epics

Validación de permisos

Tarea	Descripción	Habilidades requeridas
Valide su función Cuenta de AWS y la de IAM.	Confirme que tiene un rol de IAM con permisos para implementar CloudFormation plantillas en su. Cuenta de AWS Si piensa utilizar la consola AWS CLI en lugar de la CloudFormation consola para implementar la plantilla en el último paso de este procedimiento, también debe configurar credenciales temporales para ejecutar AWS CLI comandos. Para obtener instrucciones, consulte la documentación de IAM.	Arquitecto de la nube

Cree una CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Crea una CloudFormation plantilla.	1. Cree una CloudFormation plantilla siguiendo las instrucciones de la CloudFormation documentación. Puede utilizar el formato JSON o YAML. Este patrón supone que utiliza el formato YAML. 2. Guarde la plantilla con el nombre `get_unique_user_id.yaml` .	AWS DevOps, arquitecto de nube

Agregue un parámetro de entrada para el nombre de usuario.	Añada el siguiente código a la `Parameters` sección de la CloudFormation plantilla:
	`Parameters:`
	`  NewIamUserName:`
	`  Type: String`
	`  Description: Unique username for the new IAM user`
	Este parámetro solicita al usuario el nombre de usuario.
		AWS DevOps, arquitecto de nube

Agregue un recurso personalizado para crear un usuario de IAM.	Añada el siguiente código a la `Resources` sección de la CloudFormation plantilla:
	`Resources:`
	`  rNewIamUser:`
	`  Type: 'AWS::IAM::User'`
	`  Properties:`
		AWS DevOps, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	`UserName: !Ref NewIamUserName` Este código añade un CloudFormation recurso que crea un usuario de IAM con el nombre proporcionado por el `NewIamUserName` parámetro.	
Agregue un rol de ejecución para la función de Lambda.	En este paso, crea un rol de IAM que otorga un permiso a una AWS Lambda función para obtener el `UserId` IAM. Especifique los siguientes permisos mínimos necesarios para que Lambda se ejecute: • `logs:CreateLogStream` • `logs:PutLogEvents` • `CreateLogGroup` • `iam:GetUser` • `AssumeRole` para `lambda.amazonaws.com` Para obtener instrucciones sobre cómo crear un rol de ejecución, consulte la documentación de Lambda. Hará referencia a este rol en el paso siguiente, cuando cree la función de Lambda.	Administrador de AWS, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas

Agregue una función de Lambda para obtener el `UserId` de IAM único.	En este paso, se define una función de Lambda con un tiempo de ejecución de Python para obtener el `UserId` de IAM único. Para ello, añada el siguiente código a la `Resources` sección de la CloudFormation plantilla. Sustituya `<<ROLENAME>>` por el nombre del rol de ejecución que creó en el paso anterior.
	
	`GetUserLambdaFunction:`
	`Type: 'AWS::Lambda::Function'`
	`Properties:`
	`Handler: index.handler`
	`Role: <<ROLENAME>>`
	`Timeout: 30`
	`Runtime: python3.11`
	`Code:`
	`ZipFile: |`
	`import cfnresponse, boto3`
	`def handler(event, context):`
	`try:`
	`print(event)`
	`user = boto3.client('iam').get_user(UserName=event['ResourceP`
		AWS DevOps, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	roperties']['NewIa mUserName'])['User'] cfnrespon se.send(event, context, cfnrespon se.SUCCESS, {'NewIamU serId': user['Use rId'], 'NewIamUs erPath': user['Pat h'], 'NewIamUserArn': user['Arn']}) except Exception as e: cfnrespon se.send(event, context, cfnrespon se.FAILED, {'NewIamU ser': str(e)})	

Tarea	Descripción	Habilidades requeridas

Agregue un recurso personalizado.	Añada el siguiente código a la `Resources` sección de la CloudFormation plantilla:
	
	`rCustomGetUniqueUserId:`
	`  Type: 'Custom::rCustomGetUniqueUserIdWithLambda'`
	`  Properties:`
	`  ServiceToken: !GetAtt GetUserLambdaFunction.Arn`
	`  NewIamUserName: !Ref NewIamUserName`
	
	Este recurso personalizado llama a la función de Lambda para obtener el `UserID` de IAM.
		AWS DevOps, arquitecto de nube

Defina CloudFormation los resultados.	Añada el siguiente código a la `Outputs` sección de la CloudFormation plantilla:
	
	`Outputs:`
	`  NewIamUserId:`
	`  Value: !GetAtt rCustomGetUniqueUserId.NewIamUserId`
	
	Muestra el `UserID` de IAM del nuevo usuario de IAM.
		AWS DevOps, arquitecto de nube

Guarde la plantilla.	Guarde los cambios en la CloudFormation plantilla.	AWS DevOps, arquitecto de nube

Implemente la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla.	Para implementar la `get_unique_user_id.yaml` plantilla mediante la CloudFormation consola, siga las instrucciones de la CloudFormation documentación. Como alternativa, puede ejecutar el siguiente AWS CLI comando para implementar la plantilla: `aws cloudformation create-stack \ --stack-name DemoNewUser \ --template-body file://get_unique_user_id.yaml \ --parameters ParameterKey=NewIamUserName,ParameterValue=demouser \ --capabilities CAPABILITY_NAMED_IAM`	AWS DevOps, arquitecto de nube

Recursos relacionados

- Cree una pila desde la CloudFormation consola (CloudFormation documentación)
- Recursos personalizados respaldados por Lambda (documentación) CloudFormation
- Identificadores únicos (documentación de IAM)
- Utilice credenciales temporales con los AWS recursos (documentación de IAM)

Validar Account Factory para el código Terraform (AFT) localmente

Alexandru Pop y Michal Gorniak, Amazon Web Services

Resumen

Este patrón muestra cómo probar localmente el código de HashiCorp Terraform administrado por AWS Control Tower Account Factory for Terraform (AFT). Terraform es una herramienta de infraestructura como código (IaC) que facilita usar el código para aprovisionar y administrar los recursos y la infraestructura en la nube. AFT configura una canalización de Terraform que le ayuda a aprovisionar y personalizar múltiples entradas. Cuentas de AWS AWS Control Tower

Durante el desarrollo del código, puede resultar útil probar su infraestructura de Terraform como código (IaC) a nivel local, fuera de la canalización de AFT. Este ejemplo muestra cómo hacer lo siguiente:

- Recupere una copia local del código de Terraform que está almacenado en los AWS CodeCommit repositorios de su cuenta de administración de AFT.
- Simule la canalización de AFT de forma local con el código recuperado.

Este procedimiento también se puede utilizar para ejecutar comandos de Terraform que no forman parte de la canalización AFT normal. Por ejemplo, puede usar este método para ejecutar comandos como `terraform validate`, `terraform plan`, `terraform destroy`, `yterraform import`.

Requisitos previos y limitaciones

Requisitos previos

- Un entorno activo de AWS múltiples cuentas que utiliza AWS Control Tower
- Un entorno AFT completamente implementado
- AWS Command Line Interface (AWS CLI), instalado y configurado
- AWS CLI asistente de credenciales para AWS CodeCommit, instalado y configurado
- Python 3.x
- Git, instalado y configurado en su equipo local
- Utilidad de `git-remote-commit` instalada and configurada
- Terraform, instalado y configurado (la versión local del paquete Terraform debe coincidir con la versión que se utiliza en la implementación de AFT)

Limitaciones

- Este patrón no cubre los pasos de implementación necesarios para AWS Control Tower el AFT o cualquier módulo específico de Terraform.
- El resultado que se genera localmente durante este procedimiento no se guarda en los registros de tiempo de ejecución de AFT Pipeline.

Arquitectura

Pila de tecnología de destino

- Infraestructura AFT implementada dentro de una AWS Control Tower implementación
- Terraform
- Git
- AWS CLI versión 2

Automatización y escala

Este patrón muestra cómo invocar localmente el código de Terraform para las personalizaciones de cuentas globales de AFT en una sola cuenta administrada por AFT. Cuenta de AWS Una vez validado el código de Terraform, puede aplicarlo al resto de las cuentas de su entorno de múltiples cuentas. Para obtener más información, consulte Volver a invocar las personalizaciones en la documentación. AWS Control Tower

También puede usar un proceso similar para ejecutar las personalizaciones de la cuenta AFT en una terminal local. Para invocar localmente el código de Terraform desde las personalizaciones de la cuenta AFT, clone el aft-account-customizationsrepositorio en lugar del aft-global-account-customizationsrepositorio desde CodeCommit su cuenta de administración de AFT.

Tools (Herramientas)

Servicios de AWS

- AWS Control Towerle ayuda a configurar y gobernar un entorno de AWS cuentas múltiples, siguiendo las mejores prácticas prescriptivas.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que te ayuda a interactuar Servicios de AWS mediante los comandos de tu shell de línea de comandos.

Otros servicios

- HashiCorp Terraform es una herramienta de infraestructura como código (IaC) que facilita usar el código para aprovisionar y administrar los recursos y la infraestructura en la nube.
- Git es un sistema de control de versiones distribuido y de código abierto.

Código

El siguiente es un ejemplo de un script bash que se puede usar para ejecutar localmente el código de Terraform administrado por AFT. Para usar el script, siga las instrucciones de la sección Epics de este patrón.

```
#! /bin/bash
# Version: 1.1 2022-06-24 Unsetting AWS_PROFILE since, when set, it interferes with
 script operation
#          1.0 2022-02-02 Initial Version
#
# Purpose: For use with AFT: This script runs the local copy of TF code as if it were
 running within AFT pipeline.
#        * Facilitates testing of what the AFT pipline will do
#           * Provides the ability to run terraform with custom arguments (like 'plan'
 or 'move') which are currently not supported within the pipeline.
#
# © 2021 Amazon Web Services, Inc. or its affiliates. All Rights Reserved.
# This AWS Content is provided subject to the terms of the AWS Customer Agreement
# available at http://aws.amazon.com/agreement or other written agreement between
# Customer and either Amazon Web Services, Inc. or Amazon Web Services EMEA SARL or
 both.
#
# Note: Arguments to this script are passed directly to 'terraform' without parsing nor
 validation by this script.
#
# Prerequisites:
#    1. local copy of ct GIT repositories
#    2. local backend.tf and aft-providers.tf filled with data for the target account
 on which terraform is to be run
#       Hint: The contents of above files can be obtain from the logs of a previous
 execution of the AFT pipeline for the target account.
#    3. 'terraform' binary is available in local PATH
#    4. Recommended: .gitignore file containing 'backend.tf', 'aft_providers.tf' so the
 local copy of these files are not pushed back to git
```

```
readonly credentials=$(aws sts assume-role \
    --role-arn arn:aws:iam::$(aws sts get-caller-identity --query "Account" --output
 text ):role/AWSAFTAdmin \
    --role-session-name AWSAFT-Session \
    --query Credentials )

unset AWS_PROFILE
export AWS_ACCESS_KEY_ID=$(echo $credentials | jq -r '.AccessKeyId')
export AWS_SECRET_ACCESS_KEY=$(echo $credentials | jq -r '.SecretAccessKey')
export AWS_SESSION_TOKEN=$(echo $credentials | jq -r '.SessionToken')
terraform "$@"
```

Epics

Guardar el código de ejemplo como un archivo local

Tarea	Descripción	Habilidades requeridas
Guardar el código de ejemplo como un archivo local.	1. Copie el script bash de ejemplo que se encuentra en la sección Código de este patrón y péguelo en un editor de código. 2. Asigne un nombre al archivo `ct_terraform.sh` y, a continuación, guarde el archivo localmente en una carpeta dedicada, como `~/scripts` o `~/bin`.	Administrador de AWS
Haga que el código de ejemplo sea ejecutable.	Abra una ventana de terminal y autentifíquese en su cuenta de administración de AWS AFT realizando una de las siguientes acciones: • Utilice un perfil de AWS CLI existente que esté configura	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	do con los permisos necesarios para acceder a la cuenta de administr ación de AFT. Para utilizar el perfil, puede ejecutar el siguiente comando: `export AWS_PROFILE=<aft account profile name>` • Si su organización utiliza el SSO para acceder AWS, introduzca las credenciales de su cuenta de administr ación de AFT en la página de SSO de su organización. **Note** Es posible que su organización también tenga una herramien ta personalizada para proporcionar credenciales de autenticación a su AWS entorno.	

Tarea	Descripción	Habilidades requeridas

Verifique el acceso a la cuenta de administración de AFT en la Región de AWS correcta.	**⚠ Important**
	Asegúrese de utilizar la misma sesión de terminal con la que se autenticó en su cuenta de administración de AFT.
	
	1. Navegue hasta su implementación de AFT Región de AWS ejecutando el siguiente comando:
	`export AWS_REGIO N=<aft_region>`
	2. Asegúrese de estar en la cuenta correcta.
	a. Use el siguiente comando:
	`aws code-commit list-repositories`
	b. Compruebe que los repositorios que aparecen en el resultado coincidan con los nombres de los repositor ios que se encuentran en su cuenta de administr ación de AFT.
		Administrador de AWS

Tarea	Descripción	Habilidades requeridas

Crear un nuevo directorio local para almacenar el código del repositorio de AFT.	En la misma sesión de terminal, ejecute los siguientes comandos:
	`mkdir my_aft`
	`cd my_aft`
		Administrador de AWS

Tarea	Descripción	Habilidades requeridas

Clone el código del repositorio AFT remoto.	1. Ejecute el siguiente comando desde el terminal:
	`git clone codecommit::$AWS_REGION://aft-global-customizations`
	Note
	Para simplificar, este procedimiento y AFT utilizan solo una rama de código principal. Para utilizar la ramificación de código, también puede introducir comandos de ramificación de código aquí. Sin embargo, cualquier cambio aplicado desde la rama no principal se revertirá cuando la automatización de AFT aplique el código desde la rama principal.
	2. Vaya al directorio clonado:
	`cd aft-global-customizations/terraform`
		Administrador de AWS

Cree los archivos de configuración de Terraform necesarios para que la canalización AFT se ejecute localmente

Tarea	Descripción	Habilidades requeridas
Abra una canalización AFT previamente ejecutada y copie los archivos de configuración de Terraform en una carpeta local.	**Note** Los archivos de configuración `backend.tf` y `aft-providers.tf` que se crean en esta epic son necesarios para que la canalización de AFT se ejecute localmente. Estos archivos se crean automáticamente dentro de la canalización de AFT basada en la nube, pero deben crearse manualmente para que la canalización se ejecute localmente. La ejecución local de la canalización de AFT requiere un conjunto de archivos que represente la ejecución de la canalización en una sola Cuenta de AWS. 1. Con las credenciales AWS Control Tower de	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	su cuenta de administración, inicie sesión en la Consola de administración de AWSAWS CodePipeline consola y ábrala. Asegúrese de estar en el mismo Región de AWS lugar donde implementó AFT. 2. En el panel de navegación izquierdo, seleccione Canalizaciones. 3. Seleccione ##########-customizations-pipeline. (El ########## es el Cuenta de AWS ID que está utilizando para ejecutar el código de Terraform de forma local). 4. Asegúrese de que la ejecución más reciente marcada muestre un valor correcto. Si el valor es diferente, debe volver a invocar las personalizaciones en el proceso de AFT. Para obtener más información, consulte Volver a invocar las AWS Control Tower personalizaciones en la documentación.	

Tarea	Descripción	Habilidades requeridas
	5. Seleccione el tiempo de ejecución más reciente para ver sus detalles. 6. En la sección Apply-AFT -Global-Customizations, busque la etapa Apply-Ter raform. 7. Seleccione la sección Detalles de la etapa Apply-Terraform. 8. Busque el registro de tiempo de ejecución de la etapa Apply-Terraform. 9. En el registro de tiempo de ejecución, busque la sección que comienza y termina con las líneas siguientes: `"\n\n aft-provi ders.tf ... "\n \n backend.tf"` 10. Copie el resultado entre estas dos etiquetas y guárdelo como un archivo local con un nombre `aft-providers.tf` dentro de la carpeta Terraform local (el directorio de trabajo actual de su sesión de terminal).	

Tarea	Descripción	Habilidades requeridas

	Ejemplo de sentencia providers.tf generada automáticamente
	
	`## Autogenerated providers.tf ## ## Updated on: 2022-05-31 16:27:45 ## provider "aws" { region = "us-east-2" assume_role { role_arn = "arn:aws:iam::########:role/AWSAFTExecution" } default_tags { tags = { managed_by = "AFT" } } }`
	
	11. En el registro de tiempo de ejecución, busque la sección que comienza y termina con las líneas siguientes:
	
	`"\n\n tf ... "\n \n backend.tf"`
	
	12. Copie el resultado entre estas dos etiquetas y guárdelo como un archivo	

Tarea	Descripción	Habilidades requeridas
	local con un nombre `tf` dentro de la carpeta Terraform local (el directorio de trabajo actual de su sesión de terminal). Ejemplo de instrucción backend.tf generada automáticamente `## Autogenerated backend.tf ## ## Updated on: 2022-05-31 16:27:45 ## terraform { required_version = ">= 0.15.0" backend "s3" { region = "us-east-2" bucket = "aft-backend-#######-primary-region" key = "##########-aft-global-customizations/terraform.tfstate" dynamodb_table = "aft-backend-#######" encrypt = "true" kms_key_id = "########-####-####-####-############" role_arn = "arn:aws:iam::####`	

Tarea	Descripción	Habilidades requeridas

	`#########:role/AWS AFTExecution"`
	`  }`
	`}`
	
	Note
	Los `aft-providers.tf` archivos `backend.tf` y están vinculados a una implementación y una carpeta específicas Cuenta de AWS de AFT. Estos archivos también son diferentes, dependiendo de si están en el aft-account-customizationsrepositorio aft-global-customizationsy dentro de la misma implementación de AFT. Asegúrese de generar ambos archivos a partir de la misma lista de tiempo de ejecución.	

Ejecute la canalización AFT localmente mediante el script bash de ejemplo

Tarea	Descripción	Habilidades requeridas
Implemente los cambios de configuración de Terraform que desee validar.	1. Navegue hasta el aft-global-customizations repositorio clonado ejecutando el siguiente comando: `cd aft-global-customizations/terraform` **Note** Los archivos `backend.tf` y `aft-providers.tf` están en este directorio. El directorio también contiene los archivos de Terraform del aft-global-customizations repositorio. 2. Incorpore los cambios de código de Terraform que desee probar localmente en los archivos de configuración.	Administrador de AWS
Ejecute el script `ct_terraform.sh` y revise el resultado.	1. Navegue hasta la carpeta local que contiene el script sh. 2. Para validar el código de Terraform modificad	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	o, ejecute el script `ct_terraform.sh` ejecutando el siguiente comando:
	`~/scripts/ct_terraform.sh apply`
	`terraform --help`
	Note
	Puede ejecutar cualquier comando de Terraform durante este paso. Para ver una lista completa de comandos de Terraform, ejecute el siguiente comando:
	3. Revise el resultado del comando y, a continuación, depure los cambios de código localmente antes de confirmarlos y devolverlos al repositorio de AFT.
	Important	

Tarea	Descripción	Habilidades requeridas
	• Cualquier cambio hecho localmente y que no se devuelva al repositor io remoto es temporal y se podría deshacer en cualquier momento mediante una automatiz ación de canalización de AFT en ejecución. • La automatización de AFT se puede ejecutar en cualquier momento, ya que otros usuarios pueden invocarla y activar la automatización de AFT. • AFT siempre aplicará el código de la rama principal del repositorio, deshacien do cualquier cambio no confirmado.	

Devolución de los cambios de código local al repositorio de AFT

Tarea	Descripción	Habilidades requeridas
Agregue referencias a los archivos `backend.tf` y `aft-providers.tf` a un archivo `.gitignore` .	Añada los archivos `backend.tf` y `aft-providers.tf` que creó a un archivo `.gitignore` ejecutando los siguientes comandos: `echo backend.tf >> .gitignore`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	`echo aft-providers.tf >>.gitignore` **Note** Al mover los archivos al archivo `.gitignore` , se garantiza que no se confirmen ni se devuelvan al repositorio de AFT remoto.	

Tarea	Descripción	Habilidades requeridas

Confirme y envíe los cambios de código al repositorio AFT remoto.	1. Para añadir nuevos archivos de configuración de Terraform al repositorio, ejecute el siguiente comando:
	`git add <filename>`
	2. Para confirmar los cambios y enviarlos al repositorio AFT remoto CodeCommit, ejecute los siguientes comandos:
	`git commit -a`
	`git push`
	Important
	Los cambios de código que introduzca siguiendo este procedimiento hasta ese momento se aplicarán Cuenta de AWS únicamente a uno de ellos.
		Administrador de AWS

Implementación de los cambios en varias cuentas

Tarea	Descripción	Habilidades requeridas
Implemente los cambios en todas sus cuentas administradas por AFT.	Para implementar los cambios en varios Cuentas de AWS gestionados por AFT, siga las instrucciones de la documentación sobre cómo volver a invocar las personalizaciones. AWS Control Tower	Administrador de AWS

Más patrones

- Agregue HA a Oracle PeopleSoft en Amazon RDS Custom mediante una réplica de lectura
- Audite automáticamente los grupos de AWS seguridad que permiten el acceso desde direcciones IP públicas
- Automatice la creación de cuentas mediante el acelerador de zonas de aterrizaje en AWS
- Automatice la adición o actualización de entradas de registro de Windows con AWS Systems Manager
- Automatice la evaluación de recursos de AWS
- Automatice la implementación de productos y la cartera de AWS Service Catalog mediante AWS CDK
- Automatización de la conmutación por error y la conmutación por recuperación entre regiones mediante DR Orchestrator Framework
- Automatice la eliminación de AWS CloudFormation pilas y recursos asociados
- Automatización de la ingesta y visualización de métricas personalizadas de Amazon MWAA en Amazon Managed Grafana mediante Terraform
- Automatizar la configuración de RabbitMQ en Amazon MQ
- Automatice la implementación de lagos de Supply Chain datos en una configuración de múltiples repositorios
- Automatice la replicación de las instancias de Amazon RDS en Cuentas de AWS
- Adjunte automáticamente una política gestionada por AWS para Systems Manager a los perfiles de EC2 instancia mediante Cloud Custodian y AWS CDK
- Cree CI/CD canalizaciones y clústeres de Amazon ECS de forma automática para microservicios mediante AWS CDK
- Detecta automáticamente los cambios e inicia diferentes CodePipeline canalizaciones para un monorepo en CodeCommit
- Cree una canalización de datos para incorporar, transformar y analizar los datos de Google Analytics con el kit de AWS DataOps desarrollo
- Cree un PAC de servidor empresarial Micro Focus con Amazon EC2 Auto Scaling y Systems Manager
- Cree e inserte imágenes de Docker en Amazon ECR mediante GitHub Actions y Terraform
- Construye una AWS landing zone que incluya MongoDB Atlas

- Centralización de la administración de claves de acceso de IAM en AWS Organizations mediante Terraform
- Centralización de la distribución de paquetes de software en AWS Organizations mediante Terraform
- Configure el registro de invocación de modelos en Amazon Bedrock mediante AWS CloudFormation
- Configurar el enrutamiento de solo lectura en los grupos de disponibilidad de Always On en SQL Server on AWS
- Cree un portal para microinterfaces mediante Angular AWS Amplify y Module Federation
- Cree un marco de orquestación de recursos basado en API con GitHub Actions y Terragrunt
- Crear una EventBridge conexión entre cuentas de Amazon en una organización
- Crear automáticamente canalizaciones de CI dinámicas para proyectos de Java y Python
- Implemente una API de Amazon API Gateway en un sitio web interno mediante puntos de conexión privados y un Equilibrador de carga de aplicación
- Implemente y gestione AWS Control Tower los controles mediante el uso AWS CDK y CloudFormation
- Implemente y gestione AWS Control Tower controles mediante Terraform
- Despliega canarios de CloudWatch Synthetics con Terraform
- Implemente un clúster de CockroachDB en Amazon EKS mediante Terraform
- Implementación de un sistema de archivos de Lustre para un procesamiento de datos de alto rendimiento mediante Terraform y DRA
- Implemente un caso de uso de RAG AWS mediante Terraform y Amazon Bedrock
- Despliega recursos en una AWS Wavelength zona mediante Terraform
- Implemente instancias de clústeres de conmutación por error de SQL Server en Amazon EC2 y Amazon FSx mediante Terraform
- Implemente las automatizaciones de seguridad para la AWS WAF solución mediante Terraform
- Detección de las instancias de bases de datos de Amazon RDS y Aurora que tienen certificados CA vencidos
- Documentación del diseño de su AWS Landing Zone
- Habilite el modo automático de Amazon EKS en todos los clústeres de EKS mediante GitHub acciones

- Exportar los informes de AWS Backup de toda la organización en AWS Organizations como un archivo CSV
- Genere recomendaciones personalizadas y reclasificadas con Amazon Personalize
- Control de los conjuntos de permisos para varias cuentas mediante Account Factory for Terraform
- Asegurar AWS IAM Roles Anywhere con un certificado privado
- Identifique y avise cuando los recursos de Amazon Data Firehose no estén cifrados con una clave AWS KMS
- Implementación del Generador de cuentas para Terraform (AFT) mediante una canalización de arranque
- Implementación del control de versiones de API basado en rutas mediante dominios personalizados en Amazon API Gateway
- Instalación del agente SSM en los nodos de trabajo de Amazon EKS mediante Kubernetes DaemonSet
- Instale el agente SSM y el CloudWatch agente en los nodos de trabajo de Amazon EKS mediante preBootstrapCommands
- Administre los conjuntos de AWS IAM Identity Center permisos como código mediante AWS CodePipeline
- Administre los conjuntos de AWS permisos de forma dinámica mediante Terraform
- Administre los productos de AWS Service Catalog en varias cuentas y regiones de AWS
- Gestión de las aplicaciones de contenedores en las instalaciones mediante la configuración de Amazon ECS Anywhere con AWS CDK
- Gestione AWS Organizations las políticas como código mediante AWS CodePipeline Amazon Bedrock
- Migración de registros DNS de forma masiva a una zona alojada privada de Amazon Route 53
- Migre Oracle PeopleSoft a Amazon RDS Custom
- Migración de los sistemas BYOL de RHEL a instancias con licencia incluida de AWS mediante AWS MGN
- Supervise ElastiCache los clústeres de Amazon para comprobar el cifrado en reposo
- Supervise la actividad de las aplicaciones mediante CloudWatch Logs Insights
- Supervisión de los clústeres de SAP RHEL Pacemaker mediante los servicios de AWS
- Cree una arquitectura IPAM jerárquica y multirregional mediante Terraform AWS

- Optimice las implementaciones sin servidor con varias cuentas mediante los flujos de trabajo y Actions AWS CDK GitHub
- AWS Service Catalog Aprovisione productos en función de AWS CloudFormation plantillas mediante GitHub acciones
- Aprovisionamiento de roles de IAM con privilegio mínimo mediante la implementación de una solución de máquina expendedora de roles
- Elimine EC2 las entradas de Amazon Cuentas de AWS de un lado a otro AWS Managed Microsoft AD mediante AWS Lambda la automatización
- Elimine EC2 las entradas de Amazon en el mismo Cuenta de AWS AWS Managed Microsoft AD formulario mediante AWS Lambda la automatización
- Proteja las transferencias de archivos mediante Transfer Family, Amazon Cognito y GuardDuty
- Enviar una notificación cuando se cree un usuario de IAM
- Configuración de un router de celdas sin servidor para una arquitectura basada en celdas
- Configure una CI/CD canalización para cargas de trabajo híbridas en Amazon ECS Anywhere mediante AWS CDK y GitLab
- Configure una HA/DR arquitectura para Oracle E-Business Suite en Amazon RDS Custom con una base de datos en espera activa
- Configurar la resolución de DNS para redes híbridas en un entorno de cuentas múltiples AWS
- Configure una infraestructura Multi-AZ para una FCI Always On de SQL Server mediante Amazon FSx
- Configure la funcionalidad UTL_FILE de Oracle en Aurora compatible con PostgreSQL
- Simplificación de la autenticación de aplicaciones con TLS mutuo en Amazon ECS mediante el equilibrador de carga de aplicación
- Simplifique la administración de certificados privados mediante AWS Private CA y AWS RAM
- Optimice los flujos de trabajo de aprendizaje automático desde el desarrollo local hasta los experimentos escalables mediante el uso de SageMaker IA e Hydra
- Etiquete automáticamente las conexiones de puerta de enlace de tránsito con AWS Organizations
- Funciones de transición para una PeopleSoft aplicación de Oracle en Amazon RDS Custom for Oracle
- Uso de Amazon Q Developer como asistente de codificación para aumentar la productividad

Aplicaciones web y móviles

Temas

- Autentique a los usuarios de la aplicación React mediante las interfaces de usuario de Amazon Cognito y AWS Amplify
- Crear una aplicación React con AWS Amplify y añadir autenticación con Amazon Cognito
- Cree un portal para microinterfaces mediante Angular AWS Amplify y Module Federation
- Implemente una aplicación de una sola página basada en React en Amazon S3 y CloudFront
- Implemente una API de Amazon API Gateway en un sitio web interno mediante puntos de conexión privados y un Equilibrador de carga de aplicación
- Incorpore componentes visuales de Amazon Quick Sight en aplicaciones web mediante Amazon Cognito y la automatización iAC
- Explore el desarrollo completo de aplicaciones web nativas en la nube con Green Boost
- Estructure un proyecto de Python en una arquitectura hexagonal con AWS Lambda
- Más patrones

Autentique a los usuarios de la aplicación React mediante las interfaces de usuario de Amazon Cognito y AWS Amplify

Daniel Kozhemyako, Amazon Web Services

Resumen

Este patrón muestra cómo añadir capacidades de autenticación a una aplicación React de frontend existente mediante una biblioteca de interfaz de usuario de AWS Amplify y un grupo de usuarios de Amazon Cognito.

El patrón emplea Amazon Cognito para proporcionar autenticación, autorización y administración de usuarios en la aplicación. También utiliza un componente de Amplify UI, una biblioteca de código abierto que amplía las capacidades del desarrollo de la interfaz de AWS Amplify usuario (UI). El componente de interfaz de usuario de Authenticator administra los inicios de sesión y ejecuta el flujo de trabajo conectado a la nube que autentica a los usuarios a través de Amazon Cognito.

Tras implementar este patrón, los usuarios pueden iniciar sesión con cualquiera de las siguientes credenciales:

- Nombre de usuario y contraseña
- Proveedores de identidad social, como Apple, Facebook, Google y Amazon
- Proveedores de identidad empresarial compatibles con SAML 2.0 o con OpenID Connect (OIDC)

> **Note**
>
> Para crear un componente de interfaz de usuario de autenticación personalizado, puede ejecutar el componente de interfaz de usuario de Authenticator en modo sin periféricos.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Una aplicación web de React 18.2.0 o posterior
- Node.js y npm 6.14.4 o posterior, instalados

Limitaciones

- Este patrón se aplica únicamente a aplicaciones web React.
- Este patrón emplea un componente de Amplify UI prediseñado. La solución no abarca los pasos necesarios para implementar un componente de interfaz de usuario personalizado.

Versiones de producto

- Amplify UI 6.1.3 o posterior (Gen 1)
- Amplify 6.0.16 o posterior (Gen 1)

Arquitectura

Arquitectura de destino

En el siguiente diagrama se muestra una arquitectura que emplea Amazon Cognito para autenticar usuarios en una aplicación web React.

Tools (Herramientas)

Servicios de AWS

- Amazon Cognito ofrece autenticación, autorización y administración de usuarios para aplicaciones móviles y web.

Otras herramientas

- Amplify UI es una biblioteca de interfaz de usuario de código abierto que proporciona componentes personalizables que se pueden conectar a la nube.
- Node.js es un entorno de JavaScript ejecución basado en eventos diseñado para crear aplicaciones de red escalables.
- npm es un registro de software que se ejecuta en un entorno Node.js y se utiliza para compartir o tomar prestados paquetes y administrar la implementación de paquetes privados.

Prácticas recomendadas

Si está desarrollando una nueva aplicación, le recomendamos que use Amplify Gen 2.

Epics

Crear un grupo de usuarios de Amazon Cognito

Tarea	Descripción	Habilidades requeridas
Cree un grupo de usuarios.	Crear un grupo de usuarios de Amazon Cognito. Configure las opciones de inicio de sesión y los requisitos de seguridad del grupo de usuarios según su caso de uso.	Desarrollador de aplicaciones
Agregar un cliente de aplicación.	Configure un cliente de aplicación para un grupo de usuarios. Este cliente es necesario para que la aplicación interactúe con el grupo de usuarios de Amazon Cognito.	Desarrollador de aplicaciones

Integración del grupo de usuarios de Amazon Cognito con el componente de interfaz de usuario de Authenticator

Tarea	Descripción	Habilidades requeridas
Instale las dependencias.	Para instalar los paquetes `aws-amplify` y `@aws-amplify/ui-react`, ejecute el comando siguiente desde el directorio raíz de la aplicación: `npm i @aws-amplify/ui-react aws-amplify`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Configure el grupo de usuarios.	Según el siguiente ejemplo, cree un archivo `aws-exports.js` y guárdelo en la carpeta `src`. El archivo dene tener la información siguiente:
	• Región de AWS en el que se encuentra su grupo de usuarios de Amazon Cognito
	• ID del grupo de usuarios de Amazon Cognito
	• ID de cliente de la aplicación
	
	`// replace the user pool region, id, and app client id details`
	`const awsmobile = {`
	`"aws_project_region": "put_your_region_here",`
	`"aws_cognito_region": "put_your_region_here",`
	`"aws_user_pools_id": "put_your_user_pool_id_here",`
	`"aws_user_pools_web_client_id": "put_your_user_pool_app_id_here"`
	`}`
	
	`export default awsmobile;`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Importe y configure el servicio Amplify.	1. En el archivo de punto de entrada de la aplicación (por ejemplo, `App.js`), importe y cargue el archivo `aws-exports.js` introduciendo las siguientes líneas de código:
	`import { Amplify } from 'aws-amplify'; import awsExports from './aws-exports';`
	2. Según el siguiente ejemplo, configure el cliente de Amplify mediante el archivo `aws-exports.js` :
	`// Configure Amplify in index file or root file Amplify.configure({ ...awsExports });`
	Para más información, consulte Configuración de las categorías de Amplify en la documentación de Amplify.
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Agregue el componente de interfaz de usuario de Authenticator.	Para mostrar el componente de interfaz de usuario de `Authenticator` , añada las siguientes líneas de código al archivo de punto de entrada de la aplicación (`App.js`):
	`import { Authenticator } from '@aws-amplify/ui-react';`
	`import '@aws-amplify/ui-react/styles.css';`
	Note
	El fragmento de código de ejemplo importa el componente de interfaz de usuario `Authenticator` y el archivo de Amplify UI styles.css (obligatorio cuando se usan los temas prediseñados del componente).
	El componente de interfaz de usuario `Authenticator` proporciona dos valores de retorno:
	• Detalles del usuario
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	• Una función que puede invocarse para cerrar la sesión del usuario Vea el siguiente ejemplo de componente: `function App() { return ( <Authenticator> {({ signOut, user }) => ( <div> <p>Welcome {user.username}</p> <button onClick={signOut}>Sign out</button> </div> )} </Authenticator> ); }` **Note** Para ver un ejemplo de un archivo `App.js`, consulte la sección de información adicional de este patrón.	

Tarea	Descripción	Habilidades requeridas

(Opcional) Recupere la información de la sesión.	Una vez autenticado un usuario, puede recuperar sus datos de sesión del cliente Amplify. Por ejemplo, puede recuperar el token web JSON (JWT) de la sesión de un usuario para autenticar las solicitudes de su sesión en una API de backend.
	
	Consulte el siguiente ejemplo de un encabezado de solicitud que incluye un JWT:
	
	`import { fetchAuthSession } from 'aws-amplify/auth';`
	`(await fetchAuthSession()).tokens?.idToken?.toString();`
		Desarrollador de aplicaciones

Resolución de problemas

Problema	Solución
Los usuarios nuevos no pueden registrarse en la aplicación.	Asegúrese de que su grupo de usuarios de Amazon Cognito esté configurado para permitir que los usuarios puedan registrarse ellos mismos en el grupo de usuarios. • Inicie sesión en la Consola de administración de AWS consola de Amazon Cognito y ábrala. • En el panel de navegación izquierdo, elija Grupos de usuarios.

Problema	Solución
	• Elija su grupo de usuario de la lista. • En General Settings (Configuración general), elija Policies (Políticas). • Seleccione Permitir que los usuarios se registren por sí mismos.
El componente de autenticación dejó de funcionar después de actualizar de la v5 a la v6.	La categoría `Auth` ha pasado a un enfoque funcional y ha denominado parámetros en Amplify v6. Ahora debe importar la función APIs directamente desde la `aws-amplify/auth` ruta. Para más información, consulte Migración de v5 a v6 en la documentación de Amplify.

Recursos relacionados

- Introducción a Amazon Cognito (sitio web)AWS
- Cree una nueva aplicación de React (documentación de React)
- ¿Qué es Amazon Cognito? (Documentación de Amazon Cognito)
- Librería de Amplify UI (documentación de Amplify)

Información adicional

El archivo `App.js` debe contener el siguiente código:

```
import './App.css';
import { Amplify } from 'aws-amplify';
import awsExports from './aws-exports';
import { fetchAuthSession } from 'aws-amplify/auth';
import { Authenticator } from '@aws-amplify/ui-react';
import '@aws-amplify/ui-react/styles.css';
Amplify.configure({ ...awsExports });
let token = (await fetchAuthSession()).tokens?.idToken?.toString();
function App() {
  return (
```

```
      <Authenticator>
        {({ signOut, user }) => (
            <div>
              <p>Welcome {user.username}</p>
                <p>Your token is: {token}</p>
              <button onClick={signOut}>Sign out</button>
            </div>
        )}
      </Authenticator>
  );
}

export default App;
```

Crear una aplicación React con AWS Amplify y añadir autenticación con Amazon Cognito

Rishi Singla, Amazon Web Services

Resumen

Este patrón muestra cómo usar AWS Amplify para crear una aplicación basada en React y cómo añadir autenticación a frontend mediante Amazon Cognito. AWS Amplify consta de un conjunto de herramientas (marco de código abierto, entorno de desarrollo visual, consola) y servicios (alojamiento de aplicaciones web y sitios web estáticos) para acelerar el desarrollo de aplicaciones móviles y web en AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Node.js y npm instalados en su equipo

Versiones de producto

- Node.js versión 10.x o posterior (para verificar su versión, ejecute `node -v` en una ventana de terminal)
- npm versión 6.x o posterior (para verificar su versión, ejecute `npm -v` en una ventana de terminal)

Arquitectura

Pila de tecnología de destino

- AWS Amplify
- Amazon Cognito

Tools (Herramientas)

- Amplificar la interfaz de la línea de comandos (CLI)
- Bibliotecas Amplify (bibliotecas cliente de código abierto)

- Amplify Studio (interfaz visual)

Epics

Instalar la CLI de AWS Amplify

Tarea	Descripción	Habilidades requeridas

Instalar la CLI de Amplify	La CLI de Amplify es una cadena de herramientas unificada para crear servicios en la nube de AWS para su aplicación React. Para instalar la CLI de Amplify, ejecute:
	`npm install -g @aws-amplify/cli`
	npm le notificará si hay una nueva versión principal disponible. Si es así, utilice el siguiente comando para actualizar su versión de npm:
	`npm install -g npm@9.8.0`
	donde 9.8.0 se refiere a la versión que desea instalar.
		Desarrollador de aplicaciones

Crear una aplicación React

Tarea	Descripción	Habilidades requeridas

Crear una React App.	Para crear una nueva aplicación React, utilice el comando:
	`npx create-react-app amplify-react-application`
	donde `ampify-react-application` es el nombre de la aplicación.
	Cuando haya creado correctamente la aplicación, verá el siguiente mensaje:
	`Success! Created amplify-react-application`
	Se creará un directorio con varias subcarpetas para la aplicación React.
		Desarrollador de aplicaciones

Inicie la aplicación en el equipo local.	Vaya al directorio `amplify-react-application` que se creó en el paso anterior y ejecute el comando: `amplify-react-application% npm start` Esto inicia la aplicación React en la máquina local.	Desarrollador de aplicaciones

Configurar la CLI de Amplify

Tarea	Descripción	Habilidades requeridas
Configure Amplify para que se conecte a su cuenta de AWS.	Configure Amplify ejecutando el comando: `amplify-react-application % amplify configure` La CLI de Amplify le pide que siga estos pasos para configurar el acceso a su cuenta de AWS: 1. Inicie sesión en su cuenta de administrador de AWS. 2. Especifique la región de AWS que quiere utilizar. 3. Cree un usuario de AWS Identity and Access Management (IAM) con acceso programático y adjunte la política de permisos `AdministratorAccess-Amplify` al usuario. 4. Cree y luego copie el ID de la clave de acceso y la clave de acceso secreta. 5. Introduzca estos detalles en la terminal. 6. Cree un nombre de perfil o utilice el perfil por defecto.	AWS general, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	Warning En este escenario, se requieren usuarios de IAM con acceso programático y credenciales de larga duración, lo que supone un riesgo de seguridad. Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten. Las claves de acceso se pueden actualizar si es necesario. Para obtener más información, consulte Actualización de claves de acceso en la Guía de usuario de IAM. Estos pasos se muestran en la terminal de la siguiente manera.	

Tarea	Descripción	Habilidades requeridas

	`Follow these steps to set up access to your AWS account:`
	`Sign in to your AWS administrator account: https://console.aws.amazon.com/`
	`Press Enter to continue`
	`Specify the AWS Region`
	`? region:  us-east-1`
	`Follow the instructions at https://docs.amplify.aws/cli/start/install/#configure-the-amplify-cli`
	`to complete the user creation in the AWS console`
	`https://console.aws.amazon.com/iamv2/home#/users/create`
	`Press Enter to continue`
	`Enter the access key of the newly created user:`
	`? accessKeyId: ********************`
	`? secretAccessKey: ********************`
	`This would update/create the AWS Profile in your local machine`
	`? Profile Name:  new`
	
	`Successfully set up the new user.`
	
	Para obtener más información sobre estos pasos, consulte	

Tarea	Descripción	Habilidades requeridas
	la documentación del Amplify Dev Center.	

Inicializar Amplify

Tarea	Descripción	Habilidades requeridas

Inicialice Amplify.	1. Para inicializar Amplify en el nuevo directorio, ejecute:
	`amplify init`
	Amplify le solicita el nombre del proyecto y los parámetros de configura ción
	2. Especifique todos los parámetros y, a continuac ión, pulse Y para inicializar el proyecto con la configura ción especificada.
	`Project information`
	`| Name: amplifyre actproject`
	`| Environment: dev`
	`| Default editor: Visual Studio Code`
	`| App type: javascrip t`
	`| Javascript framework: react`
		Desarrollador de aplicaciones, AWS general

Tarea	Descripción	Habilidades requeridas

	<pre>| Source Directory
	 Path: src
	
	| Distribution
	 Directory Path: build
	
	| Build Command: npm
	 run-script build
	
	| Start Command: npm
	 run-script start</pre>
	3. Seleccione el perfil que creó en el paso anterior. Los recursos se desplegar án en el entorno `dev` del proyecto Amplify que creó.
	4. Para confirmar que se han creado los recursos, puede abrir la consola de AWS Amplify y ver la CloudForm ation plantilla de AWS que se utilizó para crear los recursos y los detalles.
	
	<pre>Deploying root stack
	 amplifyreactproject
	 [==================
	==----------------
	----] 2/4
	amplify-amplif
	yreactproject-d…
	 AWS::CloudFormatio
	n::Stack
	 CREATE_IN_PROGRESS
	
	UnauthRole
	 AWS::IAM:</pre>	

Tarea	Descripción	Habilidades requeridas

	`:Role CREATE_COMPLETE`
	
	`DeploymentBucket AWS::S3::Bucket CREATE_IN_PROGRESS`
	
	`AuthRole AWS::IAM::Role CREATE_COMPLETE`	

Agregar la autenticación a frontend

Tarea	Descripción	Habilidades requeridas
Añada la autenticación.	Puede usar el comando `amplify add <category>` para agregar característica como el inicio de sesión de un usuario o una API de backend. En este paso, utilizará el comando para añadir la autenticación. Amplify proporciona un servicio de autenticación de backend con Amazon Cognito, bibliotecas de frontend y un componente de Authenticator UI integrado. Las características incluyen el registro de usuarios, el inicio de sesión	Desarrollador de aplicaciones, AWS general

Tarea	Descripción	Habilidades requeridas
	de los usuarios, la autentica ción multifactorial, el cierre de sesión de los usuarios y el inicio de sesión sin contraseñ a. También puede autentica r a los usuarios mediante la integración con proveedores de identidad federados, como Amazon, Google y Facebook. La categoría de autentica ción de Amplify se integra perfectamente con otras categorías de Amplify, como API, análisis y almacenam iento, para que pueda definir reglas de autorización para usuarios autenticados y no autenticados. 1. Para configurar la autentica ción de su aplicación React, ejecute el comando: `amplify-react-appl ication1 % amplify add auth` Esto muestra la siguiente información y solicitudes. Puede elegir la configura ción adecuada en función de sus requisitos empresari ales y de seguridad.	

Tarea	Descripción	Habilidades requeridas
	``` Using service: Cognito, provided by: awscloudformation The current configure d provider is Amazon Cognito. Do you want to use the default authentic ation and security configuration? (Use arrow keys) # Default configura tion Default configura tion with Social Provider (Federati on) Manual configura tion I want to learn more. ``` 2. Para ver un ejemplo sencillo, seleccione la configuración predeterm inada y, a continuación, seleccione el mecanismo de inicio de sesión para los usuarios (en este caso, el correo electrónico): ``` How do you want users to be able to sign in? Username	

Tarea	Descripción	Habilidades requeridas

	<pre>```
	# Email
	
	  Phone Number
	
	  Email or Phone
	 Number
	
	  I want to learn
	 more.
	``</pre>
	3. Omita la configuración avanzada para completar la adición de los recursos de autenticación:
	<pre>```
	Do you want to
	 configure advanced
	 settings? (Use arrow
	 keys)
	# No, I am done.
	
	  Yes, I want to make
	 some additional
	 changes.
	``</pre>
	4. Cree sus recursos de backend locales y aprovisió nelos en la nube:
	<pre>```
	amplify-react-appl
	ication1 % amplify
	 push
	``</pre>
	Este comando realiza los cambios adecuados en los grupos de usuarios de Congito de su cuenta.	

Tarea	Descripción	Habilidades requeridas

	5. Pulse Y para configurar el `auth` recurso mediante CloudFormation.
	
	Esto configura los siguiente s recursos:
	
	`UserPool AWS::Cognito::UserPool CREATE_COMPLETE UserPoolClientWeb AWS::Cognito::UserPoolClient CREATE_COMPLETE`
	
	`UserPoolClientWeb AWS::Cognito::UserPoolClient CREATE_COMPLETE`
	
	`UserPoolClientRole AWS::IAM::Role CREATE_COMPLETE`
	
	`UserPoolClientLambda AWS::Lambda::Function CREATE_COMPLETE UserPoolClientLambdaPolicy AWS::IAM::Policy CREATE_COMPLETE`
	
	`UserPoolClientLogPolicy AWS::IAM::Policy CREATE_IN`	

Tarea	Descripción	Habilidades requeridas
	<pre>_PROGRESS</pre> También puede usar la Consola de AWS Cognito para ver estos recursos (busque grupos de usuarios y grupos de identidades de Cognito). Este paso actualiza el archivo `aws-exports.js` de la carpeta `src` de la aplicación React con las configuraciones del grupo de usuarios y del grupo de identidades de Cognito.	

Cómo cambiar el archivo App.js

Tarea	Descripción	Habilidades requeridas

Cambie el archivo App.js.	En la carpeta `src`, abra y revise el archivo `App.js`. El archivo modificado debe tener el siguiente aspecto:
	
	<pre>{ App.Js File after
	 modifications:
	import React from
	 'react';
	import logo from './
	logo.svg';
	import './App.css';
	import { Amplify } from
	 'aws-amplify';</pre>
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	`import { withAuthenticator, Button, Heading } from '@aws-amplify/ui-react';`
	`import awsconfig from './aws-exports';`
	`Amplify.configure(awsconfig);`
	`function App({ signOut }) {`
	`return (`
	`<div>`
	`<h1>Thankyou for doing verification</h1>`
	`<h2>My Content</h2>`
	`<button onClick={signOut}>Sign out</button>`
	`</div>`
	`);`
	`}`
	`export default withAuthenticator(App);`	

Importe paquetes de React.	El archivo `App.js` importa dos paquetes de React. Instale estos paquete mediante el comando: `amplify-react-application1 % npm install --save aws-amplify @aws-amplify/ui-react`	Desarrollador de aplicaciones

Inicie la aplicación React y compruebe la autenticación

Tarea	Descripción	Habilidades requeridas
Inicie la aplicación.	Inicie la aplicación React en su máquina local: `amplify-react-appl ication1 % npm start`	Desarrollador de aplicaciones, AWS general
Compruebe la autenticación.	Compruebe si la aplicació n solicita los parámetros de autenticación. (En nuestro ejemplo, configuramos el correo electrónico como método de inicio de sesión). La frontend UI debería pedirle las credenciales de inicio de sesión y ofrecerle la opción de crear una cuenta. También puede configurar el proceso de compilación de Amplify para añadir el backend como parte de un flujo de trabajo de implement ación continua. Sin embargo, este patrón no aborda esa opción.	Desarrollador de aplicaciones, AWS general

Recursos relacionados

- Introducción (documentación de npm)
- Crear una cuenta de AWS independiente (documentación de administración de cuentas de AWS)
- Documentación de AWS Amplify

- Documentación de Amazon Cognito

Cree un portal para microinterfaces mediante Angular AWS Amplify y Module Federation

Milena Godau y Pedro Garcia, Amazon Web Services

Resumen

Una arquitectura de micro-frontend permite a varios equipos trabajar en diferentes partes de una aplicación de frontend de forma independiente. Cada equipo puede desarrollar, crear e implementar un fragmento del frontend sin interferir con otras partes de la aplicación. Desde la perspectiva del usuario final, parece ser una aplicación única y cohesiva. Sin embargo, están interactuando con varias aplicaciones independientes publicadas por diferentes equipos.

En este documento se describe cómo crear una arquitectura de micro-frontend mediante el uso de AWS Amplify, el marco de frontend de Angular y Module Federation. En este patrón, los micro-frontends se combinan en el lado del cliente mediante una aplicación de intérprete de comandos (o principal). La aplicación de intérprete de comandos actúa como un contenedor que recupera, muestra e integra los micro-frontends. La aplicación de intérprete de comandos gestiona el enrutamiento global, que carga diferentes micro-frontends. El complemento @angular-architects/module-federation integra Module Federation con Angular. Para implementar la aplicación shell y las microinterfaces, utilice. AWS Amplify Los usuarios finales acceden a la aplicación a través de un portal web.

El portal está dividido verticalmente. Esto significa que los micro-frontends son vistas completas o grupos de vistas, en lugar de partes de la misma vista. Por lo tanto, la aplicación de intérprete de comandos carga solo un micro-frontend cada vez.

Los micro-frontends se implementan como módulos remotos. La aplicación de intérprete de comandos carga estos módulos remotos de forma lenta, lo que aplaza la inicialización del micro-frontend hasta que sea necesaria. Este enfoque optimiza el rendimiento de la aplicación al cargar solo los módulos necesarios. Esto reducirá el tiempo de carga inicial y mejorará la experiencia general del usuario. Además, comparte dependencias comunes entre los módulos a través del archivo de configuración del paquete web (webpack.config.js). Esta práctica promueve la reutilización del código, reduce la duplicación y agiliza el proceso de agrupación.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Node.js y npm instalados.
- CLI de Amplify instalada
- CLI de Angular instalada
- Permisos de uso AWS Amplify
- Familiaridad con Angular

Versiones de producto

- Versión 13.1.2 o posterior de la CLI de Angular
- @angular-architects/module-federation versión 14.0.1 o posterior
- webpack versión 5.4.0 o posterior
- AWS Amplify Generación 1

Limitaciones

Una arquitectura de micro-frontend es un enfoque poderoso para crear aplicaciones web escalables y resilientes. Sin embargo, es fundamental comprender los siguientes desafíos potenciales antes de adoptar este enfoque:

- Integración: uno de los principales desafíos es el posible aumento de la complejidad en comparación con los micro-frontends monolíticos. Organizar múltiples micro-frontends, gestionar la comunicación entre ellos y gestionar las dependencias compartidas puede resultar más complejo. Además, puede haber una sobrecarga de rendimiento asociada a la comunicación entre los micro-frontends. Esta comunicación puede aumentar la latencia y reducir el rendimiento. Esto debe abordarse mediante mecanismos de mensajería eficientes y estrategias de intercambio de datos.
- Duplicación de código: dado que cada micro-frontend se desarrolla de forma independiente, existe el riesgo de duplicar el código para funciones comunes o bibliotecas compartidas. Esto puede aumentar el tamaño total de la aplicación e introducir problemas de mantenimiento.
- Coordinación y administración: coordinar los procesos de desarrollo e implementación en múltiples micro-frontends puede ser un desafío. Garantizar un control de versiones uniforme, gestionar las dependencias y mantener la compatibilidad entre los componentes se vuelve más fundamental en una arquitectura distribuida. Establecer una gobernanza clara, directrices y procesos automatizados de pruebas e implementación es esencial para una colaboración y una entrega fluidas.

- Pruebas: probar arquitecturas de micro-frontends puede ser más complejo que probar micro-frontends monolíticos. Se requieren esfuerzos adicionales y estrategias de prueba especializadas para realizar end-to-end pruebas y ensayos de integración entre componentes y para validar experiencias de usuario consistentes en múltiples microinterfaces.

Antes de decidirse por el enfoque de las microinterfaces, le recomendamos que consulte Cómo entender e implementar las microinterfaces en. AWS

Arquitectura

En una arquitectura de micro-frontend, cada equipo desarrolla e implementa las características de forma independiente. La siguiente imagen muestra cómo trabajan juntos varios DevOps equipos. El equipo del portal desarrolla la aplicación de intérprete de comandos. La aplicación de intérprete de comandos actúa como contenedor. Recupera, muestra e integra las aplicaciones de microinterfaz publicadas por otros equipos. DevOps Se utiliza AWS Amplify para publicar la aplicación shell y las aplicaciones de microinterfaz.

El diagrama de la arquitectura muestra el flujo de trabajo siguiente:

1. El equipo del portal desarrolla y mantiene la aplicación de intérprete de comandos. La aplicación de intérprete de comandos organiza la integración y el renderizado de los micro-frontends para componer todo el portal.
2. Los equipos A y B desarrollan y mantienen uno o más micro-frontends o características que se integran en el portal. Cada equipo puede trabajar de forma independiente en sus respectivos micro-frontends.
3. El usuario final se autentica mediante Amazon Cognito.
4. El usuario final accede al portal y se carga la aplicación de intérprete de comandos. A medida que el usuario navega, la aplicación de intérprete de comandos se encarga del enrutamiento y recupera el micro-frontend solicitado y carga su paquete.

Tools (Herramientas)

Servicios de AWS

- AWS Amplifyes un conjunto de herramientas y funciones especialmente diseñadas que ayudan a los desarrolladores frontend, web y móvil a crear rápidamente aplicaciones completas. AWS En

este patrón, se utiliza la CLI de Amplify para implementar las aplicaciones de micro-frontend de Amplify.

- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que te ayuda a interactuar Servicios de AWS mediante los comandos de tu consola de línea de comandos.

Otras herramientas

- @angular-architects/module-federation es un complemento que integra Angular con Module Federation.
- Angular es un marco de aplicaciones web de código abierto para crear aplicaciones de una sola página modernas, escalables y comprobables. Sigue una arquitectura modular y basada en componentes que promueve la reutilización y el mantenimiento del código.
- Node.js es un entorno de JavaScript ejecución basado en eventos diseñado para crear aplicaciones de red escalables.
- npm es un registro de software que se ejecuta en un entorno Node.js y se utiliza para compartir o tomar prestados paquetes y administrar la implementación de paquetes privados.
- Webpack Module Federation lo ayuda a cargar código que se compila e implementa de forma independiente, como micro-frontends o complementos, en una aplicación.

Repositorio de código

El código de este patrón está disponible en el portal Microfrontend utilizando Angular y los repositorios Module Federation. GitHub Este repositorio contiene las dos carpetas siguientes:

- `shell-app` contiene el código de la aplicación de intérprete de comandos.
- `feature1-app` contiene un ejemplo de micro-frontend. La aplicación de intérprete de comandos busca este micro-frontend y lo muestra como una página dentro de la aplicación del portal.

Prácticas recomendadas

Las arquitecturas de micro-frontend ofrecen numerosas ventajas, pero también introducen complejidad. Las siguientes son algunas de las prácticas recomendadas para un desarrollo fluido, un código de alta calidad y una excelente experiencia de usuario:

- Planificación y comunicación: para agilizar la colaboración, invierta en planificación, diseño y canales de comunicación claros desde el principio.

- Coherencia en el diseño: aplique un estilo visual coherente en todos los micro-frontends mediante el uso de sistemas de diseño, guías de estilo y bibliotecas de componentes. Esto proporciona una experiencia de usuario coherente y acelera el desarrollo.
- Gestión de las dependencias: dado que los micro-frontends evolucionan de forma independiente, adopte contratos y estrategias de control de versiones estandarizados para administrar las dependencias de forma eficaz y evitar problemas de compatibilidad.
- Arquitectura de micro-frontend: para permitir el desarrollo y la implementación independientes, cada micro-frontend debe tener una responsabilidad clara y bien definida en relación con una funcionalidad encapsulada.
- Integración y comunicación: para facilitar una integración fluida y minimizar los conflictos, defina contratos y protocolos de comunicación claros entre las microinterfaces APIs, incluidos los eventos y los modelos de datos compartidos.
- Pruebas y control de calidad: implemente la automatización de las pruebas y los procesos de integración continua para los micro-frontends. Esto mejora la calidad general, reduce el esfuerzo de realizar pruebas manuales y valida la funcionalidad entre las interacciones de los micro-frontends.
- Optimización del rendimiento: supervise continuamente las métricas de rendimiento y realice un seguimiento de las dependencias entre los micro-frontends. Esto lo ayuda a identificar los cuellos de botella y a mantener un rendimiento óptimo de las aplicaciones. Para ello, utilice herramientas de supervisión del rendimiento y análisis de dependencias.
- Experiencia de desarrollador: para centrarse en la experiencia del desarrollador, proporcione documentación, herramientas y ejemplos claros. Esto lo ayuda a agilizar el desarrollo e incorporar nuevos miembros al equipo.

Epics

Creación de la aplicación de intérprete de comandos

Tarea	Descripción	Habilidades requeridas
Cree la aplicación de intérpret e de comandos.	1. En la CLI de Angular, introduzca el comando siguiente:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	`ng new shell --routing`
	2. Introduzca el siguiente comando para navegar a la carpeta del proyecto:
	`cd shell`
	Note
	La estructura de carpetas y proyectos de las aplicaciones del intérprete de comandos y micro-frontend puede ser totalmente independiente. Se pueden gestionar como aplicacio nes de angular independientes.	

Tarea	Descripción	Habilidades requeridas
Instale el complemento.	En la CLI de Angular, introduzca el siguiente comando para instalar el complemento @angular-architects/module-federation: `ng add @angular-architects/module-federation --project shell --port 4200`	Desarrollador de aplicaciones
Añada la URL del micro-frontend como variable de entorno.	1. Abra el archivo environment.ts. 2. Añada `mfe1URL: 'http://localhost:5000'` al objeto `environment` : `export const environment = { production: false, mfe1URL: 'http://localhost:5000', };` 3. Guarde y cierre el archivo environment.ts.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Defina el enrutamiento.	1. Abra el archivo app-routing.module.ts.
	2. En la CLI de Angular, introduzca el siguiente comando para importar el módulo `loadRemoteModule` del complemento @angular-architects/module-federation:
	`import { loadRemoteModule } from '@angular-architects/module-federation';`
	3. Establezca la ruta predeterminada de la siguiente manera:
	`{ path: '', pathMatch: 'full', redirectTo: 'mfe1' },`
	4. Establezca la ruta para el micro-frontend:
	`{ path: 'mfe1', loadChildren: () => loadRemoteModule({ type: 'module',`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	<pre>remoteEntry:
	`${environment.mfe1URL}/remoteEntry.js`,
	exposedModule: './Module'
	})
	.then(m => m.Mfe1Module)
	},</pre>
	5. Guarde y cierre el archivo app-routing.module.ts.	

Declare el módulo `mfe1`.	1. En la carpeta `src`, cree un archivo nuevo llamado decl.d.ts. 2. Abra el archivo decl.d.ts. 3. Agregue lo siguiente al archivo: <pre>declare module 'mfe1/Module';</pre> 4. Guarde y cierre el archivo decl.d.ts.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Prepare la precarga para el micro-frontend.	La precarga del micro-fro ntend ayuda al paquete web a negociar adecuadamente las bibliotecas y paquetes compartidos.
	1. Abra el archivo main.ts.
	2. Sustituya el contenido por lo siguiente:
	`import { loadRemot eEntry } from '@angular-architec ts/module-federati on';`
	`Promise.all([ loadRemoteEntry(` ${environment.mfe1U RL}/remoteEntry.js `, 'mfe1'), ]) .catch(err => console.error('Err or loading remote entries', err)) .then(() => import('. /bootstrap')) .catch(err => console.error(err) );`
	3. Guarde y cierre el archivo main.ts.
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Ajuste el contenido HTML.	1. Abra el archivo app.component.html. 2. Sustituya el contenido por lo siguiente: `<h1>Shell application is running!</h1> <router-outlet></router-outlet>` 3. Guarde y cierre el archivo app.component.html.	Desarrollador de aplicaciones

Creación de la aplicación de micro-frontend

Tarea	Descripción	Habilidades requeridas

Cree el micro-frontend.	1. En la CLI de Angular, introduzca el comando siguiente:
	`ng new mfe1 --routing`
	2. Introduzca el siguiente comando para navegar a la carpeta del proyecto:
	`cd mfe1`
		Desarrollador de aplicaciones

Instale el complemento.	Introduzca el siguiente comando para instalar el complemento @angular-architects/module-federation: `ng add @angular-architects/module-`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`federation --project mfe1 --port 5000`	

Cree un módulo y un componente.	Introduzca los siguientes comandos para crear un módulo y un componente y exportarlos como módulo de entrada remota:
	`ng g module mfe1 --routing`
	`ng g c mfe1`
		Desarrollador de aplicaciones

Defina la ruta de enrutamiento predeterminada.	1. Abra el archivo mfe-routing.module.ts. 2. Establezca la ruta predeterminada de la siguiente manera: `{ path: '', component: Mfe1Component },` 3. Guarde y cierre el archivo mfe-routing.module.ts.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Añada la ruta `mfe1`.	1. Abra el archivo app-routing.module.ts.
	2. Establezca la ruta predeterminada de la siguiente manera:
	`{ path: '', pathMatch: 'full', redirectTo: 'mfe1' }`
	3. Agregue la siguiente ruta `mfe1`:
	`{ path: 'mfe1', loadChildren: () => import('./mfe1/mfe1.module').then((m) => m.Mfe1Module), }`
	4. Guarde y cierre el archivo app-routing.module.ts.
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Edite el archivo webpack.config.js.	1. Abra el archivo webpack.config.js. 2. Edite la sección `For remotes` para que coincida con lo siguiente: 3. En la sección `shared`, añada las dependencias que la aplicación `mfe1` comparta con la aplicación de intérprete de comandos:	Desarrollador de aplicaciones

```
// For remotes (please
 adjust)
    name: "mfe1",
    filename:
 "remoteEntry.js",
    exposes: {
        './Module':
 './src/app/mfe1/mf
e1.module.ts',
    },
```

```
shared: share({
        "@angular/
core": { singleton
: true, strictVer
sion: true, requiredV
ersion: 'auto' },
        "@angular/
common": { singleton
: true, strictVer
sion: true, requiredV
ersion: 'auto' },
        "@angular
/common/http":
 { singleton: true,
 strictVersion: true,
```

Tarea	Descripción	Habilidades requeridas
	``` requiredVersion: 'auto' }, "@angular/ router": { singleton : true, strictVer sion: true, requiredV ersion: 'auto' }, ...shared Mappings.getDescri ptors() }) ``` 4. Guarde y cierre el archivo webpack.config.js.	
Ajuste el contenido HTML.	1. Abra el archivo app.compo nent.html. 2. Sustituya el contenido por lo siguiente: ``` <router-outlet></r outer-outlet> ``` 3. Guarde y cierre el archivo app.component.html.	Desarrollador de aplicaciones

Ejecución local de las aplicaciones

Tarea	Descripción	Habilidades requeridas
Ejecute la aplicación `mfe1`.	1. Escriba el siguiente comando para iniciar la aplicación `mfe1`: ``` npm start ```	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	2. En un navegador web, acceda a `http://localhost:5000` . 3. Compruebe que el micro-frontend se puede ejecutar de forma independiente. La aplicación `mfe1` debería renderizarse correctamente y sin errores.	
Ejecute la aplicación de intérprete de comandos.	1. Escriba los siguientes comandos para iniciar la aplicación de intérprete de comandos: `npm start` 2. En un navegador web, acceda a `http://localhost:4200/mfe1` . 3. Compruebe que el micro-frontend `mfe1` esté integrado en la aplicación de intérprete de comandos. La aplicación del portal debe renderizarse correctamente sin errores y la aplicación `mfe1` debe estar incrustada en ella.	Desarrollador de aplicaciones

Refactorice la aplicación de intérprete de comandos para gestionar un error de carga en el micro-frontend.

Tarea	Descripción	Habilidades requeridas

Cree un módulo y un componente.	En la carpeta raíz de la aplicación de intérprete de comandos, introduzca los siguientes comandos para crear un módulo y un componente para una página de errores:
	`ng g module error-page --routing`
	`ng g c error-page`
		Desarrollador de aplicaciones

Ajuste el contenido HTML.	1. Abra el archivo error-page.component.html 2. Sustituya el contenido por lo siguiente: `<p>Sorry, this page is not available.</p>` 3. Guarde y cierre el archivo error-page.component.html.	Desarrollador de aplicaciones
Defina la ruta de enrutamiento predeterminada.	1. Abra el archivo error-page-routing.module.ts. 2. Establezca la ruta predeterminada de la siguiente manera: `{ path: '', component: ErrorPageComponent`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	<pre>},</pre> 3. Guarde y cierre el archivo .module.ts. error-page-routing	

Tarea	Descripción	Habilidades requeridas

Cree una función para cargar micro-frontends.	1. Abra el archivo app-routing.module.ts.
	2. Cree la siguiente función:
	`function loadMFE(url: string) { return loadRemoteModule({ type: 'module', remoteEntry: `${url}/remoteEntry.js`, exposedModule: './Module' }) .then(m => m.Mfe1Module) .catch( () => import('./error-page/error-page.module').then(m => m.ErrorPageModule) ); }`
	3. Modificar la ruta `mfe1` para que sea como la siguiente:
	`{ path: 'mfe1', loadChildren: () => loadMFE(environment.mfe1URL) },`
	4. Guarde y cierre el archivo app-routing.module.ts.
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Pruebe la gestión de errores.	1. Si aún no se está ejecutando, ejecute el siguiente comando para iniciar la aplicación de intérprete de comandos:
	`npm start`
	2. En un navegador web, acceda a `http://localhost:4200/mfe1` .
	3. Compruebe que esté representada la página de error. Debería ver el texto siguiente:
	`Sorry, this page is not available.`
		Desarrollador de aplicaciones

Implemente las aplicaciones mediante AWS Amplify

Tarea	Descripción	Habilidades requeridas
Implemente el micro-frontend.	1. En la CLI de Amplify, vaya hasta la carpeta raíz de la aplicación de micro-frontend. 2. Introduzca el comando siguiente para inicializar Amplify: `amplify init`	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	3. Cuando se le pida que introduzca un nombre para su proyecto de Amplify, pulse Intro. De esta forma, se reutiliza el nombre del archivo package.json. 4. Cuando se le pida que inicialice el proyecto con la configuración anterior, introduzca `Yes`. 5. Cuando se le pida que seleccione un método de autenticación, elija `AWS Profile`. 6. Seleccione el perfil que desea usar. 7. Espere a que Amplify inicie el proyecto. Cuando se complete este proceso, recibirá un mensaje de confirmación en el terminal. 8. Introduzca el siguiente comando para agregar una categoría de alojamiento de Amplify al micro-frontend: `amplify add hosting` 9. Cuando se le pida que seleccione el módulo del complemento, elija `Hosting with Amplify Console`.	

Tarea	Descripción	Habilidades requeridas

	10. Cuando se le pida que seleccione un tipo, elija `Manual deployment` .
	11. Para instalar las dependencias de npm del proyecto, introduzca el comando siguiente:
	`npm install`
	12. Publique la aplicación en la consola de Amplify; para ello, ejecute el siguiente comando:
	`amplify publish -y`
	Cuando se completa la publicación, Amplify devuelve la URL del micro-frontend.
	13. Copie la dirección URL. Necesitará este valor para actualizar la aplicación de intérprete de comandos.	

Tarea	Descripción	Habilidades requeridas

Implemente la aplicación de intérprete de comandos.	1. En la src/app/environmentscarpeta, abra el archivo environments.prod.ts.
	2. Sustituya el valor `mfe1URL` por la URL del micro-frontend implementado:
	`export const environment = { production: true, mfe1URL: 'https://<env>.<Amplify-app-ID>.amplifyapp.com' };`
	3. Guarde y cierre el archivo environments.prod.ts.
	4. En la CLI de Amplify, vaya hasta la carpeta raíz de la aplicación de intérprete de comandos.
	5. Introduzca el comando siguiente para inicializar Amplify:
	`amplify init`
	6. Cuando se le pida que introduzca un nombre para su proyecto de Amplify, pulse Intro. De esta forma, se reutiliza el nombre del archivo package.json.
	7. Cuando se le pida que inicialice el proyecto con
		Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas

	la configuración anterior, introduzca `Yes`.
	8. Cuando se le pida que seleccione un método de autenticación, elija `AWS Profile`.
	9. Seleccione el perfil que desea usar.
	10. Espere a que Amplify inicie el proyecto. Cuando se complete este proceso, recibirá un mensaje de confirmación en el terminal.
	11. Añada una categoría de alojamiento de Amplify a la aplicación de intérprete de comandos:
	`amplify add hosting`
	12. Cuando se le pida que seleccione el módulo del complemento, elija `Hosting with Amplify Console`.
	13. Cuando se le pida que seleccione un tipo, elija `Manual deployment` .
	14. Instale las dependencias de npm del proyecto con el siguiente comando:
	`npm install`	

Tarea	Descripción	Habilidades requeridas
	15. Publique la aplicación de intérprete de comandos en la consola de Amplify; para ello, ejecute el siguiente comando: `amplify publish -y` Cuando se completa la publicación, Amplify devuelve la URL de la aplicación de intérprete de comandos implementada. 16. Anote la URL de la aplicación de intérprete de comandos.	

Tarea	Descripción	Habilidades requeridas
Habilite CORS.	Como las aplicaciones de intérprete de comandos y micro-frontend se alojan de forma independiente en dominios diferentes, debe habilitar el uso compartido de recursos entre orígenes (CORS) en el micro-frontend. Esto permite que la aplicación de intérprete de comandos cargue el contenido desde un origen diferente. Para habilitar CORS, añada encabezados personalizados. 1. En la CLI de Amplify, vaya hasta la carpeta raíz del micro-frontend. 2. Introduzca el siguiente comando: `amplify configure hosting` 3. Cuando se le pida configuración personalizada, introduzca Y. 4. Inicia sesión en la consola de Amplify y Consola de administración de AWS, a continuación, ábrela. 5. Elija el micro-frontend. 6. En el panel de navegación, seleccione Alojamiento y, a continuación, seleccion	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas

	e Encabezados personali zados.
	7. Seleccione Editar.
	8. En la ventana Editar encabezados personali zados, introduzca lo siguiente:
	`customHeaders:`
	`  - pattern: '*.js'`
	`    headers:`
	`      - key: Access-Co ntrol-Allow-Origin`
	`        value: '*'`
	`      - key: Access-Co ntrol-Allow-Methods`
	`        value: 'GET, OPTIONS'`
	`      - key: Access-Co ntrol-Allow-Headers`
	`        value: '*'`
	9. Seleccione Save.
	10. Vuelva a implementar el micro-frontend para aplicar los nuevos encabezados personalizados.	

Tarea	Descripción	Habilidades requeridas
Cree una regla de reescritura en la aplicación de intérprete de comandos.	La aplicación Angular shell está configurada para usar el HTML5 enrutamiento. Si el usuario realiza una actualización exhaustiva, Amplify intenta cargar una página desde la URL actual. Esto genera un error 403. Para evitarlo, añada una regla de reescritura en la consola de Amplify. Para crear la regla de reescritura, siga estos pasos: 1. En la CLI de Amplify, vaya hasta la carpeta raíz de la aplicación de intérprete de comandos. 2. Introduzca el siguiente comando: `amplify configure hosting` 3. Cuando se le pida configuración personalizada, introduzca Y. 4. Abra la consola de Amplify. 5. Elija la aplicación de intérprete de comandos. 6. En el panel de navegación, elija Alojamiento y, a continuación, elija Reescrituras y redireccionamientos.	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	7. En la página Reescrituras y redireccionamientos, seleccione Administrar redireccionamientos. 8. Seleccione Abrir editor de texto. 9. En el editor de texto JSON, introduzca el siguiente redireccionamiento: `[ { "source": "/<*>", "target": "/index.html", "status": "404-200", "condition": null } ]` 10. Seleccione Save.	
Pruebe el portal web.	1. En un navegador web, escriba la URL de la aplicación de intérprete de comandos implementada. 2. Compruebe que la aplicación de intérprete de comandos y el micro-frontend se carguen correctamente.	Desarrollador de aplicaciones

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Elimine las aplicaciones.	Si ya no necesita las aplicaciones de intérprete de comandos y micro-frontend, elimínelas. Esto ayudará a evitar cargos por recursos que no utiliza. 1. Inicia sesión en la consola de Amplify y Consola de administración de AWS, a continuación, ábrela. 2. Elija el micro-frontend. 3. En el panel de navegació n, elija Configuración de la aplicación y, a continuación, Configuración general. 4. Elija Eliminar aplicación. 5. En la ventana de confirmac ión, introduzca `delete` y, a continuación, elija Eliminar aplicación. 6. Para eliminar la aplicación de intérprete de comandos, repita estos pasos.	AWS general

Resolución de problemas

Problema	Solución
No hay ningún AWS perfil disponible al ejecutar el comando `amplify init`	Si no tiene un AWS perfil configurado, puede continuar con el `amplify init` comando.

Problema	Solución
	Sin embargo, debe seleccionar la opción `AWS access keys` cuando se le pida el método de autenticación. Tenga AWS a mano su clave de acceso y su clave secreta. Como alternativa, puede configurar un perfil con nombre para AWS CLI. Para obtener instrucciones, consulte los ajustes de configuración y del archivo de credenciales en la AWS CLI documentación.
Error al cargar las entradas remotas	Si se produce un error al cargar las entradas remotas en el archivo main.ts de la aplicación de intérprete de comandos, asegúrese de que la variable `environment.mfe1URL` esté configurada correctamente. El valor de esta variable debe ser la URL del micro-frontend.
Error 404 al acceder al micro-frontend.	Si recibe un error 404 al intentar acceder al micro-frontend local, por ejemplo, en `http://localhost:4200/mfe1` , compruebe lo siguiente: • Para la aplicación de intérprete de comandos, asegúrese de que la configuración de enrutamiento del archivo app-routing.module.ts esté configurada correctamente y de que la función `loadRemoteModule` llame correctamente al micro-frontend. • Para el micro-frontend, compruebe que el archivo webpack.config.js tenga la configuración `exposes` correcta y asegúrese de que el archivo remoteEntry.js se esté generando correctamente.

Información adicional

AWS documentación

- Comprensión e implementación de las microinterfaces en AWS(orientaciónAWS prescriptiva)
- CLI de Amplify (documentación de Amplify)
- Alojamiento de Amplify (documentación de Amplify)

Otras referencias

- Module Federation
- Node.js
- Angular
- @angular-architects/module-federation

Implemente una aplicación de una sola página basada en React en Amazon S3 y CloudFront

Jean-Baptiste Guillois, Amazon Web Services

Resumen

Una aplicación de una sola página (SPA) es un sitio web o una aplicación web que actualiza dinámicamente el contenido de una página web mostrada mediante el uso de. JavaScript APIs Este enfoque mejora la experiencia del usuario y el rendimiento de un sitio web porque solo actualiza los datos nuevos en lugar de volver a cargar toda la página web desde el servidor.

Este patrón proporciona un step-by-step enfoque para codificar y alojar un SPA escrito en React en Amazon Simple Storage Service (Amazon S3) y Amazon. CloudFront El SPA de este patrón usa una API REST que está configurada en Amazon API Gateway y expuesta a través de una CloudFront distribución de Amazon para simplificar la administración del intercambio de recursos entre orígenes (CORS).

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- Node.js y `npm`, instalados y configurados. Para obtener más información, consulte la sección Descargas de la documentación de Node.js.
- Yarm, instalado y configurado. Para obtener más información, consulte la documentación de Yarn.
- Git, instalado y configurado. Para obtener más información, consulte la documentation de Git.

Arquitectura

Esta arquitectura se implementa automáticamente mediante el uso de AWS CloudFormation (infraestructura como código). Utiliza servicios regionales como Amazon S3 para almacenar los activos estáticos y Amazon CloudFront con Amazon API Gateway para exponer los puntos de enlace de la API regional (REST). Los registros de la aplicación se recopilan a través de Amazon CloudWatch. Todas las llamadas a la AWS API se auditan. AWS CloudTrail Toda la configuración de seguridad (por ejemplo, las identidades y los permisos) se gestiona en AWS Identity and Access

Management (IAM). El contenido estático se entrega a través de la red de entrega de CloudFront contenido (CDN) de Amazon y Amazon Route 53 gestiona las consultas de DNS.

Tools (Herramientas)

Servicios de AWS

- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket APIs a cualquier escala.
- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas Cuentas de AWS las regiones.
- Amazon CloudFront acelera la distribución de tu contenido web al distribuirlo a través de una red mundial de centros de datos, lo que reduce la latencia y mejora el rendimiento.
- AWS CloudTraille ayuda a auditar la gobernanza, el cumplimiento y el riesgo operativo de su empresa Cuenta de AWS.
- Amazon le CloudWatch ayuda a supervisar las métricas de sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Código

El código de aplicación de muestra de este patrón está disponible en el repositorio de aplicaciones de una sola página GitHub CORS basado en React.

Prácticas recomendadas

Al utilizar el almacenamiento de objetos Amazon S3, puede almacenar los activos estáticos de su aplicación de forma segura, altamente resiliente, eficaz y rentable. No es necesario utilizar un contenedor dedicado ni una instancia de Amazon Elastic Compute Cloud (Amazon EC2) para esta tarea.

Al utilizar la red de entrega de CloudFront contenido de Amazon, puedes reducir la latencia que pueden experimentar los usuarios cuando acceden a tu aplicación. También puede conectar un firewall de aplicaciones web (AWS WAF) para proteger sus activos de ataques malintencionados.

Epics

Cree e implemente la aplicación de forma local

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Ejecute el siguiente comando para clonar el repositorio de la aplicación de ejemplo: `git clone https://github.com/aws-samples/react-cors-spa react-cors-spa && cd react-cors-spa`	Desarrollador de aplicaciones, AWS DevOps
Implemente la aplicación de forma local.	1. En el directorio del proyecto, ejecute el comando `npm install` para iniciar las dependencias de la aplicación. 2. Ejecute el comando `yarn dev` para iniciar la aplicación localmente.	Desarrollador de aplicaciones, AWS DevOps
Acceda a la aplicación de forma local.	Abra una ventana del navegador e introduzca la URL `http://localhost:3000` para acceder a la aplicación.	Desarrollador de aplicaciones, AWS DevOps

Implemente de la aplicación

Tarea	Descripción	Habilidades requeridas
Implemente la AWS CloudFormation plantilla.	1. Inicie sesión en la AWS CloudFormation consola y Consola de administración de AWS, a continuación, ábrala. 2. Elija Create stack (Crear pila), y, a continuación, elija With new resources (standard) (Con nuevos recursos [estándar]). 3. Elija Upload a template file (Cargar un archivo de plantilla). 4. Elija Choose file (Elegir archivo), elija el archivo `react-cors-spa-stack.yaml` del repositorio clonado y, a continuación, elija Next (Siguiente). 5. Escriba un nombre para la pila y después elija Next (Siguiente). 6. Conserve todas las opciones predeterminadas, y luego elija Next (Siguiente). 7. Revise la configuración final de su pila, y luego seleccione Create stack (Crear pila).	Desarrollador de aplicaciones, AWS DevOps
Personalice los archivos de origen de su aplicación.	1. Una vez implementada la pila, abra la pestaña Salida	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	e identifique el nombre de `Bucket` y el valor de `APIDomain` . 2. Copie el dominio CloudFront de distribución de la API REST. 3. Navegue hasta la URL `<project_root>/src/pages/index.tsx` y, a continuación, inserte o pegue este dominio en el valor de la variable `APIEndPoint` en la línea 13 del archivo `index.tsx` .	
Cree el paquete de aplicación.	En el directorio del proyecto, ejecute el comando `yarn build` para crear el paquete de aplicación.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Implemente el paquete de aplicación.	1. Abra la consola de Amazon S3. 2. Identifique y elija el depósito de S3 que creó anteriormente la CloudFormation pila. 3. Elija Upload (Cargar) y, a continuación, Add files (Añadir archivos). 4. Elija el contenido de su carpeta de `out`. 5. Elija Añadir carpeta y, a continuación, elija el directorio `_next`. **Important** Elija el directorio `_next`, no el contenido. 6. Elija Upload (Cargar) para cargar los archivos y el directorio a su bucket de S3.	Desarrollador de aplicaciones, AWS DevOps

Pruebe la aplicación

Tarea	Descripción	Habilidades requeridas
Acceda y pruebe la aplicación.	Abra una ventana del navegador y, a continuación, pegue el dominio de CloudFront distribución (el	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`SPADomain` resultado de la CloudFormation pila que implementó anteriormente) para acceder a la aplicación.	

Limpie los recursos

Tarea	Descripción	Habilidades requeridas
Elimine el contenido del bucket de S3.	1. Abra la consola de Amazon S3 y elija el bucket que creó anteriormente con la pila (el primer bucket cuyo nombre comience por `react-cors-spa-`). 2. Seleccione Empty (Vaciar) para eliminar el contenido del bucket. 3. Abra el segundo bucket que creó anteriormente con la pila (el segundo bucket cuyo nombre comience por `react-cors-spa-` y termine por `-logs`). 4. Seleccione Empty (Vaciar) para eliminar el contenido del bucket.	AWS DevOps, desarrollador de aplicaciones
Elimine la CloudFormation pila.	1. Abra la consola de CloudFormation y elija la pila que creó anteriormente.	AWS DevOps, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	2. Elija Delete (Eliminar) para eliminar la pila y todos los recursos relacionados.	

Recursos relacionados

Para implementar y alojar su aplicación web, también puede utilizar AWS Amplify Hosting, que proporciona un flujo de trabajo basado en Git para alojar aplicaciones web sin servidor y full stack con implementación continua. Amplify Hosting forma parte de AWS Amplify, que proporciona un conjunto de herramientas y funciones especialmente diseñadas que permiten a los desarrolladores frontend, web y móvil crear aplicaciones completas de forma rápida y sencilla. AWS

Información adicional

Para gestionar las solicitudes URLs no válidas del usuario que puedan generar 403 errores, una página de errores personalizada configurada en la CloudFront distribución detecta 403 errores y los redirige al punto de entrada de la aplicación (). `index.html`

Para simplificar la administración de CORS, la API REST se expone a través de una CloudFront distribución.

Implemente una API de Amazon API Gateway en un sitio web interno mediante puntos de conexión privados y un Equilibrador de carga de aplicación

Saurabh Kothari, Amazon Web Services

Resumen

Este patrón muestra cómo implementar una API de Amazon API Gateway en un sitio web interno al que se puede acceder desde una red en las instalaciones. Aprenderá a crear un nombre de dominio personalizado para una API privada mediante una arquitectura diseñada con puntos de enlace privados, un Application Load Balancer, PrivateLink AWS y Amazon Route 53. Esta arquitectura evita las consecuencias imprevistas del uso de un nombre de dominio y un servidor proxy personalizados para facilitar el enrutamiento basado en el dominio en una API. Por ejemplo, si despliega un punto de conexión de nube privada virtual (VPC) en una subred no enrutable, su red no podrá acceder a API Gateway. Una solución habitual consiste en utilizar un nombre de dominio personalizado y, a continuación, implementar la API en una subred enrutable, pero esto puede dañar otros sitios internos cuando la configuración del proxy transfiere el tráfico (`execute-api.{region}.vpce.amazonaws.com`) a AWS Direct Connect. Por último, este patrón puede ayudarle a cumplir los requisitos organizativos relacionados con el uso de una API privada a la que no se pueda acceder desde Internet y un nombre de dominio personalizado.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un certificado de indicación de nombre de servidor (SNI) para su sitio web y API
- Una conexión desde un entorno local a una cuenta de AWS configurada mediante AWS Direct Connect o AWS VPN Site-to-Site
- Una zona alojada privada con el dominio correspondiente (por ejemplo, domain.com) que se resuelve desde una red en las instalaciones y reenvía las consultas de DNS a Route 53
- Una subred privada enrutable a la que se puede acceder desde una red en las instalaciones

Limitaciones

Para obtener más información sobre las cuotas (antes denominadas límites) para los equilibradores de carga, las reglas y otros recursos, consulte Cuotas para los Equilibrador de carga de aplicación en la documentación de Elastic Load Balancing.

Arquitectura

Pila de tecnología

- Amazon API Gateway
- Amazon Route 53
- Equilibrador de carga de aplicación
- AWS Certificate Manager
- AWS PrivateLink

Arquitectura de destino

En el siguiente diagrama, se muestra cómo se implementa un Equilibrador de carga de aplicación en una VPC que dirige el tráfico web a un grupo objetivo de un sitio web o a un grupo objetivo de la API Gateway en función de las reglas de oyenete de Equilibrador de carga de aplicación. El grupo objetivo de API Gateway es una lista de direcciones IP para el punto de conexión de VPC en la API Gateway. Puerta de enlace de API está configurado para hacer que la API sea privada con su política de recursos. La política deniega todas las llamadas que no procedan de un punto de conexión de VPC específico. Los nombres de dominio personalizados de la API Gateway se actualizan para usar api.domain.com para la API y su fase. Las reglas de Equilibrador de carga de aplicación se agregan para enrutar el tráfico en función del nombre del host.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario de una red en las instalaciones intenta acceder a un sitio web interno. La solicitud se envía a ui.domain.com y api.domain.com. A continuación, la solicitud se resuelve en el Equilibrador de carga de aplicación interno de la subred privada enrutable. El SSL finaliza en el Equilibrador de carga de aplicación de ui.domain.com y api.domain.com.
2. Las reglas de oyente, configuradas en Equilibrador de carga de aplicación, comprueban el encabezado del host.

a. Si el encabezado del host es api.domain.com, la solicitud se reenvía al grupo objetivo de la API Gateway. El Equilibrador de carga de aplicación inicia una nueva conexión a la API Gateway a través del puerto 443.

b. Si el encabezado del host es ui.domain.com, la solicitud se reenvía al grupo objetivo del sitio web.

3. Cuando la solicitud llega a la API Gateway, la asignación de dominios personalizada configurada en la API Gateway determina el nombre de host y la API que se debe ejecutar.

Automatizar y escalar

Los pasos de este patrón se pueden automatizar mediante AWS CloudFormation o el AWS Cloud Development Kit (AWS CDK). Para configurar el grupo objetivo de las llamadas a la API Gateway, debe usar un recurso personalizado para recuperar la dirección IP del punto de conexión de VPC. Las llamadas a la API describe-network-interfacesenvían describe-vpc-endpointsy devuelven las direcciones IP y el grupo de seguridad, que se pueden utilizar para crear el grupo de direcciones IP objetivo de la API.

Tools (Herramientas)

- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket APIs a cualquier escala.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.
- AWS Certificate Manager (ACM) le ayuda a crear, almacenar y renovar claves y certificados SSL/TLS X.509 públicos y privados que protegen sus sitios web y aplicaciones de AWS.
- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que lo ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- AWS le PrivateLink ayuda a crear conexiones unidireccionales y privadas entre sus servicios externos VPCs a la VPC.

Epics

Crear un certificado SNI

Tarea	Descripción	Habilidades requeridas
Cree un certificado SNI e impórtelo a ACM.	1. Cree un certificado SNI para ui.domain.com y api.domain.com. Para obtener más información, consulta Cómo CloudFront atender las solicitudes HTTPS en la CloudFront documentación de Amazon. 2. Importe los certificados SNI a AWS Certificate Manager (ACM). Para obtener más información sobre estas dos opciones, consulte Importar certificados a AWS Certificate Manager en la documentación de ACM.	Administrador de red

Implemente un punto de conexión de VPC en una subred privada no enrutable

Tarea	Descripción	Habilidades requeridas
Creación de un punto de conexión de VPC de la interfaz para API Gateway.	Para crear un punto de conexión de VPC de interfaz, siga las instrucciones de Acceder a un servicio de AWS mediante un punto de conexión de VPC de interfaz en la documentación de Amazon Virtual Private Cloud (Amazon VPC).	Administrador de la nube

Configure el Equilibrador de carga de aplicación

Tarea	Descripción	Habilidades requeridas
Creación de un grupo de destino para la aplicación.	Creación de un grupo de destino para los recursos de interfaz de usuario de su aplicación.	Administrador de la nube
Cree un grupo objetivo para el punto de conexión de la API Gateway.	1. Cree un grupo de destino con un tipo de dirección IP y, a continuación, añada la dirección IP del punto de conexión de VPC del punto de conexión de la API Gateway al grupo de destino. 2. Configure las comprobaciones de estado para los grupos de destino con el código 403 de éxito. El código 403 es obligatorio porque el punto de conexión de VPC de API Gateway devuelve un código 403 cuando la comprobación de estado del grupo de destino lo invoca sin ningún encabezado.	Administrador de la nube
Cree un Equilibrador de carga de aplicación.	1. Cree un Equilibrador de carga de aplicación (interno) en una subred privada enrutable. 2. Añada el oyente 443 al Equilibrador de carga de	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	aplicación y, a continuación, elija el certificado de ACM.	
Cree reglas de oyentes.	Cree reglas de oyente para hacer lo siguiente: 1. Reenviar el host api.domain.com al grupo objetivo de la API Gateway 2. Reenvíe el host ui.domain.com al grupo de destino de los recursos de la interfaz de usuario	Administrador de la nube

Configure Route 53

Tarea	Descripción	Habilidades requeridas
Crear una zona alojada privada.	Cree una zona alojada privada para domain.com.	Administrador de la nube
Cree registros de dominio.	Cree registros CNAME para lo siguiente: • Una API con el valor establecido en el nombre DNS del Equilibrador de carga de aplicación • Una interfaz de usuario con el valor establecido en el nombre DNS del Equilibrador de carga de aplicación	Administrador de la nube

Cree un punto de conexión de API privado en la API Gateway

Tarea	Descripción	Habilidades requeridas
Cree y configure un punto de conexión de API privado.	1. Para crear un punto de conexión de API privado, siga las instrucciones de Cómo crear una API privada en Amazon API Gateway en la documentación de API Gateway. 2. Configure la política de recursos para permitir las llamadas únicamente a la API desde el punto de conexión de VPC. Para obtener más información, consulte Controlar el acceso a una API con las políticas de recursos de API Gateway en la documentación de API Gateway.	Desarrollador de aplicaciones, administrador de la nube
Cree un nombre de dominio personalizado.	1. Crea un nombre de dominio personalizado para api.domain.com. Para obtener más información, consulte Configuración de nombres de dominio personalizados para REST APIs en la documentación de API Gateway. 2. Seleccione la API y la etapa creadas. Para obtener más información, consulta Cómo trabajar con asignaciones de API para REST APIs en	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	la documentación de API Gateway.	

Recursos relacionados

- Amazon API Gateway
- Amazon Route 53
- Equilibrador de carga de aplicación
- AWS PrivateLink
- AWS Certificate Manager

Incorpore componentes visuales de Amazon Quick Sight en aplicaciones web mediante Amazon Cognito y la automatización iAC

Ishita Gupta, Saurabh Singh y Srishti Wadhwa, de Amazon Web Services

Resumen

Este patrón ofrece un enfoque especializado para integrar los componentes visuales de Amazon Quick Sight en las aplicaciones de React mediante la incorporación de usuarios registrados con la autenticación simplificada de Amazon Cognito. Luego, estos recursos se implementan a través de una plantilla de infraestructura como código (IaC). A diferencia de la integración tradicional de cuadros de mando, esta solución aísla cuadros y gráficos específicos para integrarlos directamente en las aplicaciones de React, lo que mejora drásticamente tanto el rendimiento como la experiencia del usuario.

La arquitectura establece un flujo de autenticación eficiente entre la administración de usuarios de Amazon Cognito y los permisos de Quick Sight: los usuarios se autentican a través de Amazon Cognito y acceden a sus visualizaciones autorizadas según las reglas de uso compartido de paneles de Quick Sight. Este enfoque simplificado elimina la necesidad de acceder directamente a la consola Quick Sight y, al mismo tiempo, mantiene sólidos controles de seguridad.

El entorno completo se implementa a través de una AWS CloudFormation plantilla única que aprovisiona todos los componentes de infraestructura necesarios, incluidos:

- Un backend sin servidor que utiliza Amazon API AWS Lambda Gateway
- Alojamiento frontend seguro a través de Amazon CloudFront, Amazon Simple Storage Service (Amazon S3) y AWS WAF
- Administración de identidades mediante Amazon Cognito

Todos los componentes se configuran siguiendo las prácticas recomendadas de seguridad con políticas de privilegios mínimos AWS Identity and Access Management (IAM), AWS WAF protección y cifrado. end-to-end

Esta solución es ideal para los equipos de desarrollo y las organizaciones que desean integrar análisis interactivos y seguros en sus aplicaciones y, al mismo tiempo, mantener un control detallado del acceso de los usuarios. La solución utiliza servicios AWS gestionados y automatización para simplificar el proceso de integración, mejorar la seguridad y garantizar la escalabilidad para satisfacer las cambiantes necesidades empresariales.

Público objetivo y casos de uso:

- Desarrolladores front-end que desean integrar análisis en las aplicaciones de React
- Equipos de productos de software como servicio (SaaS) que desean ofrecer visualizaciones de datos por usuario o basadas en roles
- Arquitectos de soluciones que estén interesados en integrar la analítica en portales personalizados AWS
- Desarrolladores de inteligencia empresarial (BI) que desean exponer imágenes a usuarios autenticados sin necesidad de acceder por completo al panel
- Equipos empresariales que desean integrar gráficos interactivos de Quick Sight en las herramientas internas

Requisitos previos y limitaciones

Requisitos previos

Para implementar correctamente este patrón, asegúrese de contar con lo siguiente:

- Activo Cuenta de AWS: y Cuenta de AWS con permisos para implementar CloudFormation pilas y crear recursos de Lambda, API Gateway, Amazon Cognito CloudFront y Amazon S3.
- Cuenta Amazon Quick Sight: una cuenta Quick Sight activa con al menos un panel de control que contiene imágenes. Para obtener instrucciones de configuración, consulte el tutorial: Creación de un panel de Amazon Quick Sight con datos de ejemplo en la documentación de Amazon Quick.
- Un entorno de desarrollo que consiste en:
  - Node.js (versión 16 o posterior)
  - npm o yarn instalados
  - Vite como herramienta de compilación de React
  - React (versión 19.1.1)
- Uso compartido de paneles: los paneles deben compartirse en Quick Sight y el implementador debe iniciar sesión para acceder a las imágenes o paneles integrados.

Limitaciones

- Este patrón utiliza el método de incrustación de usuarios registrados, que requiere que los implementadores tengan una cuenta de Quick Sight activa.

- El acceso está restringido a los paneles e imágenes que se comparten explícitamente con el usuario autenticado de Quick Sight que está implementando este patrón. Si el implementador no tiene los derechos de acceso correctos, la generación de la URL incrustada fallará y las imágenes no se cargarán.
- La CloudFormation pila debe implementarse en un entorno en el que Región de AWS se admitan Quick Sight, API Gateway y Amazon Cognito. Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region.

Versiones de producto

- SDK de incrustación de Quick Sight, versión 2.10.1
- React, versión 19.1.1
- Node.js versión 16 o posterior para garantizar la compatibilidad con las últimas versiones de React y Vite utilizadas en esta solución

Arquitectura

Arquitectura de destino

En el siguiente diagrama se muestran los componentes de la arquitectura y el flujo de trabajo de este patrón.

En este flujo de trabajo:

1. El usuario accede a la aplicación. El usuario abre la aplicación web React mediante un navegador. La solicitud se enruta a una CloudFront distribución, que actúa como una red de entrega de contenido para la aplicación.
2. AWS WAF filtra las solicitudes maliciosas. Antes de que llegue la solicitud CloudFront, se tramita AWS WAF. AWS WAF inspecciona el tráfico y bloquea cualquier solicitud maliciosa o sospechosa según las normas de seguridad.
3. Amazon S3 sirve archivos estáticos. Si la solicitud está limpia, CloudFront recupera los recursos estáticos de la interfaz (HTML, JS, CSS) de un bucket privado de S3 mediante el control de acceso de origen (OAC) y los envía al navegador.
4. El usuario inicia sesión. Una vez cargada la aplicación, el usuario inicia sesión a través de Amazon Cognito, que autentica al usuario y devuelve un token web JSON (JWT) seguro para el acceso autorizado a la API.

5. La aplicación realiza una solicitud a la API. Tras iniciar sesión, la aplicación React realiza una llamada segura al `/get-embed-url` punto final de API Gateway y pasa el token JWT al encabezado de la solicitud para su autenticación.
6. El token está validado. API Gateway valida el token mediante un autorizador de Amazon Cognito. Si el token es válido, la solicitud continúa; de lo contrario, se deniega con una respuesta 401 (no autorizada).
7. La solicitud se dirige a Lambda para su procesamiento. A continuación, la solicitud validada se reenvía a una función Lambda de backend. Esta función se encarga de generar la URL de inserción del elemento visual de Quick Sight solicitado.
8. Lambda genera la URL de inserción desde Quick Sight. IAM utiliza una función de IAM con los permisos adecuados para llamar a la `GenerateEmbedUrlForRegisteredUser` API Quick Sight y generar una URL visual segura y orientada al usuario.
9. Lambda devuelve la URL de inserción a API Gateway. Lambda devuelve la URL de inserción generada a API Gateway como parte de una respuesta de JSON. Luego, esta respuesta se prepara para su entrega a la interfaz.
10. La URL de inserción se envía al navegador. La URL de inserción se devuelve al navegador como respuesta de la API.
11. La imagen se muestra al usuario. La aplicación React recibe la respuesta y utiliza el SDK de incrustación Quick Sight para renderizar la imagen específica para el usuario.

Automatización y escala

Las implementaciones de backend y frontend se automatizan por completo mediante el uso de CloudFormation, lo que aprovisiona todos AWS los recursos necesarios, incluidos Amazon Cognito, Lambda, API Gateway, Amazon S3,,, funciones de IAM y Amazon en una sola implementación. CloudFront AWS WAF CloudWatch

Esta automatización garantiza una infraestructura uniforme y repetible en todos los entornos. Todos los componentes se escalan automáticamente: Lambda se ajusta a las invocaciones de funciones, entrega contenido en caché a nivel CloudFront mundial y API Gateway se escala en función de las solicitudes entrantes.

Tools (Herramientas)

Servicios de AWS

- Amazon Quick Sight es un servicio de inteligencia empresarial nativo de la nube que le ayuda a crear, administrar e integrar cuadros de mando y elementos visuales interactivos.
- Amazon API Gateway gestiona APIs la función de puente entre la aplicación React y los servicios de backend.
- AWS Lambdaes un servicio de cómputo sin servidor que este patrón utiliza para generar una integración segura de Quick Sight de forma URLs dinámica y escalable automáticamente en función de las solicitudes.
- Amazon Cognito proporciona autenticación y autorización a los usuarios y emite tokens seguros para el acceso a la API.
- Amazon S3 aloja activos de frontend estáticos para este patrón y los proporciona de forma segura. CloudFront
- Amazon CloudFront ofrece contenido front-end a nivel mundial con baja latencia y se integra con él AWS WAF para filtrar el tráfico.
- AWS WAFprotege la aplicación web del tráfico malicioso mediante la aplicación de reglas de seguridad y la limitación de velocidad.
- AWS CloudFormationautomatiza el aprovisionamiento y la configuración de todos los recursos de la aplicación en una sola implementación.
- Amazon CloudWatch recopila registros y métricas de Lambda, API Gateway y AWS WAF para la supervisión y la solución de problemas.

Herramientas de desarrollo

- React JS es un marco de interfaz que este patrón utiliza para crear la aplicación web e integrar imágenes de Quick Sight integradas.
- Vite es una herramienta de compilación que se utiliza para desarrollar rápidamente y optimizar las compilaciones de producción de la aplicación React.
- El SDK de incrustación de Quick Sight facilita la integración de imágenes de Quick Sight en la aplicación React y permite una interacción perfecta entre la aplicación y las imágenes.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub Amazon Quick Sight Visual Embedding in React.

Prácticas recomendadas

Este patrón implementa automáticamente las siguientes mejores prácticas de seguridad:

- Utiliza grupos de usuarios de Amazon Cognito para la autenticación basada en JWT, con autenticación multifactor (MFA) opcional.
- Se protege APIs con los autorizadores de Amazon Cognito y aplica políticas de IAM con privilegios mínimos en todos los servicios.
- Implementa la incrustación de usuarios registrados de Quick Sight y aprovisiona automáticamente a los usuarios con la función de lector.
- Aplica un cifrado en tránsito compatible con TLS 1.2 y versiones posteriores hasta HTTPS. CloudFront
- Cifra los datos en reposo mediante AES-256 para Amazon S3 con control de versiones y OAC.
- Configura los planes de uso de API Gateway con limitaciones y cuotas.
- Protege Lambda con concurrencia reservada y protección de variables de entorno.
- Permite el registro para Amazon S3 CloudFront, Lambda y API Gateway; monitorea los servicios mediante el uso. CloudWatch
- Cifra los registros, aplica controles de acceso y aplica políticas de denegación para las subidas sin HTTPS o sin cifrar.

Además, recomendamos lo siguiente:

- CloudFormation Utilícelo para automatizar las implementaciones y mantener configuraciones consistentes en todos los entornos.
- Asegúrese de que cada usuario tenga los permisos de Quick Sight correctos para acceder a las imágenes integradas.
- Proteja los puntos de enlace de API Gateway con los autorizadores de Amazon Cognito y aplique el principio de privilegios mínimos para todas las funciones de IAM.
- Guarde información confidencial, como los nombres de los recursos de Amazon (ARNs) y las variables de entorno, IDs en lugar de codificarla de forma rígida.
- Optimice las funciones Lambda reduciendo las dependencias y mejorando el rendimiento del arranque en frío. Para obtener más información, consulte la AWS entrada del blog Cómo optimizar el rendimiento del arranque en frío AWS Lambda mediante el uso de estrategias de cebado avanzadas con. SnapStart

- Añada su CloudFront dominio a la lista de dominios permitidos de Quick Sight para permitir una incrustación visual segura.
- Supervise el rendimiento y la seguridad mediante CloudWatch el uso AWS WAF de registros, alertas y protección del tráfico.

Otras prácticas recomendadas

- Utilice dominios personalizados con certificados SSL de AWS Certificate Manager para ofrecer una experiencia de usuario segura y personalizada.
- Cifre los datos y CloudWatch registros de Amazon S3 mediante claves administradas por el cliente AWS Key Management Service (AWS KMS) para tener un mayor control del cifrado.
- Amplíe AWS WAF las reglas con el bloqueo geográfico, la protección por inyección de SQL (SQLi), la protección contra secuencias de comandos entre sitios (XSS) y filtros personalizados para mejorar la prevención de amenazas.
- Active CloudWatch las alarmas y supervise AWS Config, audite y AWS CloudTrail cumpla con la configuración en tiempo real.
- Aplique políticas de IAM detalladas, refuerce la rotación de claves de API y permita el acceso entre cuentas solo cuando sea absolutamente necesario.
- Realice evaluaciones de seguridad periódicas para garantizar la alineación con los marcos de cumplimiento, como los Controles de Sistemas y Organizaciones 2 (SOC 2), el Reglamento General de Protección de Datos (GDPR) y la Ley de Portabilidad y Responsabilidad de los Seguros de Salud (HIPAA).

Epics

Prepare el entorno

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Clone el GitHub repositor io de esta solución en su sistema local y navegue hasta el directorio del proyecto: `git clone https://g ithub.com/aws-samp`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	`les/sample-quicksight-visual-embedding.git`
	
	`cd sample-quicksight-visual-embedding`
	
	Este repositorio contiene la CloudFormation plantilla y el código fuente de React necesarios para implementar la solución.	

Despliega la CloudFormation pila

Tarea	Descripción	Habilidades requeridas
Implemente la plantilla.	1. Inicie sesión en la AWS CloudFormation consola Consola de administración de AWS y ábrala. 2. En la página Stacks, selecciona Crear pila en la esquina superior derecha y, a continuación, seleccion a Con nuevos recursos (estándar). 3. En la página Crear pila, en Requisito previo: preparar plantilla, selecciona Elegir una plantilla existente. 4. En Specify template (Especificar plantilla), elija Upload a template	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	file (Cargar un archivo de plantilla). 5. Cargue el `template.yaml` archivo desde su GitHub repositorio local y, a continuación, seleccione Siguiente. 6. En la página Especificar los detalles de la pila, introduce el nombre de la pila (por ejemplo,`quicksight-embedding-stack`). 7. En la página Configurar opciones de pila, mantenga la configuración predeterminada y active la casilla para confirmar la creación de recursos de IAM. Elija Siguiente. 8. En la página Revisar y crear, elija Enviar. Para obtener más información, consulte Creación y administración de pilas en la CloudFormation documentación.	
Supervise la creación de pilas.	Supervisa la pila en la pestaña Eventos hasta que su estado sea CREATE_COMPLETE.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Recupera los resultados de la pila.	1. Cuando se complete el despliegue, seleccione la pestaña Salidas. 2. Anote los resultados clave: `ApiGatewayUrl` `UserPoolId` ,`UserPoolClientId` ,`CloudFrontDomainName` , `yS3BucketName` . Utilizará esta información en los pasos siguientes.	Administrador de AWS

Configure el entorno de interfaz

Tarea	Descripción	Habilidades requeridas
Recupere los identificadores visuales de Quick Sight.	1. Abra el panel de control de Quick Sight. 2. Anote el ID del panel, el ID de la hoja y el ID visual de cada elemento visual que desee incrustar en su aplicación web.	Administrador de Quick Sight
Configura tu entorno local de React.	Para configurar tu entorno local de React y vincularlo a AWS los recursos, crea un `.env` archivo en la `my-app/` carpeta de tu GitHub repositorio local. Rellena el archivo con: • Tu Región de AWS	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	• Información sobre el pool de Amazon Cognito (a partir de los resultados de la CloudFormation pila)
	• Punto final de API Gateway (a partir de las salidas de la CloudFormation pila)
	• Vista rápida IDs (`Dashboard Id` ,`SheetId`,`VisualId`)
	
	Este es un `.env` archivo de ejemplo:
	
	`VITE_AWS_REGION=us-east-1`
	
	`# Cognito Configuration (from CloudFormation outputs)`
	`VITE_USER_POOL_ID=us-east-1_xxxxxxxx`
	`x VITE_USER_POOL_WEB_CLIENT_ID=xxxxxxx`
	`xxxxxxxxxxxxxxxxxx`
	
	`# API Configuration (from CloudFormation outputs)`
	`VITE_API_URL=https:/your-api-id.execute-api.us-east-1.amazonaws.com/prod`
	
	`# QuickSight Visual Configuration`
	`VITE_DASHBOARD_ID=your-dashboard-id`	

Tarea	Descripción	Habilidades requeridas
	`VITE_SHEET_ID=your-sheet-id` `VITE_VISUAL_ID=your-visual-id`	

Configura la autenticación de usuarios

Tarea	Descripción	Habilidades requeridas
Crear o administrar usuarios en Cognito	Para permitir el acceso de los usuarios autenticados a las imágenes de Quick Sight integradas, primero debe crear los usuarios en Amazon Cognito: 1. En la consola de Amazon Cognito, elija Grupos de usuarios y, a continuación, elija el grupo que coincida `UserPoolId` (de los CloudFormation resultados). 2. Agregue usuarios al grupo. Puede elegir entre dos opciones. • En Amazon Cognito, cree usuarios manualmente con direcciones de correo electrónico y contraseñas temporales (para obtener más información, consulte la documentación de Amazon Cognito)	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	—o— • Habilite el registro automático en la interfaz de usuario configurá ndolo en el archivo. `hideSignUp={false}` `my-app/src/auth/AuthWrapper.jsx`	

Tarea	Descripción	Habilidades requeridas
Proporcione acceso al panel de control de Quick Sight	Para permitir el acceso a las imágenes de Quick Sight, conceda permiso de Visor a los usuarios autenticados: 1. En la consola Quick Sight, seleccione Paneles de control. 2. Seleccione el panel que desee compartir eligiendo su nombre. 3. En la esquina superior derecha de la página del panel de control, selecciona Compartir. 4. En el panel para compartir , selecciona Compartir con usuarios específicos. 5. Para añadir nuevos usuarios, selecciona Invitar usuarios o el icono con el signo más (+). 6. En el campo de correo electrónico, introduce la dirección de correo electrónico completa del destinatario. (Este correo electrónico debe coincidir exactamente con el inicio de sesión de Amazon Cognito del usuario) 7. En el menú de permisos situado junto al campo	Administrador de Quick Sight

Tarea	Descripción	Habilidades requeridas
	de correo electrónico, seleccione Visor. 8. Para enviar la invitación y conceder el acceso, selecciona Compartir. Cada usuario recibirá un correo electrónico con un enlace al panel de control. Puede modificar los permisos en cualquier momento a través del menú Compartir. Para obtener más información, consulte Conceder acceso a usuarios y grupos individuales de Amazon Quick Sight a un panel de Amazon Quick Sight en la documentación de Amazon Quick.	

Cree e implemente la interfaz de React

Tarea	Descripción	Habilidades requeridas

Instala las dependencias y crea el proyecto.	En el directorio de aplicaciones de React, ejecuta los siguientes comandos para generar archivos de producción optimizados:
	
	`cd my-app`
	`npm install`
	`npm run build`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Cargue los archivos de compilación en Amazon S3.	Cargue todos los archivos del `my-app/dist/` directorio al bucket de S3 aprovisionado por CloudFormation (no cargue la carpeta propiamente dicha).	Desarrollador de aplicaciones
Cree una CloudFront invalidación.	En la CloudFront consola, cree una invalidación para que Path `/*` actualice el contenido en caché tras la implementación. Para obtener instrucciones, consulte Invalidar archivos en la documentación. CloudFront	Administrador de AWS

Configure la lista de permitidos de Quick Sight

Tarea	Descripción	Habilidades requeridas
Agregue el CloudFront dominio a la lista permitida de Quick Sight.	Para permitir que su CloudFront dominio incorpore imágenes de Quick Sight de forma segura: 1. En la consola de Quick Sight, selecciona Administrar Quick Sight, los dominios y la incrustación. 2. Agregue el CloudFront dominio al cuadro Dominio (por ejemplo,`https://d1234567890abc.cloudfront.net`).	Administrador de Quick Sight

Tarea	Descripción	Habilidades requeridas
	3. Elija Añadir dominio.	

Acceda a la aplicación y verifique su funcionalidad

Tarea	Descripción	Habilidades requeridas
Abre la aplicación React.	Usa el CloudFront dominio (de CloudFormation las salidas) para abrir la aplicación web React implementada en un navegador.	Propietario de la aplicación
Verifica la autenticación.	Inicie sesión en la aplicación con las credenciales de Amazon Cognito para verificar el flujo de autenticación y la validación de JWT a través de API Gateway.	Propietario de la aplicación
Verifique las imágenes incrustadas.	Confirme que las imágenes de Quick Sight se carguen correctamente en la aplicación en función de los permisos de acceso específicos del usuario.	Propietario de la aplicación
Valide la conectividad API y Lambda.	Confirme que la aplicación puede llamar correctamente a la `/get-embed-url` API y recuperar una inserción de Quick Sight válida URLs sin errores.	Propietario de la aplicación

Supervise y mantenga la aplicación

Tarea	Descripción	Habilidades requeridas
Supervise mediante el uso de CloudWatch.	Puede usar herramientas de AWS observabilidad para monitorear la aplicación y mantener un rendimiento seguro y escalable en la producción. Revise los registros de Lambda, las métricas de API Gateway y los eventos de autenticación de Amazon Cognito para garantizar CloudWatch el estado de las aplicaciones y detectar anomalías.	Administrador de AWS
Realice un seguimiento y registre. AWS WAF CloudFront	Inspeccione AWS WAF los registros para detectar solicitudes bloqueadas o sospechosas y CloudFront acceda a los registros para ver las métricas de rendimiento y almacenamiento en caché.	Administrador de AWS

Resolución de problemas

Problema	Solución
Error «Dominio no permitido»	1. En la consola Quick Sight, seleccione Administrar Quick Sight, Dominios e Incrustaciones.

Problema	Solución
	2. Agrega tu CloudFront dominio (por ejemplo,`https://d1234567890abc.cloudfront.net`). 3. Guarde la configuración y vuelva a cargar la aplicación.
Errores de autenticación	Causas posibles: • El ID del grupo de usuarios de Amazon Cognito o el ID de cliente de la aplicación son incorrectos en el `.env` archivo. • No se confirmó el usuario en el grupo de usuarios de Amazon Cognito. • El token JWT no es válido o falta en las solicitudes de API. Soluciones: • Compruebe los valores de configuración de Amazon Cognito en el `.env` archivo. • En la consola de Amazon Cognito, compruebe la pestaña Usuarios para comprobar que el usuario está activo. • Confirme que el encabezado de autorización contenga un token JWT válido. • En la consola de API Gateway, compruebe Authorizers para comprobar que API Gateway utiliza el autorizador de Amazon Cognito para la autenticación.

Problema	Solución
Errores de API Gateway	Causas posibles: • Falta o está mal configurado el autorizador de Amazon Cognito en API Gateway. • Permisos Lambda insuficientes para llamar a la API Quick Sight. • La URL de la API no coincide entre los resultados `.env` y los resultados. CloudFormation Soluciones: • Vuelva a confirmar que la URL de invocación de API Gateway está en su `.env` archivo. • En la consola de API Gateway, compruebe Autorizadores para comprobar la configuración de Amazon Cognito. • Adjunte la política de IAM requerida `quicksight:GenerateEmbedUrlForRegisteredUser` a la función de ejecución de Lambda. • Revise CloudWatch los registros para ver si hay errores detallados de API o permisos. Para obtener más información, consulte la documentación de API Gateway.

Problema	Solución
Las imágenes de Quick Sight no se cargan	Causas posibles: • El ID del panel de control, el ID de hoja o el ID visual de Quick Sight son incorrectos en la configuración del entorno. • Los usuarios de Quick Sight no pueden acceder a la imagen o al panel de control. • Falta la configuración de uso compartido de recursos entre orígenes (CORS) en API Gateway. Soluciones: • Confirme la vista rápida IDs desde el menú de tres puntos situado en la esquina superior derecha de la imagen del panel de control. • Confirme que el usuario de Quick Sight tiene la función de visualizador del panel compartido. • Habilite CORS en API Gateway y vuelva a implementar la API. Para obtener más información, consulte la documentación de API Gateway. • Inspeccione la consola del navegador en busca de CORS para ver si hay errores relacionados con la red.

Problema	Solución
Error «El usuario no tiene acceso»	Causas posibles: • El correo electrónico del usuario no se compartió con el panel de Quick Sight. • El rol o el permiso de usuario en Quick Sight son incorrectos. Solución: 1. En la consola de Quick Sight, abra el panel y, a continuación, seleccione Compartir, compartir panel. 2. Añada la dirección de correo electrónico del usuario (que coincida con el correo electrónico de inicio de sesión de Amazon Cognito). 3. Asigne el rol de permiso de espectador. 4. Pide al usuario que cierre sesión y vuelva a iniciarla para actualizar los permisos.

Recursos relacionados

AWS documentación

- Registrarse para obtener una suscripción a Amazon Quick
- Análisis integrados para Amazon Quick Sight
- Referencia de la API Quick Sight: GenerateEmbedUrlForRegisteredUser
- Grupos de usuarios de Amazon Cognito
- AWS Lambda Guía para desarrolladores
- Guía para desarrolladores de Amazon API Gateway
- Monitorización básica y monitorización detallada en CloudWatch
- AWS CloudFormation Guía del usuario
- Guía para CloudFront desarrolladores de Amazon

- AWS WAF Guía para desarrolladores

Tutoriales y videos

- Análisis integrados para Amazon Quick Sight
- YouTube Tutoriales de Amazon Quick Sight

Explore el desarrollo completo de aplicaciones web nativas en la nube con Green Boost

Ben Stickley y Amiin Samatar, Amazon Web Services

Resumen

En respuesta a las necesidades cambiantes de los desarrolladores, Amazon Web Services (AWS) reconoce la demanda crítica de un enfoque eficiente para desarrollar aplicaciones web nativas en la nube. El objetivo de AWS es ayudarlo a superar los obstáculos comunes asociados con la implementación de aplicaciones web en la nube de AWS. Al aprovechar las capacidades de las tecnologías modernas, como el TypeScript AWS Cloud Development Kit (AWS CDK), React y Node.js, este patrón tiene como objetivo agilizar y acelerar el proceso de desarrollo.

Basado en el kit de herramientas Green Boost (GB), el patrón ofrece una guía práctica para crear aplicaciones web que utilicen al máximo las amplias capacidades de AWS. Actúa como una hoja de ruta integral que lo guía a través del proceso de implementación de una aplicación web CRUD (creación, lectura, actualización, eliminación) fundamental integrada con la edición compatible con Amazon Aurora PostgreSQL. Esto se logra mediante el uso de la interfaz de la línea de comandos de Green Boost (CLI de Green Boost) y el establecimiento de un entorno de desarrollo en las instalaciones.

Tras la implementación exitoso de la aplicación, el patrón profundiza en los componentes clave de la aplicación web, como el diseño de la infraestructura, el desarrollo del backend y el frontend, y en herramientas esenciales como cdk-dia para la visualización, lo que facilita la gestión eficiente de los proyectos.

Requisitos previos y limitaciones

Requisitos previos

- Git instalado
- Visual Studio Code (VS Code) instalado
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada
- Kit de herramientas de AWS CDK instalado
- Node.js 18 instalado o Node.js 18 con pnpm activado
- pnpm está instalado, si no forma parte de la instalación de Node.js
- Familiaridad básica con TypeScript AWS CDK, Node.js y React

- Una cuenta de AWS activa
- Una cuenta de AWS iniciada mediante AWS CDK en `us-east-1`. La región de `us-east-1` AWS es necesaria para admitir las funciones de Amazon CloudFront Lambda @Edge.
- Credenciales de seguridad de AWS, incluida `AWS_ACCESS_KEY_ID`, correctamente configuradas en su entorno de terminal
- Para los usuarios de Windows, un terminal en modo administrador (para adaptarse a la forma en que pnpm gestiona los módulos de nodos)

Versiones de producto

- AWS SDK para la JavaScript versión 3
- AWS CDK versión 2
- CLI de AWS versión 2.2
- Node.js versión 18
- React versión 18

Arquitectura

Pila de tecnología de destino

- Edición de Amazon Aurora compatible con PostgreSQL
- Amazon CloudFront
- Amazon CloudWatch
- Amazon Elastic Compute Cloud (Amazon EC2)
- AWS Lambda
- AWS Secrets Manager
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- AWS WAF

Arquitectura de destino

El siguiente diagrama muestra que las solicitudes de los usuarios pasan por Amazon CloudFront, AWS WAF y AWS Lambda antes de interactuar con un bucket de S3, una base de datos de Aurora

o EC2 una instancia y, finalmente, llegar a los desarrolladores. Los administradores, por otro lado, utilizan Amazon SNS y Amazon con CloudWatch fines de notificación y supervisión.

Para obtener una visión más profunda de la aplicación tras su implementación, puede crear un diagrama con cdk-dia, como se muestra en el siguiente ejemplo.

Estos diagramas muestran la arquitectura de la aplicación web desde dos ángulos distintos. El diagrama cdk-dia ofrece una vista técnica detallada de la infraestructura de CDK de AWS y destaca servicios específicos de AWS, como Amazon Aurora, compatible con PostgreSQL, y AWS Lambda. Por el contrario, el otro diagrama adopta una perspectiva más amplia y hace hincapié en el flujo lógico de los datos y las interacciones de los usuarios. La diferencia clave reside en el nivel de detalle: el cdk-dia profundiza en las complejidades técnicas, mientras que el primer diagrama ofrece una visión más centrada en el usuario.

La creación del diagrama cdk-dia se describe en la epopeya Comprenda la infraestructura de aplicaciones mediante AWS CDK.

Tools (Herramientas)

Servicios de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.
- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- La Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de la línea de comandos.
- Amazon CloudFront acelera la distribución de tu contenido web al distribuirlo a través de una red mundial de centros de datos, lo que reduce la latencia y mejora el rendimiento.
- Amazon le CloudWatch ayuda a supervisar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.

- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Secrets Manager le permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- AWS Systems Manager le permite administrar las aplicaciones y la infraestructura que se ejecutan en la nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo requerido para detectar y resolver problemas operativos y ayuda a utilizar y administrar los recursos de AWS a escala de manera segura. Este patrón utiliza el administrador de sesiones de AWS Systems Manager.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le permite almacenar, proteger y recuperar cualquier cantidad de datos. Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- AWS WAF es un firewall de aplicación web que le permite monitorizar las solicitudes HTTP y HTTPS que se reenvíen a los recursos de su aplicación web protegida

Otras herramientas

- Git es un sistema de control de versiones distribuido y de código abierto.
- Green Boost es un conjunto de herramientas para crear aplicaciones web en AWS.
- Next.js es un marco de React para añadir funciones y optimizaciones.
- Node.js es un entorno de JavaScript ejecución basado en eventos diseñado para crear aplicaciones de red escalables.
- pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.
- pnpm es un administrador de paquetes para las dependencias del proyecto Node.js.

Prácticas recomendadas

Consulte la sección Epics para obtener más información sobre las siguientes recomendaciones:

- Supervise la infraestructura mediante Amazon CloudWatch Dashboards y alarmas.
- Aplique las prácticas recomendadas de AWS mediante cdk-nag para ejecutar análisis estáticos de infraestructura como código (IaC).
- Establezca el reenvío de puertos de base de datos a través de túneles SSH (Secure Shell) con Systems Manager Session Manager, que es más seguro que tener una dirección IP expuesta públicamente.
- Gestione las vulnerabilidades ejecutando `pnpm audit`.
- Aplique las mejores prácticas utilizando Prettier ESLintpara realizar análisis estáticos del TypeScript código y estandarizar el formato del código.

Epics

Implemente una aplicación web CRUD con Aurora compatible con PostgreSQL

Tarea	Descripción	Habilidades requeridas
Instale la CLI de Green Boost.	Para instalar Green Boost CLI, ejecute el siguiente comando. `pnpm add -g gboost`	Desarrollador de aplicaciones
Cree una aplicación GB.	1. Para crear una aplicación mediante Green Boost, ejecute el comando `gboost create`. 2. Elige la plantilla `CRUD App with Aurora PostgreSQL` .	Desarrollador de aplicaciones
Instale las dependencias e implemente la aplicación.	1. Desplácese hasta el directorio del proyecto: `cd <your directory>` . 2. Utilice el comando `pnpm i` para instalar las dependencias.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	3. Vaya al directorio infra: `cd infra`. 4. Para implementar la aplicación, ejecute el siguiente comando `pnpm deploy:local` . Se trata de un alias para un comando `cdk deploy ...` definido en `infra/package.json` . Espere a que finalice la implementación (aproxima damente 20 minutos). Mientras espera, supervise las CloudFormation pilas de AWS en la CloudFormation consola. Observe cómo las estructur as definidas en el código se corresponden con el recurso implementado. Revise la vista en árbol de CDK Construct en la CloudFormation consola.	

Tarea	Descripción	Habilidades requeridas
Accede a la aplicación.	Tras implementar su aplicación GB de forma local, puede acceder a ella mediante la CloudFront URL. La URL se imprime en la salida del terminal, pero encontrar la puede resultar un poco abrumador. Siga los pasos siguientes para encontrarlo rápidamente: 1. Abra la terminal en la que ejecutó el comando `pnpm deploy:local` . 2. Busque una sección en la salida del terminal que se parezca al texto siguiente. `myapp5stickbui9C39A55A.CloudFrontDomainName = d1q16n5pof924c.cloudfront.net` La URL será exclusiva para la implementación. Como alternativa, puedes encontrar la CloudFront URL accediendo a la CloudFront consola de Amazon: 1. Inicie sesión en la consola de administración de	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	AWS y navegue hasta el CloudFront servicio. 2. Busque la última distribución implementada en la lista. Copie el nombre de dominio asociado a la distribución. Tendrá un aspecto similar a `your-unique-id.cloudfront.net` .	

Supervisa con Amazon CloudWatch

Tarea	Descripción	Habilidades requeridas
Ver el CloudWatch panel de control.	1. Abre la CloudWatch consola y selecciona Paneles de mandos. 2. Seleccione el panel que tiene el nombre <appId>-<stageName>-dashboard. 3. Revise el panel. ¿Qué recursos se están supervisando? ¿Qué métricas se registran? Este panel es posible gracias a la construcción de código abierto. cdk-monitoring-constructs	Desarrollador de aplicaciones
Habilitar de alertas.	Un CloudWatch panel de control le ayuda a monitorear activamente su aplicación	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	web. Para supervisar de forma pasiva su aplicación web, puede activar las alertas.
	
	1. Navegue hasta `/infra/src/app/stateless/monitor-stack.ts` , que define la pila de monitores.
	2. Elimine los comentarios de la siguiente línea y sustituya `admin@example.com` por su dirección de correo electrónico.
	
	`onAlarmTopic.addSubscription(new EmailSubscription("admin@example.com"));`
	
	3. Añada la información siguiente sobre las importaciones a la parte superior del archivo.
	
	`import { EmailSubscription } from "aws-cdk-lib/aws-sns-subscriptions";`
	
	4. En `infra/`, ejecute el siguiente comando.
	
	`cdk deploy "*/monitor" --exclusively.`
	
	5. Para confirmar su suscripción al tema de SNS que se	

Tarea	Descripción	Habilidades requeridas
	inicia cuando se activa una alarma de monitorización, elija el enlace del mensaje de correo electrónico.	

Comprenda la infraestructura de aplicaciones mediante AWS CDK

Tarea	Descripción	Habilidades requeridas
Cree un diagrama de arquitectura.	Genere un diagrama de arquitectura de su aplicación web mediante cdk-dia. La visualización de la arquitectura ayuda a mejorar la comprensión y la comunicación entre los miembros del equipo. Proporciona una visión general clara de los componentes del sistema y sus relaciones. 1. Instale Graphviz. 2. En `infra/`, ejecute el comando `pnpm cdk-dia`. 3. Ver su `infra/diagram.png` .	Desarrollador de aplicaciones
Use cdk-nag para aplicar las prácticas recomendadas.	Utilice cdk-nag para ayudarle a mantener una infraestructura segura y que cumpla con las normas, aplicando las prácticas recomendadas y reduciendo el riesgo de	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	vulnerabilidades de seguridad y errores de configuración. 1. Conozca las prácticas recomendadas de cdk-nag en su sección de reglas, que incluye las comprobaciones del paquete de reglas de la biblioteca de soluciones de AWS. 2. Para ver cómo cdk-nag aplica las reglas, realice un cambio en el código. Por ejemplo, en `infra/src/app/stateful/data-stacks.ts` , cambie `storageEncrypted: true` a `storageEncrypted: false` . 3. En `infra/`, ejecute el comando `cdk synth "*/data"`. Durante la síntesis, se producirá un error de compilación que indica una infracción de la regla. `AwsSolutions-RDS2: The RDS instance or Aurora DB cluster does not have storage encryption enabled.` Este error muestra cómo cdk-nag es un mecanismo	

Tarea	Descripción	Habilidades requeridas
	de seguridad para aplicar las prácticas recomendadas de infraestructura y evitar errores de configuración de seguridad. 4. Si es necesario, también puede suprimir las reglas en diferentes ámbitos. Por ejemplo, para suprimir AwsSolutions -RDS2, añade el siguiente código debajo de la instanciación de. `DbIamCluster` `NagSuppressions.addResourceSuppressions( cluster.node.findChild("Resource"), [ { id: "AwsSolutions-RDS2", reason: "Customer requirement necessitates having unencrypted DB storage", }, ], );` 5. Tras la supresión, vuelva a ejecutar `cdk synth "*/data"`. Su aplicación AWS CDK ahora debería sintetizarse correctamente. Puede encontrar todas	

Tarea	Descripción	Habilidades requeridas
	las reglas suprimidas en `infra/cdk.out/assembly-<appId>-<stageName>/AwsSolutions-<appId>-<stageName>-${stackId}-NagReport.csv` .	

Evalúe la configuración y el esquema de la base de datos

Tarea	Descripción	Habilidades requeridas
Adquiera variables de entorno.	Para obtener las variables de entorno requeridas, siga los siguientes pasos: 1. Para encontrar el`DB_BASTION_ID` , inicia sesión en la consola y navega hasta ella. EC2 Selecciona Instancias (en ejecución) y busca la fila que contiene - ssm-db-bastion Nombre<stageName>. El Identificador de instancia comienza por i-. 2. Para buscar `DB_ENDPOINT` , en la consola de Amazon Relational Database Service (Amazon RDS), elija Instancias de base de datos y seleccione el clúster regional que tiene un identificador de base de	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	datos que comience por <appId>-<stageName>-data-. Localice el punto de conexión de la instancia de escritura, que termina en rds.amazonaws.com.	
Establezca el reenvío de puertos.	Para establecer el reenvío de puertos, siga estos pasos: 1. Instale el complemento Administrador de sesiones de AWS Systems Manager. 2. Inicie el reenvío de puertos ejecutando `pnpm db:connect` dentro de `core/` para establecer una conexión segura a través del host bastión. 3. Cuando vea el texto `Waiting for connections...,` en su terminal, significa que se ha establecido correctam ente un túnel SSH entre su máquina local y el servidor Aurora a través del host EC2 bastión.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Ajuste el tiempo de espera del Administrador de sesiones de Systems Manager.	(Opcional) Si el tiempo de espera predeterminado de la sesión de 20 minutos es demasiado corto, puede aumentarlo hasta 60 minutos en la consola de Systems Manager seleccionando Administrador de sesiones, Preferencias, Editar, Tiempo de espera de sesión inactiva.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Visualice la base de datos.	pgAdmin es una herramienta de código abierto fácil de usar para administrar bases de datos PostgreSQL. Simplific a las tareas de las bases de datos, lo que le permite crear, administrar y optimizar las bases de datos de manera eficiente. Esta sección le guía a través de la instalación de pgAdmin y el uso de sus funciones para la administr ación de bases de datos PostgreSQL. 1. En el Explorador de objetos, abra el menú contextual (haga clic con el botón derecho) de Servidores y, a continuac ión, seleccione Registrar, Servidor. 2. En la pestaña General, escriba <appId>-< stageName> para el campo Nombre. 3. Para obtener la contraseñ a de la base de datos, abra la consola de AWS Secrets Manager, seleccione el secreto que contenga la descripción Generated by the CDK for the stack: <appId>-<stageName	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	>-data y elija la tarjeta Valor secreto. Seleccione Recuperar Valor secreto y copie el Valor secreto con una clave o contraseña. 4. En la pestaña Conexión, introduzca 0.0.0 para el name/address campo Host y _admin <appId>para el campo Nombre de usuario. Para el campo Contraseña, use el secreto que obtuvo anteriormente. Seleccione Sí en el campo ¿Guardar contraseña?. 5. Seleccione Guardar. 6. Para ver las tablas, vaya a <appId>-<stageName>, Bases de datos, <appId>_db, Esquemas, <appId>, Tablas. 7. Abra el menú contextual (haga clic con el botón derecho) de la tabla de Elementos y, a continuación, seleccione Ver/editar datos, Todas las filas. 8. Explore la tabla.	

Depuración con Node.js

Tarea	Descripción	Habilidades requeridas
Depura el caso práctico de creación de objetos.	Para depuración del caso práctico de creación de elementos, siga estos pasos: 1. Abra el archivo `core/src/modules/item/create-item.use-case.ts` e inserte el siguiente código. 2. El código agregado en el paso anterior garantiza que se llame a la función de `createItemUseCase` cuando este módulo se ejecute directamente.	Desarrollador de aplicaciones

```
import { fileURLTo
Path } from "node:url
";

// existing create-it
em.use-case.ts code
 here

if (process.argv[1]
 === fileURLTo
Path(import.meta.u
rl)) {
  createItemUseCase(
{
    description:
 "Item 1's Descripti
on",
    name: "Item 1",
  });
}
```

Tarea	Descripción	Habilidades requeridas
	Establezca puntos de interrupción en las líneas de este bloque de código en las que desee iniciar la depuración. line-by-line 1. Abre la terminal de JavaScript depuración de VS Code y, a continuación, ejecuta `pnpm tsx core/src/modules/item/create-item.use-case.ts` para ejecutar el código con la depuración. line-by-line Como alternativa, puedes usar `console.log` sentencias, pero las instrucciones impresas pueden resultar inadecuadas cuando trabajas con una lógica empresarial compleja. Line-by-linela depuración te da más contexto.	

Desarrolle el frontend

Tarea	Descripción	Habilidades requeridas
Configure el servidor de desarrollo.	1. Navegue hasta `ui/` y ejecute `pnpm dev` para iniciar el servidor de desarrollo Next.js.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	2. Acceda a su aplicación web de forma local en `http://localhost:3000` . El servidor de desarrollo Next.js está configurado con información instantánea de Fast Refresh sobre las modificaciones realizadas en sus componentes de React. 3. Experimente con la personalización del color de la barra de la aplicación. Abre el archivo `ui/src/components/theme/theme.tsx` y busque la sección que define el tema de la barra de la aplicación. En la sección `colorSchemes.light.palette.primary` , actualice el valor principal de `colors.lagoon` a `colors.carrot` . Tras realizar este cambio, guarde el archivo y observe la actualización en su navegador. 4. Experimente modificando el texto y los componentes y añadiendo nuevas páginas.	

Trabajando con Green Boost

Tarea	Descripción	Habilidades requeridas
Configure monorepo y el administrador de paquetes pnpm.	1. Revise `pnpm-workspace.yaml` en la raíz de su repositorio de GB y observe cómo se definen los espacios de trabajo. Para obtener más información sobre espacios de trabajo, consulte la documentación de pnpm. 2. Revise `ui/package.json` y observe cómo hace referencia al espacio de trabajo `core/` con el nombre de paquete `"<appId>/core": "workspace:^",` . 3. Observe cómo TypeScript se centraliza ESLint la configuración en los paquetes de utilidades definidos en `packages/` él. Esta configuración es utilizada luego por paquetes de aplicaciones como `core/`, `infra/` y `ui/`. Esto resulta útil cuando la aplicación se escala y se definen más paquetes de aplicaciones, que pueden hacer referencia a los paquetes de utilidades	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	sin duplicar el código de configuración.	
Ejecute scripts pnpm.	Ejecute los siguientes comandos en la raíz de su repositorio: 1. Ejecute `pnpm lint`. Este comando ejecuta un análisis de código estático con ESLint. 2. Ejecute `pnpm typecheck`. Este comando ejecuta el TypeScript compilador para comprobar los tipos de código. 3. Ejecute `pnpm test`. Este comando ejecuta Vitest para ejecutar pruebas unitarias. Observe cómo se ejecutan estos comandos en todos los espacios de trabajo. Los comandos se definen en el campo `package.json#scripts` de cada espacio de trabajo.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Se utiliza ESLint para el análisis de código estático.	Para probar la capacidad de análisis de código estático de ESLint, haga lo siguiente:
	
	1. Primero, asegúrese de que la ESLint extensión VS Code (ID:`dbaeumer.vscode-eslint`) esté instalada. También recomendamos instalar VS Code Error Lens (ID: `usernamehw.errorlens`) para ver los errores en línea.
	2. Incluya en el código una línea de código que utilice la función `eval()` como se muestra en el siguiente ejemplo.
	
	``
	const userInput = "import("fs").then((fs) => console.log(fs.readFileSync("/etc/passwd", { encoding: "utf8" })))";
	eval(userInput);
	``
	
	Important
	Esto es solo con fines de prueba. Usar `eval()` se considera potencial mente peligroso
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	y debe evitarse debido a los riesgos de seguridad. 3. Después de incluir la `eval()` línea, abre tu editor de código para confirmar que el ESLint código huele mal con garabatos rojos. 4. Revisa ESLint los complementos y la configuración en `packages/eslint-config-{node,next}/.eslintrc.cjs` .	

Tarea	Descripción	Habilidades requeridas
Gestione las dependencias y vulnerabilidades.	1. Para identificar cualquier vulnerabilidad o exposición común (CVEs), ejecútala `pnpm audit` en la raíz de tu repositorio. Debería ver No se ha encontrado ninguna vulnerabilidad conocida. 2. Instale un paquete intencionalmente vulnerable en `core/` al ejecutar `pnpm add minimist@0.2.3` y, a continuación, ejecute `pnpm audit`. Observe cómo se informa de la vulnerabilidad. 3. Desinstale el paquete vulnerable que contiene `core/` `pnpm remove minimist`al ejecutar .	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Precomete los enlaces con Husky.	1. Realiza un par de pequeños cambios en TypeScript los archivos del repositorio. Los cambios pueden ser tan básicos como añadir comentarios. 2. Organice y confirme estos cambios utilizando `git add -A` y, a continuación, `git commit -m "test husky"`. El activador del enlace Husky previo a la confirmación, que se define en `.husky/pre-commit` , ejecuta el comando `pnpm lint-staged` . 3. Observe cómo lint-staged ejecuta los comandos especificados en los archivos `*/.lintstagedrc.js` de todo el repositorio en archivos que Git ha preparado. Estas herramientas son mecanismos que ayudan a evitar que el código incorrecto llegue a su aplicación.	Desarrollador de aplicaciones

Derribe la infraestructura

Tarea	Descripción	Habilidades requeridas
Elimine la implementación de su cuenta.	1. Para destruir la infraestructura que aprovisionó en la primera epopeya, ejecute `pnpm destroy:local` en `infra/`. 2. Espere 15 minutos después de que `pnpm destroy:local` haya finalizado y, a continuación, elimine la función de Lambda @Edge retenida buscando el identificador de su aplicación en la consola de Lambda. Las funciones Lambda @Edge se replican, lo que dificulta su eliminación. Para obtener más información sobre la eliminación de funciones de Lambda @Edge, consulte la CloudFront documentación.	Desarrollador de aplicaciones

Resolución de problemas

Problema	Solución
No se pudo establecer el reenvío de puertos	Asegúrese de que sus credenciales de AWS estén configuradas correctamente y tengan los permisos necesarios.

Problema	Solución
	Compruebe que las variables de entorno del identificador de host bastión (`DB_BASTIO N_ID `) y del punto de conexión de la base de datos (`DB_ENDPOINT `) estén configuradas correctamente. Si sigue teniendo problemas, consulte la documentación de AWS para solucionar problemas de conexiones SSH y Administrador de sesiones.
Sitio web no está cargando en `localhost :3000`	Confirme que la salida del terminal indica que el reenvío de puertos se ha realizado correctam ente, incluida la dirección de reenvío. Asegúrese de que no haya procesos conflicti vos al utilizar el puerto 3000 de su máquina en las instalaciones. Compruebe que la aplicación Green Boost esté correctamente configurada y ejecutándose en el puerto esperado (3000). Compruebe en su navegador web si hay extensiones o ajustes de seguridad que puedan bloquear las conexiones en las instalacioneses.
Mensajes de error durante la implementación local (`pnpm deploy:local `)	Revise los mensajes de error detenidamente para identificar la causa del problema. Compruebe que las variables de entorno y los archivos de configuración necesarios estén configurados correctamente.

Recursos relacionados

- Documentación de AWS SDK
- Documentación de Green Boost
- Documentación de Next.js
- Documentación de Node.js
- Documentación de React
- TypeScript documentación

Estructure un proyecto de Python en una arquitectura hexagonal con AWS Lambda

Furkan Oruc, Dominik Goby, Darius Kunce y Michal Ploski, Amazon Web Services

Resumen

Este patrón muestra cómo estructurar un proyecto de Python en una arquitectura hexagonal mediante AWS Lambda. El patrón utiliza el AWS Cloud Development Kit (AWS CDK) como herramienta de infraestructura como código (IaC), Amazon API Gateway como REST API y Amazon DynamoDB como capa de persistencia. La arquitectura hexagonal sigue los principios de diseño basados en el dominio. En la arquitectura hexagonal, el software consta de tres componentes: dominio, puertos y adaptadores. Para obtener información detallada sobre las arquitecturas hexagonales y sus ventajas, consulte la guía Creación de arquitecturas hexagonales en AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Experiencia en Python
- Familiaridad con AWS Lambda, AWS CDK, Amazon API Gateway y DynamoDB
- Una GitHub cuenta (consulte las instrucciones para registrarse)
- Git (consulte las instrucciones de instalación)
- Un editor de código para realizar cambios e insertar el código GitHub (por ejemplo, Visual Studio Code o JetBrains PyCharm)
- Docker instalado y el daemon de Docker en funcionamiento

Versiones de producto

- Git versión 2.24.3 o posterior
- Python versión 3.7 o posterior
- AWS CDK v2
- Poetry versión 1.1.13 o posterior
- AWS Lambda Powertools para Python, versión 1.25.6 o posterior
- pytest versión 7.1.1 o posterior

- Moto versión 3.1.9 o posterior
- versión 1.9.0 o posterior de pydantic
- Boto3 versión 1.22.4 o posterior
- mypy-boto3-dynamodb versión 1.24.0 o posterior

Arquitectura

Pila de tecnología de destino

La pila de tecnología de destino consiste en un servicio de Python que utiliza API Gateway, Lambda y DynamoDB. El servicio utiliza un adaptador de DynamoDB para conservar los datos. Proporciona una función que utiliza Lambda como punto de entrada. El servicio usa Amazon API Gateway para exponer una REST API. La API utiliza AWS Identity and Access Management (IAM) para la autenticación de clientes.

Arquitectura de destino

Para ilustrar la implementación, este patrón despliega una arquitectura de destino sin servidor. Los clientes pueden enviar solicitudes a un punto de conexión final de API Gateway. API Gateway reenvía la solicitud a la función de Lambda de destino que implementa el patrón de arquitectura hexagonal. La función de Lambda realiza operaciones de creación, lectura, actualización y eliminación (CRUD) en una tabla de DynamoDB.

> **Important**
>
> Este patrón se probó en un entorno de PoC. Debe realizar una revisión de seguridad para identificar el modelo de amenaza y crear una base de código segura antes de implement ar cualquier arquitectura en un entorno de producción.

La API admite cinco operaciones en una entidad de producto:

- `GET /products` devuelve todos los productos.
- `POST /products` crea un nuevo producto.
- `GET /products/{id}` devuelve un producto específico.

- `PUT /products/{id}` actualiza un producto específico.
- `DELETE /products/{id}` elimina un producto específico.

Puede utilizar la siguiente estructura de carpetas para organizar el proyecto de forma que siga el patrón de arquitectura hexagonal:

```
app/  # application code
|--- adapters/  # implementation of the ports defined in the domain
     |--- tests/  # adapter unit tests
|--- entrypoints/  # primary adapters, entry points
     |--- api/  # api entry point
          |--- model/  # api model
          |--- tests/  # end to end api tests
|--- domain/  # domain to implement business logic using hexagonal architecture
     |--- command_handlers/  # handlers used to execute commands on the domain
     |--- commands/  # commands on the domain
     |--- events/  # events triggered via the domain
     |--- exceptions/  # exceptions defined on the domain
     |--- model/  # domain model
     |--- ports/  # abstractions used for external communication
     |--- tests/  # domain tests
|--- libraries/  # List of 3rd party libraries used by the Lambda function
infra/  # infrastructure code
simple-crud-app.py  # AWS CDK v2 app
```

Tools (Herramientas)

Servicios de AWS

- Amazon API Gateway es un servicio totalmente gestionado que facilita a los desarrolladores la creación, publicación, mantenimiento, supervisión y protección APIs a cualquier escala.
- Amazon DynamoDB es una base de datos NoSQL de valor clave, sin servidor y totalmente gestionada que está diseñada para ejecutar aplicaciones de alto rendimiento a cualquier escala.
- AWS Lambda es un servicio de computación controlado por eventos sin servidor que permite ejecutar código para prácticamente cualquier tipo de aplicación o servicio backend, sin aprovisionar ni administrar servidores. Puede lanzar funciones de Lambda desde más de 200 aplicaciones de software como servicio (SaaS) y pagar solo por lo que utilice.

Herramientas

- Git se utiliza como sistema de control de versiones para el desarrollo de código en este patrón.
- Python se utiliza como lenguaje de programación para este patrón. Python proporciona estructuras de datos de alto nivel y un enfoque de la programación orientada a objetos. AWS Lambda proporciona un tiempo de ejecución de Python integrado que simplifica el funcionamiento de los servicios de Python.
- Visual Studio Code se utiliza como IDE para desarrollar y probar este patrón. Puede usar cualquier IDE que soporte el desarrollo de Python (por ejemplo, PyCharm).
- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software de código abierto que le permite definir los recursos de su aplicación en la nube utilizando lenguajes de programación conocidos. Este patrón utiliza la CDK para escribir e implementar la infraestructura de la nube como código.
- Poetry se utiliza para gestionar las dependencias del patrón.
- AWS CDK utiliza Docker para crear el paquete y la capa de Lambda.

Código

El código de este patrón está disponible en el repositorio de ejemplos de arquitectura hexagonal GitHub Lambda.

Prácticas recomendadas

Para usar este patrón en un entorno de producción, siga estas prácticas recomendadas:

- Utilice las claves administradas por el cliente en AWS Key Management Service (AWS KMS) para cifrar los grupos de CloudWatch registros de Amazon y las tablas de Amazon DynamoDB.
- Configure AWS WAF para Amazon API Gateway para permitir el acceso únicamente desde la red de su organización.
- Considere otras opciones para la autorización de API Gateway si IAM no satisface sus necesidades. Por ejemplo, puede usar grupos de usuarios de Amazon Cognito o autorizadores de Lambda de API Gateway.
- Utilice Copias de seguridad de DynamoDB.
- Configure las funciones de Lambda con una implementación de nube privada virtual (VPC) para mantener el tráfico de red dentro de la nube.
- Actualice la configuración de origen permitida para la verificación previa del intercambio de recursos entre orígenes (CORS) para restringir el acceso únicamente al dominio de origen solicitante.

- Utilice cdk-nag para comprobar las prácticas recomendadas de seguridad en el código de AWS CDK.
- Considere la posibilidad de utilizar herramientas de escaneo de código para detectar problemas de seguridad comunes en el código. Por ejemplo, Bandit es una herramienta diseñada para detectar problemas de seguridad comunes en el código Python. PIP-audit escanea los entornos de Python en busca de paquetes que tengan vulnerabilidades conocidas.

Este patrón utiliza AWS X-Ray para rastrear las solicitudes a través del punto de entrada, el dominio y los adaptadores de la aplicación. AWS X-Ray ayuda a los desarrolladores a identificar los cuellos de botella y determinar las latencias altas para mejorar el rendimiento de las aplicaciones.

Epics

Inicializar el proyecto

Tarea	Descripción	Habilidades requeridas
Cree su propio repositorio.	1. Inicie sesión en. GitHub 2. Cree un nuevo repositorio. Para obtener instrucciones, consulte la documentación de GitHub . 3. Clone e inserte el repositorio de muestras de este patrón en el nuevo repositorio de su cuenta.	Desarrollador de aplicaciones
Instale las dependencias.	1. Instale Poetry. `pip install poetry` 2. Instale los paquetes desde el directorio raíz. El siguiente comando instala la aplicación y los paquetes de AWS CDK. También instala los	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	paquetes de desarrollo necesarios para ejecutar las pruebas unitarias. Todos los paquetes instalados se colocan en un nuevo entorno virtual.
	`poetry install`
	3. Para ver una represent ación gráfica de los paquetes instalados, ejecute el siguiente comando.
	`poetry show --tree`
	4. Actualice todas las dependencias.
	`poetry update`
	5. Abra un nuevo intérpret e de comandos en el entorno virtual recién creado. Contiene todas las dependencias instaladas.
	`poetry shell`	

Tarea	Descripción	Habilidades requeridas
Configure su IDE.	Recomendamos Visual Studio Code, pero puede usar cualquier IDE de su elección que sea compatibl e con Python. Los siguientes pasos son para Visual Studio Code. 1. Actualice el archivo `.vscode/settings` . `{ "python.testing.pytestArgs": [ "app/adapters/tests", "app/entrypoints/api/tests", "app/domain/tests" ], "python.testing.unittestEnabled": false, "python.testing.pytestEnabled": true, "python.envFile": "${workspaceFolder}/.env", }` 2. Cree un archivo `.env` en el directorio raíz del proyecto. Esto garantiza que el directorio raíz del proyecto esté incluido en el directori o `PYTHONPATH` para que	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`pytest` pueda encontrarlo y descubrir correctamente todos los paquetes. `PYTHONPATH=.`	
Ejecute pruebas unitarias, opción 1: utilice Visual Studio Code.	1. Elija el intérprete de Python del entorno virtual gestionado por Poetry. 2. Ejecute las pruebas desde Test Explorer.	Desarrollador de aplicaciones

Ejecute pruebas unitarias, opción 2: utilice comandos del intérprete de comandos.	1. Inicie un nuevo intérprete de comandos en el entorno virtual.
	`poetry shell`
	2. Ejecute el comando `pytest` desde el directorio raíz.
	`python -m pytest`
	Otra posibilidad es ejecutar el comando directamente desde Poetry.
	`poetry run python -m pytest`
		Desarrollador de aplicaciones

Implementar y probar la aplicación

Tarea	Descripción	Habilidades requeridas
Solicite credenciales temporales.	Para tener credenciales de AWS en el intérprete de comandos cuando ejecute `cdk deploy`, cree credencia les temporales mediante AWS IAM Identity Center (sucesor de AWS Single Sign-On). Para obtener instrucciones, consulte la entrada del blog How to retrieve short-term credentials for CLI use with AWS IAM Identity Center.	Desarrollador de aplicaciones, AWS DevOps

Implemente la aplicación .	1. Instale la v2 de AWS CDK.
	`npm install -g aws-cdk`
	Para obtener más informaci ón, consulte la documenta ción de AWS CDK.
	2. Arranque la AWS CDK en su cuenta y región.
	`cdk bootstrap aws://12345678900/ us-east-1 --profile aws-profile-name`
	3. Implemente la aplicación como una CloudFormation pila de AWS mediante un perfil de AWS.
		Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`cdk deploy --profile aws-profile-name`	
Pruebe la API, opción 1: utilice la consola.	Utilice la consola de API Gateway para probar la API. Para obtener más información sobre las operaciones y request/response los mensajes de la API, consulte la sección de uso de la API del archivo readme del GitHub repositorio.	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Pruebe la API, opción 2: utilice Postman.	Si quiere utilizar una herramienta como Postman: 1. Instale Postman como una aplicación independiente o una extensión del navegador. 2. Copie la URL del punto de conexión de la API Gateway. Deberá tener el siguiente formato: `https://{api-id}.execute-api.{region}.amazonaws.com/{stage}/{path}` 3. Configure la firma de AWS en la pestaña de autorización. Para obtener instrucciones, consulte el artículo de AWS Re:post sobre la activación de la autenticación de IAM para API Gateway REST. APIs 4. Utilice Postman para enviar solicitudes al punto de conexión de la API.	Desarrollador de aplicaciones, AWS DevOps

Desarrolle el servicio

Tarea	Descripción	Habilidades requeridas
Redacte pruebas unitarias para el dominio empresarial.	1. Cree un archivo de Python en la carpeta `app/domai`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	n/tests con el prefijo del nombre de archivo test_. 2. Cree un nuevo método de prueba para probar la nueva lógica empresarial mediante el siguiente ejemplo. 3. Cree una clase de comando en la carpeta app/domain/commands.	

```
def test_create_product_should_store_in_repository():
    # Arrange
    command = create_product_command.CreateProductCommand(
        name="Test Product",
        description="Test Description",
    )
    # Act
    create_product_command_handler.handle_create_product_command(
        command=command, unit_of_work=mock_unit_of_work
    )
    # Assert
```

Tarea	Descripción	Habilidades requeridas
	4. Si la funcionalidad es nueva, cree un código auxiliar para el controlador de comandos de la carpeta `app/domain/command_handlers` . 5. Ejecute la prueba unitaria para comprobar si falla, ya que todavía no existe una lógica empresarial. `python -m pytest`	

Tarea	Descripción	Habilidades requeridas

Implemente comandos y controladores de comandos.	1. Implemente la lógica empresarial en el archivo de controlador de comandos recién creado.
	2. Para cada dependencia que interactúe con sistemas externos, declare una clase abstracta en la carpeta `app/domain/ports` .
	
	`class ProductsRepository(ABC):`
	`  @abstractmethod`
	`  def add(self, product: product.Product) -> None:`
	`  ...`
	
	`class UnitOfWork(ABC):`
	`  products: ProductsRepository`
	
	`  @abstractmethod`
	`  def commit(self) -> None:`
	`  ...`
	
	`  @abstractmethod`
	`  def __enter__(self) -> typing.Any:`
	`  ...`
	
	`  @abstractmethod`
	`  def __exit__(self, *args) -> None:`
	`  ...`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	3. Actualice la firma del controlador de comandos para aceptar las dependencias recién declaradas utilizando la clase de puerto abstracta como anotación de tipo.
	
	`def handle_create_product_command(`
	`  command: create_product_command.CreateProductCommand,`
	`  unit_of_work: unit_of_work.UnitOfWork,`
	`) -> str:`
	`  ...`
	
	4. Actualice la prueba unitaria para simular el comportamiento de todas las dependencias declaradas para el controlador de comandos.
	
	`  # Arrange`
	`  mock_unit_of_work = unittest.mock.create_autospec(`
	`  spec=unit_of_work.UnitOfWork, instance=True`
	`  )`
	`  mock_unit_of_work.products = unittest.mock.create_autospec(`	

Tarea	Descripción	Habilidades requeridas

	<pre>spec=unit
	_of_work.ProductsR
	epository, instance=
	True
	)</pre>
	5. Actualice la lógica de aserción en la prueba para comprobar las invocaciones de dependencia esperadas.
	<pre># Assert
	mock_unit
	_of_work.commit.as
	sert_called_once()
	product =
	mock_unit_of_work.
	products.add.call_
	args.args[0]
	
	assertpy.
	assert_that(produc
	t.name).is_equal_t
	o("Test Product")
	assertpy.
	assert_that(produc
	t.description).is_
	equal_to("Test
	Description")</pre>
	6. Ejecute la prueba unitaria para comprobar que funciona correctamente.
	<pre>python -m pytest</pre>	

Tarea	Descripción	Habilidades requeridas
Escriba pruebas de integración para los adaptadores secundarios.	1. Cree un archivo de prueba en la carpeta `app/adapters/tests` utilizando `test_` como prefijo de nombre de archivo. 2. Utilice la biblioteca Moto para simular los servicios de AWS. 3. Cree un nuevo método de prueba para una prueba de integración del adaptador.	Desarrollador de aplicaciones

```
@pytest.fixture
def mock_dynamodb():
   with moto.mock
_dynamodb():
    yield boto3.res
ource("dynamodb",
 region_name="eu-ce
ntral-1")
```

```
def test_add_
and_commit_should_
store_product(mock
_dynamodb):
    # Arrange
    unit_of_work =
 dynamodb_unit_of_w
ork.DynamoDBUnitOf
Work(
        table_nam
e=TEST_TABLE_NAME,
 dynamodb_client=mo
ck_dynamodb.meta.c
lient
    )
    current_time =
 datetime.datetime.
```

Tarea	Descripción	Habilidades requeridas

	now(datetime.timezone.utc).isoformat()
	
	    new_product_id = str(uuid.uuid4())
	    new_product = product.Product(
	        id=new_product_id,
	        name="test-name",
	        description="test-description",
	        createDate=current_time,
	        lastUpdateDate=current_time,
	    )
	
	    # Act
	    with unit_of_work:
	        unit_of_work.products.add(new_product)
	        unit_of_work.commit()
	
	    # Assert
	
	4. Cree una clase de adaptador en la carpeta `app/adapters` . Utilice la clase abstracta de la carpeta de puertos como clase base.	

Tarea	Descripción	Habilidades requeridas
	5. Ejecute la prueba unitaria para ver si falla, porque todavía no hay lógica. `python -m pytest`	

Tarea	Descripción	Habilidades requeridas

Implemente adaptadores secundarios.	1. Implemente la lógica en el archivo de adaptador recién creado.
	2. Actualice las afirmaciones de las pruebas.
	
	`# Assert`
	`    with unit_of_work_readonly:`
	`        product_from_db = unit_of_work_readonly.products.get(new_product_id)`
	
	`    assertpy.assert_that(product_from_db).is_not_none()`
	`    assertpy.assert_that(product_from_db.dict()).is_equal_to(`
	`        {`
	`            "id": new_product_id,`
	`            "name": "test-name",`
	`            "description": "test-description",`
	`            "createDate": current_time,`
	`            "lastUpdateDate": current_time,`
	`        }`
	`    )`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	3. Ejecute la prueba unitaria para comprobar que funciona correctamente. `python -m pytest`	

Tarea	Descripción	Habilidades requeridas
Escribe end-to-end pruebas.	1. Cree un archivo de prueba en la carpeta `app/entry points/api/tests` utilizando `test_` como prefijo de nombre de archivo. 2. Cree un elemento de contexto de Lambda que la prueba utilizará para llamar a Lambda. 3. Cree un método de prueba para la invocación de la API.	Desarrollador de aplicaciones

```
@pytest.fixture
def lambda_co
ntext():
    @dataclass
    class LambdaCon
text:
        function_
name: str = "test"
        memory_li
mit_in_mb: int = 128
        invoked_f
unction_arn: str =
 "arn:aws:lambda:eu
-west-1:809313241:
function:test"
        aws_reque
st_id: str =
 "52fdfc07-2182-154
f-163f-5f0f9a621d7
2"

 return LambdaCon
text()
```

Tarea	Descripción	Habilidades requeridas

	`def test_crea te_product(lambda_ context):`
	`    # Arrange`
	`    name = "TestName"`
	`    description =  "Test description"`
	`    request =  api_model.CreatePr oductRequest(name= name, descripti on=description)`
	
	`    minimal_event =  api_gateway_proxy_ event.APIGatewayPr oxyEvent(`
	`        {`
	`            "path": "/ products",`
	`            "httpMeth od": "POST",`
	`            "requestC ontext": {  #  correlation ID`
	
	`  "requestId":  "c6af9ac6-7b61-11e 6-9a41-93e8deadbee f"`
	`            },`
	`            "body":  json.dumps(request .dict()),`
	`        }`
	`    )`
	
	`    create_pr oduct_func_mock =  unittest.mock.crea te_autospec(`	

Tarea	Descripción	Habilidades requeridas

	<pre>spec=crea
	te_product_command
	_handler.handle_cr
	eate_product_comma
	nd
	)
	handler.c
	reate_product_comm
	and_handler.handle
	_create_product_co
	mmand = (
	create_pr
	oduct_func_mock
	)
	
	# Act
	handler.h
	andler(minimal_eve
	nt, lambda_context)</pre>
	4. Ejecute la prueba unitaria para ver si falla, porque todavía no hay lógica.
	<pre>python -m pytest</pre>	

Tarea	Descripción	Habilidades requeridas

Implemente los adaptadores principales.	1. Cree una función para la lógica empresarial de la API y declare como un recurso de la API.
	
	`@tracer.capture_method`
	`@app.post("/products")`
	`@utils.parse_event(model=api_model.CreateProductRequest, app_context=app)`
	`def create_product(`
	`request: api_model.CreateProductRequest,`
	`) -> api_model.CreateProductResponse:`
	`"""Creates a product."""`
	`...`
	
	Note
	Todos los decoradores que ve son características de la biblioteca AWS Lambda Powertools para Python. Para obtener más información, consulte el sitio web de AWS Lambda
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	Powertools para Python.
	2. Implemente la lógica de la API.
	`id=create_product_command_handler.handle_create_product_command( command=create_product_command.CreateProductCommand( name=request.name, description=request.description, ), unit_of_work=unit_of_work, ) response = api_model.CreateProductResponse(id=id) return response.dict()`
	3. Ejecute la prueba unitaria para comprobar que funciona correctamente.
	`python -m pytest`	

Recursos relacionados

Guía de APG

- Creación de arquitecturas hexagonales en AWS

Referencias de AWS

- Documentación de AWS Lambda
- Documentación de AWS SDK
  - Su primera aplicación de AWS CDK
- Documentación de API Gateway
  - Control del acceso a una API con permisos de IAM
  - Uso de la consola de API Gateway para probar un método de la API de REST
- Documentación de Amazon DynamoDB

Herramientas

- Sitio web git-scm.com
- Instalación de Git
- Crear un GitHub repositorio nuevo
- Sitio web de Python
- AWS Lambda Powertools para Python
- Sitio web de Postman
- Biblioteca de objetos simulados de Python
- Sitio web de Poetry

IDEs

- Sitio web de Visual Studio Code
- PyCharm sitio web

Más patrones

- Acceda a las aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS Fargate PrivateLink, AWS y un Network Load Balancer
- Acceda a las aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS PrivateLink y un Network Load Balancer
- Asociar un AWS CodeCommit repositorio de una cuenta Cuenta de AWS a Amazon SageMaker AI Studio Classic de otra cuenta
- Automatice la eliminación de AWS CloudFormation pilas y recursos asociados
- Restrinja el acceso en función de la dirección IP o la geolocalización mediante AWS WAF
- Cree una aplicación móvil React Native sin servidor con AWS Amplify
- Cree y pruebe aplicaciones iOS con AWS CodeCommit CodePipeline, AWS y AWS Device Farm
- Configure el registro para las aplicaciones.NET en Amazon CloudWatch Logs mediante NLog
- Consolidación de la generación de URL prefirmadas y las descargas de objetos de Amazon S3 mediante un punto de conexión asociado a direcciones IP estáticas
- Cree una definición de tareas de Amazon ECS y monte un sistema de archivos en EC2 las instancias mediante Amazon EFS
- Implemente una aplicación basada en gRPC en un clúster de Amazon EKS y acceda a ella con un Equilibrador de carga de aplicación
- Implemente una ChatOps solución para gestionar los resultados de los escaneos SAST mediante Amazon Q Developer en aplicaciones de chat, acciones personalizadas y CloudFormation
- Despliega canarios de CloudWatch Synthetics con Terraform
- Implementar microservicios de Java en Amazon ECS con AWS Fargate
- Implemente un caso de uso de RAG AWS mediante Terraform y Amazon Bedrock
- Despliega recursos en una AWS Wavelength zona mediante Terraform
- Implementación del control de versiones de API basado en rutas mediante dominios personalizados en Amazon API Gateway
- Migración de una cola de mensajes de Microsoft Azure Service Bus a Amazon SQS
- Migración de una aplicación .NET de Microsoft Azure App Service a AWS Elastic Beanstalk
- Migración de una aplicación web Go en las instalaciones a AWS Elastic Beanstalk mediante el método binario
- Migre un servidor SFTP local para utilizar AWS AWS Transfer for SFTP

- Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2
- Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2 con Auto Scaling
- Migración de aplicaciones Java locales en las instalaciones a AWS mediante AWS App2Container
- Migración de los certificados SSL de Windows a un equilibrador de carga de aplicación mediante ACM
- Supervise la actividad de las aplicaciones mediante CloudWatch Logs Insights
- Ejecute un contenedor Docker de la API web de ASP.NET Core en una instancia de Amazon Linux EC2
- Envío de atributos personalizados a Amazon Cognito e ingesta en los tokens
- Sirva contenido estático en un bucket de Amazon S3 a través de una VPC mediante Amazon CloudFront
- Configure una PeopleSoft arquitectura de alta disponibilidad en AWS
- Simplificación del desarrollo y la implementación de los bots de Amazon Lex mediante un flujo de trabajo automatizado
- Solucione problemas de estados AWS Step Functions mediante Amazon Bedrock
- Uso de Network Firewall para capturar los nombres de dominio de DNS de la indicación del nombre del servidor para el tráfico saliente
- Visualice los resultados del AI/ML modelo con Flask y AWS Elastic Beanstalk

IoT

Temas

- Extraer y consultar atributos de AWS IoT SiteWise metadatos en un lago de datos
- Configuración y solución de problemas de AWS IoT Greengrass con dispositivos cliente
- Más patrones

Extraer y consultar atributos de AWS IoT SiteWise metadatos en un lago de datos

Ambarish Dongaonkar, Amazon Web Services

Resumen

AWS IoT SiteWise utiliza modelos y jerarquías de activos para representar sus equipos, procesos e instalaciones industriales. Cada modelo o activo puede tener varios atributos específicos de su entorno. Los ejemplos de atributos de los metadatos incluyen el sitio o la ubicación física del activo, los detalles de la planta y los identificadores del equipo. Estos valores de atributos complementan los datos de medición de los activos para maximizar el valor empresarial. El machine learning (ML) puede proporcionar información adicional sobre estos metadatos y agilizar las tareas de ingeniería.

Sin embargo, los atributos de los metadatos no se pueden consultar directamente desde el AWS IoT SiteWise servicio. Para que los atributos se puedan consultar, debe extraerlos e incorporarlos a un lago de datos. Este patrón utiliza un script de Python para extraer los atributos de todos los AWS IoT SiteWise activos e incorporarlos a un lago de datos de un bucket de Amazon Simple Storage Service (Amazon S3). Cuando haya completado este proceso, podrá utilizar consultas SQL en Amazon Athena para acceder a los atributos de los AWS IoT SiteWise metadatos y a otros conjuntos de datos, como los conjuntos de datos de medidas. La información de los atributos de los metadatos también es útil cuando se trabaja con AWS IoT SiteWise monitores o paneles. También puede crear un panel de Amazon Quick Sight mediante los atributos extraídos del bucket de Amazon S3.

El patrón tiene un código de referencia y puede implementarlo utilizando los mejores servicios de cómputo para su caso de uso, como AWS Lambda o AWS Glue.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.
- Permisos para configurar AWS Lambda funciones o AWS Glue trabajos.
- Un bucket de Amazon S3.
- Los modelos y jerarquías de activos se configuran en AWS IoT SiteWise. Para obtener más información, consulte Creación de modelos de activos en la AWS IoT SiteWise documentación.

Arquitectura

Puede usar una función Lambda o un AWS Glue trabajo para completar este proceso. Recomendamos usar Lambda si tiene menos de 100 modelos y cada modelo tiene un promedio de 15 atributos o menos. Para todos los demás casos de uso, se recomienda utilizar AWS Glue.

La arquitectura de la solución y el flujo de trabajo se muestran en el siguiente diagrama.

1. Se ejecuta el AWS Glue trabajo programado o la función Lambda. Extrae los atributos de metadatos de los activos AWS IoT SiteWise y los ingiere en un bucket de Amazon S3.
2. Un AWS Glue rastreador rastrea los datos extraídos en el bucket de Amazon S3 y crea tablas en un. AWS Glue Data Catalog
3. Con SQL estándar, Amazon Athena consulta las tablas del AWS Glue Data Catalog.

Automatización y escala

Puede programar la función o el AWS Glue trabajo de Lambda para que se ejecute diaria o semanalmente, según la frecuencia de actualización de las configuraciones de sus AWS IoT SiteWise activos.

La cantidad de AWS IoT SiteWise activos que el código de muestra puede procesar no tiene límite, pero una gran cantidad de activos puede aumentar el tiempo necesario para completar el proceso.

Tools (Herramientas)

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.
- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS IoT SiteWise lo ayuda a recopilar, modelar, analizar y visualizar datos de equipos industriales a escala.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la

capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS SDK para Python (Boto3)es un kit de desarrollo de software que le ayuda a integrar su aplicación, biblioteca o script de Python con Servicios de AWS.

Epics

Configurar el trabajo o la función

Tarea	Descripción	Habilidades requeridas
Configurar los permisos en IAM.	En la consola de IAM, conceda permisos a la función de IAM que asume la función o el AWS Glue trabajo de Lambda para realizar lo siguiente: • Lea del servicio AWS IoT SiteWise • Escriba en el bucket de Amazon S3. Para obtener más informaci ón, consulte Crear roles para un Servicio de AWS en la documentación de IAM.	AWS general
Cree la función o AWS Glue el trabajo de Lambda.	Si utiliza Lambda, cree una función de Lambda nueva. En Tiempo de ejecución, elija Python. Para más informaci ón, consulte Creación de funciones de Lambda con	AWS general

Tarea	Descripción	Habilidades requeridas
	Python en la documentación de Lambda. Si lo está utilizando AWS Glue, cree un nuevo trabajo de shell de Python en la AWS Glue consola. Para obtener más información, consulte Añadir trabajos de shell de Python en la AWS Glue documentación.	
Actualice la función o AWS Glue el trabajo de Lambda.	Modifique la nueva función o AWS Glue trabajo de Lambda e introduzca el ejemplo de código en la sección Información adicional. Modifique el código según sea necesario para su caso de uso. Para obtener más información, consulte Editar código mediante el editor de consola en la documentación de Lambda y consulte Trabajar con scripts en la AWS Glue documentación.	AWS general

Ejecutar el trabajo o la función

Tarea	Descripción	Habilidades requeridas
Ejecute la función o AWS Glue el trabajo de Lambda.	Ejecute la función o AWS Glue el trabajo de Lambda. Para obtener más información, consulte Invocar la función	AWS general

Tarea	Descripción	Habilidades requeridas
	Lambda en la documenta ción de Lambda o consulte Iniciar trabajos mediante activadores en la documenta ción. AWS Glue Esto extrae los atributos de metadatos de los activos y modelos de la AWS IoT SiteWise jerarquía y los almacena en el bucket de Amazon S3 especificado.	
Configure un AWS Glue rastreador.	Configure un AWS Glue rastreador con el clasificador de formatos necesario para un archivo con formato CSV. Utilice los detalles del bucket y el prefijo de Amazon S3 utilizados en la función AWS Glue o el trabajo de Lambda. Para obtener más información, consulte Definir rastreadores en la documentación. AWS Glue	AWS general

Tarea	Descripción	Habilidades requeridas
Ejecute el AWS Glue rastreador.	Ejecute el rastreador para procesar el archivo de datos creado por la función AWS Glue o el trabajo de Lambda. El rastreador crea una tabla en el lugar especificado. AWS Glue Data Catalog Para obtener más información, consulte la sección Cómo iniciar rastreadores mediante activadores en la AWS Glue documentación.	AWS general
Consulte los atributos de los metadatos.	Con Amazon Athena, utilice SQL estándar para realizar consultas AWS Glue Data Catalog según sea necesario para su caso de uso. Puede unir la tabla de atributos de metadatos con otras bases de datos y tablas. Para más información, consulte Introducción en la documenta ción de Amazon Athena.	AWS general

Recursos relacionados

- Documentación de Amazon Athena
- AWS Glue documentación
- AWS IoT SiteWise Referencia de la API
- AWS IoT SiteWise guía de usuario
  - Introducción
  - Crear modelos de activos industriales

  - Definición de relaciones entre los modelos de activos (jerarquías)
  - Asociación y disociación de activos
  - Creación de la AWS IoT SiteWise demostración
- IOTSiteWise (documentación del SDK para Python)
- Documentación de Lambda

Información adicional

Código

El código de ejemplo que se proporciona es de referencia y puede personalizarlo según sea necesario para su caso de uso.

```
# Following code can be used in an AWS Lambda function or in an AWS Glue Python shell
 job.
# IAM roles used for this job need read access to the AWS IoT SiteWise service and
 write access to the S3 bucket.
sw_client = boto3.client('iotsitewise')
s3_client = boto3.client('s3')
output = io.StringIO()

attribute_list=[]
bucket = '{3_bucket name}'
prefix = '{s3_bucket prefix}'
output.write("model_id,model_name,asset_id,asset_name,attribuet_id,attribute_name,attribute_val
\n")

m_resp = sw_client.list_asset_models()
for m_rec in m_resp['assetModelSummaries']:
     model_id = m_rec['id']
     model_name = m_rec['name']

     attribute_list.clear()
     dam_response = sw_client.describe_asset_model(assetModelId=model_id)
     for rec in dam_response['assetModelProperties']:
         if 'attribute' in rec['type']:
            attribute_list.append(rec['name'])

     response = sw_client.list_assets(assetModelId=model_id, filter='ALL')
     for asset in response['assetSummaries']:
```

```
         asset_id = asset['id']
         asset_name = asset['name']
         resp = sw_client.describe_asset(assetId=asset_id)
         for rec in resp['assetProperties']:
            if rec['name'] in attribute_list:
                p_resp = sw_client.get_asset_property_value(assetId=asset_id,
 propertyId=rec['id'])
                if 'propertyValue' in p_resp:
                    if p_resp['propertyValue']['value']:
                        if 'stringValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['stringValue']) + "\n")

                        if 'doubleValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['doubleValue']) + "\n")
                        if 'integerValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['integerValue']) + "\n")
                         if 'booleanValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['booleanValue']) + "\n")

output.seek(0)
s3_client.put_object(Bucket=bucket, Key= prefix + '/data.csv', Body=output.getvalue())
output.close()
```

Configuración y solución de problemas de AWS IoT Greengrass con dispositivos cliente

Marouane Sefiani y Akalanka De Silva, Amazon Web Services

Resumen

AWS IoT Greengrass es un servicio en la nube y de tiempo de ejecución de periferia de código abierto que le ayuda a crear, implementar y administrar software de Internet de las Cosas (IoT) en los dispositivos periféricos. Los casos de uso de AWS IoT Greengrass incluyen:

- Hogares inteligentes en los que se utiliza una puerta de enlace de AWS IoT Greengrass como centro de automatización del hogar
- Fábricas inteligentes donde AWS IoT Greengrass puede facilitar la incorporación y el procesamiento local de datos desde el taller

AWS IoT Greengrass puede actuar como un punto de conexión MQTT seguro y autenticado para otros dispositivos periféricos (también conocidos como dispositivos cliente) que, de otro modo, normalmente se conectarían directamente a AWS IoT Core. Esta capacidad resulta útil cuando los dispositivos cliente no tienen acceso directo a la red del punto de conexión de AWS IoT Core.

Puede configurar AWS IoT Greengrass para su uso con dispositivos cliente en los siguientes casos de uso:

- Para que los dispositivos cliente envíen datos a AWS IoT Greengrass
- Para que AWS IoT Greengrass reenvíe datos a AWS IoT Core
- Para aprovechar las características avanzadas del motor de reglas de AWS IoT Core

Estas capacidades requieren la instalación y configuración de los siguientes componentes en el dispositivo AWS IoT Greengrass:

- Intermediario MQTT
- Puente MQTT
- Autenticación del dispositivo cliente
- Detector de IP

Además, los mensajes publicados desde los dispositivos cliente deben estar en formato JSON o en formato Protocol Buffers (protobuf).

Este patrón describe cómo instalar y configurar estos componentes necesarios y proporciona consejos para la solución de problemas y las prácticas recomendadas.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2
- Dos dispositivos cliente con Python 3.7 o posterior
- Un dispositivo central que ejecute Java Runtime Environment (JRE) versión 8 o posterior y Amazon Corretto 11 u OpenJDK 11

Limitaciones

- Debe elegir una región de AWS en la que esté disponible AWS IoT Core. Para ver la lista actual de regiones de AWS IoT Core, consulte Servicios de AWS por región.
- El dispositivo principal debe tener al menos 172 MB de RAM y 512 MB de espacio en disco.

Arquitectura

El siguiente diagrama muestra la arquitectura de soluciones para este patrón.

La arquitectura incluye:

- Dos dispositivos cliente. Cada dispositivo contiene una clave privada, un certificado de dispositivo y un certificado de la entidad de certificación (CA) raíz. El SDK para dispositivos de AWS IoT, que contiene un cliente MQTT, también está instalado en cada dispositivo cliente.
- Un dispositivo principal que haya implementado AWS IoT Greengrass con los siguientes componentes:
  - Intermediario MQTT
  - Puente MQTT
  - Autenticación del dispositivo cliente

- Detector de IP

Esta arquitectura admite los siguientes escenarios:

- Los dispositivos cliente pueden usar su cliente MQTT para comunicarse entre sí a través del intermediario MQTT del dispositivo principal.
- Los dispositivos cliente también pueden comunicarse con AWS IoT Core en la nube a través del intermediario MQTT del dispositivo principal y el puente MQTT.
- AWS IoT Core en la nube puede enviar mensajes a los dispositivos cliente a través del cliente de prueba MQTT y el puento MQTT y el intermediario MQTT del dispositivo principal.

Para obtener más información sobre las comunicaciones entre los dispositivos cliente y el dispositivo principal, consulte la sección información adicional.

Tools (Herramientas)

Servicios de AWS

- AWS IoT Greengrass es un servicio en la nube y de tiempo de ejecución de borde de Internet de las Cosas (IoT) de código abierto que le ayuda a crear, implementar y administrar aplicaciones de IoT en los dispositivos.
- AWS IoT Core proporciona una comunicación bidireccional segura para que los dispositivos conectados a Internet se conecten a la nube de AWS.
- Los SDK de dispositivos de AWS IoT son un kit de desarrollo de software que contienen bibliotecas de código abierto, guías de desarrolladores con ejemplos y guías de migración para que pueda crear productos o soluciones de IoT innovadores en las plataformas de hardware deseadas.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.

Prácticas recomendadas

- La carga útil de los mensajes de los dispositivos cliente debe estar en formato JSON o Protobuf para aprovechar las características avanzadas del motor de reglas de AWS IoT Core, como la transformación y las acciones condicionales.

- Configure el puente MQTT para permitir la comunicación bidireccional.
- Configure e implemente el componente detector de IP en AWS IoT Greengrass para garantizar que las direcciones IP del dispositivo principal se incluyan en el campo del nombre alternativo del asunto (SAN) del certificado de intermediario de MQTT.

Epics

Configure el dispositivo principal

Tarea	Descripción	Habilidades requeridas
Configurar AWS IoT Greengrass en el dispositivo principal.	Instale el software AWS IoT Greengrass Core siguiendo las instrucciones de la guía para desarrolladores.	AWS IoT Greengrass

Compruebe el estado de la instalación.	Utilice el siguiente comando para comprobar el estado del servicio AWS IoT Greengrass en su dispositivo principal:
	`sudo systemctl status greengrass.service`
	El resultado esperado del comando es:
	`Launched Nucleus successfully`
		AWS general

Configure una política de IAM y asóciela al rol de servicio de Greengrass.	1. Cree una política de IAM para permitir las comunicaciones hacia y desde el puente MQTT. A continuación se muestra un ejemplo de política:	AWS general

Tarea	Descripción	Habilidades requeridas

	<pre>{
	    "Version":
	"2012-10-17",
	    "Statement": [
	
	        {
	            "Effect":
	"Allow",
	            "Action":
	[
	
	"iot:*"
	            ],
	            "Resource
	": "*"
	        },
	        {
	            "Sid":
	"GreengrassActions
	",
	            "Effect":
	"Allow",
	            "Action":
	[
	
	"greengrass:*"
	            ],
	            "Resource
	": "*"
	        }
	    ]
	}</pre> 2. Asocie la política al rol de servicio de Greengras s. Para obtener el rol de servicio, use el comando: <pre>aws greengrassv2
	get-service-role-f</pre>	

Tarea	Descripción	Habilidades requeridas
	`or-account --region <region>` donde `<region>` se refiere a su región de AWS.	
Configure e implemente los componentes necesarios en el dispositivo principal de AWS IoT Greengrass.	Configure e implemente los siguientes componentes: • `greengrass.clientdevices.mqtt.Moquette` (obtener los detalles de configuracion) • `greengrass.clientdevices.mqtt.Bridge` (obtener los detalles de configuración y la siguiente tarea) • `greengrass.clientdevices.Auth` (obtener los detalles de configuración y la tarea luego de la siguiente) • `aws.greengrass.clientdevices.IPDetector` (obtener los detalles de configuracion)	AWS IoT Greengrass

Tarea	Descripción	Habilidades requeridas
Confirme que el puente MQTT permite la comunicación bidireccional.	Para retransmitir mensajes MQTT entre los dispositivos cliente y AWS IoT Core, configure e implemente el componente puente MQTT y especifique los temas que se van a retransmitir. A continuación se muestra un ejemplo: `{ "mqttTopicMapping": { "ClientDevicesToCloud": { "topic": "dt/#", "source": "LocalMqtt", "target": "IotCore" }, "CloudToClientDevices": { "topic": "cmd/#", "source": "IotCore", "target": "LocalMqtt" } } }`	AWS IoT Greengrass

Tarea	Descripción	Habilidades requeridas
Confirme que el componente de autenticación permite a los dispositivos cliente conectarse y publicar temas o suscribirse a ellos.	La siguiente configuración `aws.greengrass.clientdevices.Auth` permite que todos los dispositivos cliente se conecten, publiquen mensajes y se suscriban a todos los temas. `{ "deviceGroups": { "formatVersion": "2021-03-05", "definitions": { "MyPermissiveDeviceGroup": { "selectionRule": "thingName: *", "policyName": "MyPermissivePolicy" } }, "policies": { "MyPermissivePolicy": { "AllowAll": { "statementDescription": "Allow client devices to perform all actions.", "operations": ["*"], "resources": ["*"] } }`	AWS IoT Greengrass

Tarea	Descripción	Habilidades requeridas

	<pre>}
	}
	}</pre>	

Configurar los dispositivos cliente

Tarea	Descripción	Habilidades requeridas
Instalar el SDK para dispositivos con AWS IoT.	Instale el SDK para dispositivos con AWS IoT en los dispositivos cliente. Para obtener una lista completa de los idiomas admitidos y los correspondientes SDKs, consulte la documentación de AWS IoT Core. Por ejemplo, el SDK de dispositivos de AWS IoT para Python se encuentra en GitHub. Para instalar este SDK: 1. Confirme que Python 3.7 o posterior esté instalado , tal y como se indica en la página de requisitos previos del GitHub repositorio. 2. Utilice el comando pip para instalar el SDK. Para macOS y Linux: <pre>python3 -m pip install awsiotsdk</pre>	AWS IoT general

Tarea	Descripción	Habilidades requeridas

	Para Windows:
	`python -m pip install awsiotsdk`
	Como opción, puede instalar el SDK desde el repositorio de origen:
	`# Create a workspace directory to hold all the SDK files`
	`mkdir sdk-workspace`
	`cd sdk-workspace`
	`# Clone the repository`
	`git clone https://github.com/aws/aws-iot-device-sdk-python-v2.git`
	`# Install using Pip (use 'python' instead of 'python3' on Windows)`
	`python3 -m pip install ./aws-iot-device-sdk-python-v2`	

Tarea	Descripción	Habilidades requeridas
Cree un objeto.	1. En la consola de AWS IoT, si aparece un botón Get started (Empezar), elíjalo. De lo contrario, en el panel de navegación, seleccione Security Policies (Políticas de seguridad). 2. Si aparece el cuadro de diálogo You don't have any policies yet (Aún no tiene ninguna política), elija Create a policy (Crear una política). De lo contrario, seleccione Create (Crear). 3. Escriba un nombre para la política de AWS IoT (por ejemplo, `ClientDevicePolicy`). 4. En la sección Add statements (Añadir instrucciones), sustituya la política existente por el siguiente código JSON. Sustituya `<region>` y `<account>` por su región de AWS y su número de cuenta AWS. `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": "iot:Connect",`	AWS IoT Core

Tarea	Descripción	Habilidades requeridas
	"Resource": "arn:aws:iot:region:account:client/*" }, { "Effect": "Allow", "Action": "iot:Publish", "Resource": "*" }, { "Effect": "Allow", "Action": "iot:Receive", "Resource": "*" }, { "Effect": "Allow", "Action": "iot:Subscribe", "Resource": "*" }, { "Effect": "Allow", "Action": ["iot:GetThingShadow", "iot:UpdateThingShadow", "iot:DeleteThingShadow"], "Resource": "arn:aws:iot:region:account:thing/*"	

Tarea	Descripción	Habilidades requeridas

	<pre>}
	]
	}</pre>
	5. Seleccione Crear.
	6. En la consola AWS IoT, en el panel de navegación, seleccione Manage (Administrar), Things (Objetos).
	7. Si aparece el cuadro de diálogo You don't have any things yet (Aún no tiene ningún objeto), elija Register a thing (Registrar un objeto). De lo contrario, seleccione Crear.
	8. En la página Creating AWS IoT things (Creación de objetos de AWS IoT), elija Create a single thing (Crear un solo objeto).
	9. En la página Añadir su dispositivo al registro de dispositivos, escriba un nombre para el objeto de IoT (por ejemplo, `ClientDevice1`) y, a continuación, elija Siguiente .	

Tarea	Descripción	Habilidades requeridas
	Note No puede modificar el nombre de un objeto una vez creado. Para cambiar el nombre,, debe crear otro objeto nuevo, asignarle el nuevo nombre y eliminar después el objeto anterior. 10. En la página Add a certificate for your thing (Añadir un certificado para el objeto), elija Create certificate (Crear certificado). 11. Elija los enlaces Descargar para descargar el certificado, la clave privada y el certificado de CA raíz. **Important** Esta es su única oportunidad para descargar su certificado y su clave privada. 12. Elija Activate (Activar) para activar su certificado. El	

Tarea	Descripción	Habilidades requeridas
	certificado debe estar activo para que un dispositivo se conecte a AWS IoT. 13. Elija Attach a policy (Asociar una política). 14. En Añadir una política para lo tuyo ClientDevicePolicy, selecciona Registrar cosa.	

Tarea	Descripción	Habilidades requeridas
Descargue el certificado de CA del dispositivo principal de Greengrass.	Si espera que el dispositivo principal de Greengrass funcione en entornos fuera de línea, debe poner el certificado de CA principal de Greengrass a disposición del dispositivo cliente para que pueda verificar el certificado del intermediario MQTT (emitido por la CA principal de Greengrass). Por lo tanto, es importante obtener una copia de este certificado. Utilice alguna de los siguientes opciones para descargar el certificado de CA: • Si tiene acceso de red al dispositivo AWS IoT Greengrass desde su PC, acceda a `https://<device IP>:8883` en su navegador web y consulte el certificado de intermediario MQTT y el certificado de CA. También puede guardar el certificado de CA en el dispositivo cliente. • Como opción, puede utilizar la línea de comando OpenSSL:	AWS general

Tarea	Descripción	Habilidades requeridas
	`openssl s_client -showcerts -connect <device IP>:8883`	
Copiar las credenciales en los dispositivos cliente.	Copiar el certificado de CA principal de Greengrass, el certificado del dispositivo y la clave privada en los dispositivos cliente.	AWS general

Tarea	Descripción	Habilidades requeridas
Asociar los dispositivos cliente al dispositivo principal.	Asociar los dispositivos cliente a un dispositivo principal para que puedan detectar el dispositivo principal. A continuación, los dispositivos cliente pueden usar la API de descubrimiento de Greengrass para recuperar la información de conectividad y los certificados de sus dispositivos principales asociados. Para obtener más información, consulte Asociación de dispositivos cliente en la documentación de AWS IoT Greengrass. 1. En la consola de AWS IoT Greengrass, elija Core devices (Dispositivos principales). 2. Elija el dispositivo principal que desee administrar. 3. En la página de detalles del dispositivo principal, elija la pestaña Client devices (Dispositivos cliente). 4. En la sección Associated client devices (Dispositivos cliente asociados), seleccione Associate client devices (Asociar dispositivos cliente).	AWS IoT Greengrass

Tarea	Descripción	Habilidades requeridas
	5. En el modal Associate client devices with core device (Asociar dispositivos cliente a dispositivos principal es), haga lo siguiente para cada dispositivo cliente que desee asociar: a. Introduzca el nombre del objeto de AWS IoT que desee asociar como dispositivo cliente. b. Elija Add (Añadir). 6. Elija Associate (Asociar). Los dispositivos cliente que asoció ahora pueden usar la API de detección de Greengrass para detectar este dispositivo principal.	

Envíe y reciba datos

Tarea	Descripción	Habilidades requeridas
Enviar datos de un dispositivo cliente a otro dispositivo cliente.	Utilice el cliente MQTT de su dispositivo para publicar un mensaje sobre el tema `dt/client1/sensor` .	AWS general
Envíe datos desde el dispositivo cliente a AWS IoT Core.	Utilice el cliente MQTT de su dispositivo para publicar un mensaje sobre el tema `dt/client1/sensor` .	AWS general

Tarea	Descripción	Habilidades requeridas
	En el cliente de prueba de MQTT, suscríbase al tema sobre el que el dispositivo está enviando mensajes o suscríbase a # para todos los temas (consulte los detalles).	
Enviar mensajes desde AWS IoT Core a dispositivos cliente.	En la página del cliente de prueba de MQTT, en la pestaña Publish to a topic (Publicar en un tema), en el campo Topic name (Nombre del tema), introduzca el nombre del tema de su mensaje. En este ejemplo, utilice `cmd/client1` para el tema.	AWS general

Resolución de problemas

Problema	Solución
No se pudo verificar el error del certificado del servidor	Este error se produce cuando el cliente MQTT no puede verificar el certificado presentado por el intermediario MQTT durante el protocolo de enlace TLS. La razón más común es que el cliente MQTT no tiene el certificado de CA. Siga estos pasos para asegurarse de que el certificado de CA se proporciona al cliente MQTT. 1. Si tiene acceso de red al dispositivo AWS IoT Greengrass desde su PC, acceda a `https://<device IP>:8883` en una ventana de navegador para consulte el

Problema	Solución

	certificado de intermediario MQTT y el certificado de CA. También puede guardar el certificado de CA en el dispositivo cliente.
	
	Como opción, puede utilizar la línea de comando OpenSSL:
	
	`openssl s_client -showcerts -connect <device IP>:8883`
	
	2. Guardar el contenido de los certificados Moquette CA y Greengrass Core CA en archivos y, a continuación, visualizar el contenido decodificado mediante el comando:
	
	`openssl x509 -in <Name of CA>.pem -text`
	
	El certificado CA de Moquette debe mostrar el campo SAN, como en este ejemplo:
	
	`X509v3 Subject Alternative Name: IP Address:XXX.XXX.XXX.XXX, IP Address:127.0.0.1, DNS:localhost`

Problema	Solución
No se pudo verificar el error del nombre del servidor	Este error se produce cuando el cliente MQTT no puede comprobar que se está conectando al servidor correcto. La razón más común es que la dirección IP del dispositivo Greengrass no aparece en el campo SAN del certificado. Siga las instrucciones de la solución anterior para obtener el certificado de intermediario MQTT y compruebe que el campo SAN contiene la dirección IP del dispositivo AWS IoT Greengrass, tal y como se explica en la sección Información adicional. Si no es así, confirme que el componente del detector de IP está instalado correctamente y reinicie el dispositivo principal.
No se puede verificar el nombre del servidor solo cuando se conecta desde un dispositivo cliente integrado	Mbed TLS, que es una biblioteca TLS popular que se utiliza en los dispositivos integrado s, actualmente solo admite la verificación de nombres DNS en el campo SAN del certificado, como se muestra en el código de la bibliotec a Mbed TLS. Como el dispositivo principal no tiene su propio nombre de dominio y depende de la dirección IP, los clientes de TLS que utilizan Mbed TLS no pasarán la verificación del nombre del servidor durante el protocolo de enlace TLS, lo que provocará un fallo de conexión. Recomendamos que añada la verificación de la dirección IP de SAN a la biblioteca Mbed TLS en la función x509_crt_ check_san.

Recursos relacionados

- Documentación de AWS IoT Greengrass
- Documentación de AWS IoT Core de AWS IoT Core
- Componente intermediario MQTT
- Componente puente MQTT
- Componente de autenticación del dispositivo cliente
- Componente detector de IP
- SDK de dispositivos AWS IoT
- Implementación de dispositivos de clientes locales con AWS IoT Greengrass (entrada del blog de AWS)
- RFC 5280: perfil del certificado de infraestructura de clave pública X.509 de Internet y de la lista de revocación de certificados (CRL)

Información adicional

Esta sección ofrece información adicional sobre las comunicaciones entre los dispositivos cliente y el dispositivo principal.

El intermediario MQTT escucha en el puerto 8883 del dispositivo principal los intentos de conexión con un cliente TLS. En la siguiente ilustración se muestra un ejemplo de un certificado de servidor de intermediario MQTT.

El certificado de ejemplo muestra los siguientes detalles:

- El certificado lo emite la CA principal de AWS IoT Greengrass, que es local y específica del dispositivo principal; es decir, actúa como una CA local.
- El componente de autenticación del cliente rota automáticamente este certificado cada semana, como se muestra en la siguiente ilustración. Puede establecer este intervalo en la configuración del componente de autenticación del cliente.

- El nombre alternativo del asunto (SAN) desempeña un papel fundamental en la verificación del nombre del servidor por parte del cliente TLS. Ayuda al cliente TLS a garantizar que se conecta al

servidor correcto y ayuda a evitar man-in-the-middle ataques durante la configuración de la sesión TLS. En el certificado de ejemplo, el campo SAN indica que este servidor escucha en localhost (el conector de dominio Unix local) y que la interfaz de red tiene la dirección IP 192.168.1.12.

El cliente TLS utiliza el campo SAN del certificado para comprobar que se está conectando a un servidor legítimo durante la verificación del servidor. Por el contrario, durante un protocolo de enlace TLS típico entre un servidor HTTP y un navegador, el nombre de dominio del campo del nombre común (CN) o del campo SAN se utiliza para comprobar el dominio al que se está conectando realmente el navegador durante el proceso de verificación del servidor. Si el dispositivo principal no tiene un nombre de dominio, la dirección IP incluida en el campo SAN sirve para el mismo propósito. Para obtener más información, consulte la sección Nombre alternativo del asunto de RFC 5280: perfil del certificado de infraestructura de clave pública X.509 de Internet y de la lista de revocación de certificados (CRL).

El componente detector de IP de AWS IoT Greengrass garantiza que se incluyan las direcciones IP correctas en el campo SAN del certificado.

El certificado del ejemplo lo firma el dispositivo AWS IoT Greengrass que actúa como CA local. El cliente TLS (cliente MQTT) no conoce esta CA, por lo que debemos proporcionar un certificado de CA similar al siguiente.

Más patrones

- Capturar datos de IoT directamente en Amazon S3 de forma rentable con AWS IoT Greengrass
- Implementación de sistemas de agentes en Amazon Bedrock con el marco CrewAI mediante Terraform
- Implemente aplicaciones en contenedores si se AWS IoT Greengrass V2 ejecutan como un contenedor Docker

&Modernización de migración

Temas

- Migración
- Modernización
- Unidades centrales

Migración

Temas

- Reinicie automáticamente el AWS El agente de replicación tras un reinicio de RHEL sin deshabilitar SELinux
- Cree CloudFormation plantillas de AWS para las tareas de AWS DMS con Microsoft Excel y Python
- Introducción a la detección automática de cartera
- Migración de cargas de trabajo de Cloudera en las instalaciones a la plataforma de datos de Cloudera en AWS
- Resolver los errores de conexión después de migrar Microsoft SQL Server a la nube de AWS
- Rediseñar
- Volver a alojar
- Reubicar
- Redefinir la plataforma
- Patrones de migración por carga de trabajo
- Más patrones

Reinicie automáticamente el AWS El agente de replicación tras un reinicio de RHEL sin deshabilitar SELinux

Anil Kunapareddy, Amazon Web Services

Resumen

AWS Transform MGN ayuda a simplificar, acelerar y automatizar la migración de las cargas de trabajo de Red Hat Enterprise Linux (RHEL) a la nube de Amazon Web Services (AWS). Para añadir servidores de origen a MGN, instale el agente de AWS replicación en los servidores.

MGN proporciona una replicación asincrónica a nivel de bloque en tiempo real. Esto significa que puede continuar con las operaciones de TI normales durante todo el proceso de replicación. Estas operaciones de TI pueden requerir que reinicie o reinicie el servidor de origen de RHEL durante la migración. Si esto ocurre, el agente de AWS replicación no se reiniciará automáticamente y la replicación de los datos se detendrá. Por lo general, puede configurar Security-Enhanced Linux (SELinux) en modo deshabilitado o permisivo para reiniciar automáticamente el agente de replicación. AWS Sin embargo, es posible que las políticas de seguridad de su organización prohíban la desactivación de SELinux y que también tenga que volver a etiquetar sus archivos.

Este patrón describe cómo reiniciar automáticamente el agente de AWS replicación sin apagar SELinux cuando el servidor de origen de RHEL se reinicia o se reinicia durante una migración.

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- Una carga de trabajo de RHEL local a la que desee migrar. Nube de AWS
- MGN se inicializó desde la consola de MGN. La inicialización solo es necesaria la primera vez que utilice este servicio. Para obtener instrucciones, consulte la documentación de MGN.
- Una política AWS Identity and Access Management (IAM) existente para MGN. Para obtener más información, consulte la documentación de MGN.

Versiones

- RHEL versión 7 o posterior

Arquitectura

La siguiente imagen muestra la arquitectura de este enfoque.

Tools (Herramientas)

Servicios de AWS

- AWS Transform MGNes una solución de elevación y traslado (realojamiento) altamente automatizada que simplifica, agiliza y reduce el costo de la migración de aplicaciones a. AWS

Comandos de Linux

La siguiente tabla proporciona una lista de los comandos de Linux que se ejecutan en el servidor fuente de RHEL. Estos también se describen en las epics y las historias de este patrón.

Comando	Descripción
`#systemctl –version`	Identifica la versión del sistema
`#systemctl list-units --type=service`	Muestra todos los servicios activos que están disponibles en el servidor RHEL
`#systemctl list-units --type=service | grep running`	Muestra todos los servicios que se están ejecutando actualmente en el servidor RHEL
`#systemctl list-units --type=service | grep failed`	Muestra todos los servicios que no se pudieron cargar después de que el servidor RHEL se reiniciara o se reiniciara
`#restorecon -Rv /etc/rc.d/init.d/aws-replication-service`	Cambia el contexto a `aws-replication-service`
`#yum install policycoreutils*`	Instala las utilidades principales de la política necesarias para el funcionamiento del sistema SELinux
`#ausearch -c "insmod" --raw | audit2allow -M my-modprobe`	Busca en el registro de auditoría y crea un módulo para las políticas

`#semodule -i my-modprobe.pp`	Activa la política
`#cat my-modprobe.te`	Muestra el contenido del `my-modprobe.te` archivo
`#semodule -l | grep my-modprobe`	Comprueba si la política se ha cargado en el módulo SELinux

Epics

Instala la AWS Agente de replicación y reinicie el servidor de origen de RHEL

Tarea	Descripción	Habilidades requeridas
Genere credenciales AWS temporales.	Las credenciales temporales proporcionadas por MGN utilizan un mecanismo similar al utilizado por AWS Identity and Access Management Roles Anywhere. Para crear credenciales temporales, debe: 1. Cree un nuevo rol de IAM con la `AWSApplicationMigrationAgentInstallationPolicy` política. 2. Solicita credenciales de seguridad temporales mediante AWS Security Token Service (AWS STS) mediante la AssumeRole API.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	Puede generar credencia les temporales mediante AWS Command Line Interface (AWS CLI). Para ver un ejemplo, consulte la Referencia de AWS CLI comandos.	
Instale el agente AWS de replicación.	1. Inicie sesión en la AWS Transform MGN consola Consola de administración de AWS y ábrala. 2. Configure los ajustes de replicación siguiendo las instrucciones de la documentación de MGN. 3. Instale el agente de AWS replicación siguiendo las instrucciones de la documentación de MGN. 4. En la página Servidores de origen, elija el servidor de origen de RHEL y, a continuación, elija Replicaci ón para iniciar la replicaci ón inicial. Para obtener más información, consulte la documentación de MGN.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Compruebe el estado de la replicación de los datos.	Espere a que se complete la replicación y, a continuación, compruebe el estado de la replicación de datos en el panel de migración. Debería estar como En buen estado.	Ingeniero de migraciones
Reinicie o resetee el servidor de origen de RHEL.	Reinicie o resetee el servidor de origen de RHEL. Observe que el estado de la replicación de datos aparece como Estancado en el panel de migración.	Ingeniero de migraciones

Compruebe la AWS El estado del agente de replicación en el servidor de origen de RHEL

Tarea	Descripción	Habilidades requeridas
Identifica la versión del sistema.	Abra la interfaz de la línea de comandos del servidor fuente de RHEL y ejecute el siguiente comando para identificar la versión del sistema: `#systemctl –version`	Ingeniero de migraciones
Enumere todos los servicios activos.	Para ver todos los servicios activos disponibles en el servidor RHEL, ejecute el siguiente comando: `#systemctl list-units --type=service`	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Enumere todos los servicios en ejecución.	Para enumerar todos los servicios que se están ejecutando actualmente en el servidor RHEL, utilice el siguiente comando: `#systemctl list-units --type=service | grep running`	Ingeniero de migraciones
Enumere todos los servicios que no se pudieron cargar.	Para mostrar todos los servicios que no se pudieron cargar después de que el servidor RHEL se reiniciar a o se reiniciara, ejecute el comando: `#systemctl list-units --type=service | grep failed`	Ingeniero de migraciones

Cree y ejecute el módulo SELinux

Tarea	Descripción	Habilidades requeridas
Cambie el contexto de seguridad.	En la interfaz de línea de comandos del servidor de origen de RHEL, ejecute el siguiente comando para cambiar el contexto de seguridad al servicio de AWS replicación:	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	`#restorecon -Rv /etc/rc.d/init.d/aws-replication-service`	
Instale las utilidades principales.	Para instalar las utilidades principales necesarias para el funcionamiento del sistema SELinux y sus políticas, ejecute el siguiente comando: `#yum install policycoreutils*`	Ingeniero de migraciones
Busca el registro de auditoría y crea un módulo para las políticas.	Use el siguiente comando: `#ausearch -c "insmod" --raw | audit2allow -M my-modprobe`	Ingeniero de migraciones
Muestra el contenido del archivo. `my-modprobe-te`	El archivo **`my-modprobe.te`** se genera mediante el comando audit2allow. Incluye los dominios de SELinux, el directorio de fuentes de políticas y los subdirectorios, y especifica las reglas y transiciones de los vectores de acceso asociadas a los dominios. Para mostrar el contenido del archivo, ejecute el siguiente comando: `#cat my modprobe.te`	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Activa la política.	Para insertar el módulo y activar el paquete de políticas, ejecute el siguiente comando: `#semodule -i my-modprobe.pp`	Ingeniero de migraciones
Compruebe si el módulo se ha cargado.	Use el siguiente comando: `#semodule -l | grep my-modprobe` Una vez cargado el módulo SELinux, ya no tendrá que configurar SELinux en modo deshabilitado o permisivo durante la migración.	Ingeniero de migraciones
Reinicie o resetee el servidor de origen de RHEL y compruebe el estado de la replicación de los datos.	Abra la AWS Transform MGN consola, vaya a Progreso de la replicación de datos y, a continuación, reinicie o reinicie el servidor fuente de RHEL. La replicación de datos ahora debería reanudarse automáticamente después de que se reinicie el servidor de origen de RHEL.	Ingeniero de migraciones

Recursos relacionados

- Documentación de MGN
- Políticas de MGN
- Materiales de formación técnica
- Solución de problemas con el agente de AWS replicación

Cree CloudFormation plantillas de AWS para las tareas de AWS DMS con Microsoft Excel y Python

Venkata Naveen Koppula, Amazon Web Services

Resumen

Este patrón describe los pasos para crear automáticamente CloudFormation plantillas de AWS para AWS Database Migration Service (AWS DMS) mediante Microsoft Excel y Python.

La migración de bases de datos mediante AWS DMS suele implicar la creación de CloudFormation plantillas de AWS para aprovisionar las tareas de AWS DMS. Anteriormente, la creación de CloudFormation plantillas de AWS requería conocimientos del lenguaje de programación JSON o YAML. Con esta herramienta, solo necesita conocimientos básicos de Excel y de cómo ejecutar un script de Python mediante una terminal o una ventana de comandos.

Como entrada, la herramienta utiliza un libro de trabajo de Excel que incluye los nombres de las tablas que se van a migrar, los nombres de los recursos de Amazon (ARNs) de los puntos de enlace de AWS DMS y las instancias de replicación de AWS DMS. A continuación, la herramienta genera CloudFormation plantillas de AWS para las tareas de AWS DMS necesarias.

Para ver los pasos detallados y la información básica, consulte la entrada del blog Crear CloudFormation plantillas de AWS para tareas de AWS DMS con Microsoft Excel en el blog AWS Database.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Microsoft Excel versión 2016 o posterior
- Python versión 2.7 o posterior
- El módulo Python xlrd (instalado en una línea de comandos con el comando: pip install xlrd)
- Puntos de conexión de origen y destino de AWS DMS e instancia de replicación de AWS DMS

Limitaciones

- Los nombres de los esquemas, las tablas y las columnas asociadas se transforman en minúsculas en los puntos de conexión de destino.

- Esta herramienta no aborda la creación de instancias de replicación y puntos de conexión de AWS DMS.
- Actualmente, la herramienta solo admite un esquema para cada tarea de AWS DMS.

Arquitectura

Pila de tecnología de origen

- Base de datos en las instalaciones
- Microsoft Excel

Pila de tecnología de destino

- CloudFormation Plantillas de AWS
- Una base de datos en la nube de AWS

Arquitectura

Tools (Herramientas)

- Pycharm IDE o cualquier entorno de desarrollo integrado (IDE) compatible con Python versión 3.6
- Microsoft Office 2016 (para Microsoft Excel)

Epics

Configurar la red, la instancia de replicación de AWS DMS y los puntos de conexión

Tarea	Descripción	Habilidades requeridas
Si es necesario, solicite un aumento de cuota de servicio.	Solicite un aumento de cuota de servicio para las tareas de AWS DMS si es necesario.	AWS general
Configure la región de AWS, las nubes privadas virtuales		AWS general

Tarea	Descripción	Habilidades requeridas
(VPCs), los rangos de CIDR, las zonas de disponibilidad y las subredes.		
Configure la instancia de replicación de AWS DMS.	La instancia de replicación de AWS DMS puede conectarse tanto a bases de datos en las instalaciones como de AWS.	AWS general
Configure los puntos de conexión de AWS DMS.	Configure los puntos de conexión para las bases de datos de origen y de destino.	AWS general

Preparación de las hojas de trabajo para las tareas y etiquetas de AWS DMS

Tarea	Descripción	Habilidades requeridas
Configure la lista de tablas.	Enumere todas las tablas implicadas en la migración.	Base de datos
Prepare la hoja de trabajo de tareas.	Prepare la hoja de cálculo de Excel con la lista de tablas que configuró.	AWS general, Microsoft Excel
Prepare la hoja de trabajo sobre las etiquetas.	Detalle las etiquetas de recursos de AWS que se deben adjuntar a las tareas de AWS DMS.	AWS general, Microsoft Excel

Descargar y ejecutar la herramienta

Tarea	Descripción	Habilidades requeridas
Descargue y extraiga la herramienta de generación de	GitHub repositorio: https://github.com/aws-samples/dms-	

Tarea	Descripción	Habilidades requeridas
plantillas del GitHub repositor io.	cloudformation-templates-gen erator/	
Ejecute la herramienta.	Siga las instrucciones detalladas de la entrada del blog que aparece en la sección "Referencias y ayuda".	

Recursos relacionados

- Cree CloudFormation plantillas de AWS para tareas de AWS DMS con Microsoft Excel (entrada del blog)
- Generador de CloudFormation plantillas de DMS (repositorio) GitHub
- Documentación de Python
- Descripción y descarga en xlrd
- Documentación de AWS DMS
- CloudFormation Documentación de AWS

Introducción a la detección automática de cartera

Pratik Chunawala y Rodolfo Jr. Cerrada, Amazon Web Services

Resumen

Evaluar la cartera y recopilar metadatos es un desafío fundamental al migrar aplicaciones y servidores a la nube de Amazon Web Services (AWS), especialmente en el caso de migraciones grandes con más de 300 servidores. El uso de una herramienta automatizada de detección de cartera puede ayudarle a recopilar información sobre sus aplicaciones, como la cantidad de usuarios, la frecuencia de uso, las dependencias y la información sobre la infraestructura de la aplicación. Esta información es esencial a la hora de planificar oleadas de migración, ya que le permite priorizar y agrupar adecuadamente las aplicaciones con características similares. El uso de una herramienta de detección agiliza la comunicación entre el equipo de cartera y los propietarios de las aplicaciones, ya que el equipo de cartera puede validar los resultados de la herramienta de detección en lugar de recopilar los metadatos manualmente. En este patrón se analizan las consideraciones clave a la hora de seleccionar una herramienta de detección automatizada, y se ofrece información sobre cómo implementar y probar una en su entorno.

Este patrón incluye una plantilla que le servirá como punto de partida para crear su propia lista de verificación de actividades de alto nivel. Junto a la lista de verificación encontrará una plantilla para crear una matriz responsable, fiable, consultada y fundamentada (RACI). Puede usar esta matriz RACI para determinar quién es responsable de cada tarea de su lista de verificación.

Epics

Selección una herramienta de detección

Tarea	Descripción	Habilidades requeridas
Determine si una herramien ta de detección es apropiada para su caso de uso.	Es posible que una herramien ta de detección no sea la mejor solución para su caso de uso. Tenga en cuenta la cantidad de tiempo que necesitará para seleccion ar, adquirir, preparar e implementar una herramienta	Líder de migración, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	de detección. La configuración del dispositivo de escaneo para una herramienta de detección sin agente en su entorno, o la instalación de agentes en todas las cargas de trabajo incluidas en el ámbito de aplicación, puede llevar de 4 a 8 semanas. Una vez implementada, la herramienta de detección tardará de 4 a 12 semanas en recopilar los metadatos escaneando las cargas de trabajo de las aplicaciones y realizar un análisis del conjunto de aplicaciones. Si va a migrar menos de 100 servidores, es posible que pueda recopilar los metadatos manualmente y analizar las dependencias en menos tiempo del que tardaría en implementar y recopilar los metadatos con una herramien ta de detección automatizada.	

Tarea	Descripción	Habilidades requeridas
Selección una herramientas de detección.	Consulte las Considera ciones para seleccionar una herramienta de detección automática en la sección Información adicional. Determine los criterios adecuados para seleccionar una herramienta de detección para su caso de uso y, a continuación, evalúe cada herramienta en función de dichos criterios. Para obtener una lista completa de herramientas de detección automatizadas, consulte Herramientas de detección , planificación y migración recomendadas.	Líder de migración, ingeniero de migraciones

Preparación para la instalación

Tarea	Descripción	Habilidades requeridas
Prepare la lista de verificación previa a la implementación.	Cree una lista de verificac ión con las tareas que debe completar antes de implement ar la herramienta. Para ver un ejemplo, consulte la Lista de verificación previa a la implementación en el sitio web de documentación de Flexera.	Responsable de compilación, ingeniero de migraciones, líder de migración, administrador de red

Tarea	Descripción	Habilidades requeridas
Prepare los requisitos de la red.	Aprovisione los puertos, protocolos, direcciones IP y enrutamiento necesarios para que la herramienta se ejecute y acceda a los servidores de destino. Para obtener más información, consulte la guía de instalación de su herramienta de detección. Para ver un ejemplo, consulte la Requisitos para la implementación en el sitio web de documentación de Flexera.	Ingeniero migraciones, administrador de redes, arquitecto de la nube
Prepare los requisitos de cuenta y credenciales.	Identifique las credenciales que necesita para acceder a los servidores de destino e instalar todos los componentes de la herramienta.	Administrador de la nube, AWS general, ingeniero de migraciones, líder de migración, administrador de redes, administrador de AWS
Prepare los dispositivos en los que va a instalar la herramienta.	Asegúrese de que los dispositivos en los que va a instalar los componentes de la herramienta cumplen las especificaciones y los requisitos de plataforma de la herramienta.	Ingeniero de migraciones, ingeniero de migraciones, líder de migraciones, administrador de red
Prepare las órdenes de cambio.	Siguiendo el proceso de gestión de cambios de su organización, prepare las órdenes de cambio necesarias y asegúrese de que se aprueben.	Responsable de compilación, líder de migración

Tarea	Descripción	Habilidades requeridas
Envíe los requisitos a las partes interesadas.	Envíe la lista de verificación previa a la implementación y los requisitos de red a las partes interesadas. Las partes interesadas deben revisar, evaluar y preparar los requisitos necesarios antes de proceder con la implementación.	Responsable de compilación, líder de migración

Implemente la herramienta

Tarea	Descripción	Habilidades requeridas
Descargue el instalador.	Descargue el instalador o la imagen de máquina virtual. Las imágenes de máquinas virtuales suelen estar en formato de virtualización abierta (OVF).	Responsable de compilación, líder de migración
Extraiga los archivos.	Si usa un instalador, debe descargarlo y ejecutarlo en un servidor en las instalaciones.	Responsable de compilación, líder de migración
Implemente la herramienta en los servidores.	Implemente la herramienta de detección en los servidores de destino en las instalaciones de la siguiente manera: • Si el archivo fuente es una imagen de máquina virtual, impleméntelo en su entorno de máquina virtual, por ejemplo VMware.	Responsable de compilación, líder de migración, administrador de red

Tarea	Descripción	Habilidades requeridas
	• Si el archivo de origen es un instalador, ejecútelo para instalar y configurar la herramienta.	
Inicie sesión en la herramienta de detección.	Siga las indicaciones que aparecen en pantalla e inicie sesión para usar la herramienta.	Líder de migración, responsable de compilación
Active el producto.	Introduzca su clave de licencia.	Responsable de compilación, líder de migración
Configure la herramienta.	Introduzca las credenciales necesarias para acceder a los servidores de destino, como las credenciales de Windows VMware, el Protocolo simple de administración de redes (SNMP) y el Protocolo Secure Shell (SSH), o las bases de datos.	Responsable de compilación, líder de migración

Pruebe la herramienta

Tarea	Descripción	Habilidades requeridas
Seleccione los servidores de prueba.	Identifique un conjunto pequeño de subredes o direcciones IP que no sean de producción y que pueda usar para probar la herramienta de detección. Esto le ayudará a validar los escaneos rápidamente, identificar y	Responsable de compilación, líder de migración, administrador de red

Tarea	Descripción	Habilidades requeridas
	solucionar cualquier error con prontitud y aislar las pruebas de los entornos de producción.	
Comience a escanear los servidores de prueba seleccionados.	Si usa una herramienta de detección sin agente, introduzca las subredes o direcciones IP de los servidores de prueba seleccionados en la consola de la herramienta de detección e inicie el escaneo. Si usa una herramienta de detección basada en agente, instale el agente en los servidores de prueba seleccionados.	Responsable de compilación, líder de migración, administrador de red
Revise los resultados escaneados.	Revise los resultados del escaneo de los servidores de prueba. Si encuentra algún error, corríjalo. Documente los errores y las soluciones. Puede hacer referencia a esta información en el futuro y añadirla al manual de procedimientos de su cartera.	Responsable de compilación, líder de migración, administrador de red
Vuelva a escanear los servidores de prueba.	Una vez completado el rescaneo, repítalo hasta que no surjan errores.	Responsable de compilación, líder de migración, administrador de red

Recursos relacionados

AWS resources

- Guía de evaluación de la cartera de aplicaciones para la migración Nube de AWS
- Herramientas de detección, planificación y migración recomendadas

Guías de implementación para las herramientas de detección más comunes

- Implemente el dispositivo virtual RN15 0 (documentación de Flexera)
- Instalación de Gatherer (documentación de ModelizeIT)
- Instalación de On-Prem Analysis Server (documentación de ModelizeIt)

Información adicional

Consideraciones para seleccionar una herramienta de detección automatizada

Cada herramienta de detección tiene sus ventajas y limitaciones. A la hora de seleccionar la herramienta adecuada para su caso de uso, tenga en cuenta lo siguiente:

- Seleccione una herramienta de detección que pueda recopilar la mayoría, si no todos, de los metadatos que necesita para alcanzar el objetivo de evaluación de su cartera.
- Identifique los metadatos incompatibles con la herramienta que necesite recopilar manualmente.
- Comunique los requisitos de la herramienta de detección a las partes interesadas para que puedan revisarla y evaluarla en función de sus necesidades internas de seguridad y conformidad, como los requisitos de servidor, red y credenciales.
  - ¿Es necesario que la herramienta instale un agente en la carga de trabajo prevista?
  - ¿Es necesario que la herramienta configure un dispositivo virtual en su entorno?
- Determine sus requisitos de residencia de datos. Algunas organizaciones no desean almacenar sus datos fuera de su entorno. Para abordar este aspecto, es posible que deba instalar algunos componentes de la herramienta en el entorno en las instalaciones.
- Asegúrese de que la herramienta sea compatible con el sistema operativo (SO) y la versión del sistema operativo de la carga de trabajo pertinente.
- Determine si su cartera incluye servidores mainframe, de gama media y heredados. La mayoría de las herramientas de detección pueden detectar estas cargas de trabajo como dependencias, pero es posible que algunas herramientas no puedan obtener detalles del dispositivo, como la utilización y las dependencias del servidor. Las herramientas de detección Device42 y ModernizeIT son compatibles con servidores de mainframe y de gama media.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migración de cargas de trabajo de Cloudera en las instalaciones a la plataforma de datos de Cloudera en AWS

Battulga Purevragchaa y Nidhi Gupta, Amazon Web Services

Nijjwol Lamsal, Cloudera, Inc.

Resumen

Este patrón describe los pasos de alto nivel para migrar sus cargas de trabajo en las instalaciones Cloudera Distributed Hadoop (CDH), Hortonworks Data Platform (HDP) y Cloudera Data Platform (CDP) a la nube pública de CDP en AWS. Le recomendamos que se asocie con los servicios profesionales de Cloudera y con un integrador de sistemas (SI) para implementar estos pasos.

Hay muchos motivos por los que los clientes de Cloudera quieren trasladar sus cargas de trabajo en las instalaciones de CDH, HDP y CDP a la nube. Algunas de las razones más habituales son las siguientes:

- Optimizar la adopción de nuevos paradigmas de plataformas de datos, como Data Lakehouse o Data Mesh
- Aumentar la agilidad empresarial, democratice el acceso y la inferencia sobre los activos de datos existentes
- Reducir el costo total de propiedad (TCO)
- Mejorar la elasticidad de la carga
- Permitir una mayor escalabilidad; reducir drásticamente el tiempo de aprovisionamiento de los servicios de datos en comparación con la base de instalación en las instalaciones heredada
- Eliminar el hardware heredado y reducir significativamente los ciclos de actualización del hardware
- Aproveche los pay-as-you-go precios, que se extienden a las cargas de trabajo de Cloudera en AWS con el modelo de licencias (CCU) de Cloudera
- Aprovechar una implementación más rápida y una mejor integración con las plataformas de integración continua y entrega continua (CI/CD)
- Utilizar una única plataforma unificada (CDP) para múltiples cargas de trabajo

Cloudera es compatible con las principales cargas de trabajo, incluidas Machine Learning, Data Engineering, Data Warehouse, Operational Database, Stream Processing (CSP) y seguridad y gobierno de datos. Cloudera lleva muchos años ofreciendo estas cargas de trabajo en las

instalaciones, y puede migrarlas a la nube de AWS mediante la nube pública de CDP con Workload Manager y Replication Manager.

Cloudera Shared Data Experience (SDX) proporciona un catálogo de metadatos compartido entre estas cargas de trabajo para facilitar la gestión y las operaciones de datos coherentes. SDX también incluye seguridad integral y granular para proteger contra las amenazas y una gobernanza unificada para las capacidades de auditoría y búsqueda a fin de cumplir con estándares como el Estándar de Seguridad de Datos del Sector de Tarjetas de Pago (PCI DSS) y el GDPR.

La migración a CDP de un vistazo

Carga de trabajo	Carga de trabajo de origen	Nube privada de CDH, HDP y CDP
	Entorno de origen	• Windows, Linux • En las instalaciones, coubicación o en cualquier entorno que no sea de AWS
	Carga de trabajo del destino	Nube pública de CDP en AWS
	Entorno de destino	• Modelo de implementación: cuenta de cliente • Modelo operativo: plano de control customer/Cloudera
	Estrategia de migración (7Rs)	Volver a alojar, redefinir la plataforma o refactorizar
Migración	¿Se trata de una actualización de la versión de carga de trabajo?	Sí
	Duración de la migración	• Implementación: aproximadamente 1 semana para crear una cuenta de cliente, una nube privada virtual (VPC) y un entorno de nube

pública de CDP administr
ado por el cliente.

- Duración de la migración: de 1 a 4 meses, según la complejidad y el tamaño de la carga de trabajo.

Costo	Costo de ejecutar la carga de trabajo en AWS	• A un alto nivel, el costo de una migración de cargas de trabajo CDH a AWS asume que establecerá un nuevo entorno en AWS. Incluye el cálculo de tiempo y esfuerzo del personal, así como el aprovisionamiento de los recursos informáticos y las licencias de software para el nuevo entorno. • El modelo de precios de Cloudera basado en el consumo de la nube le ofrece la flexibilidad necesaria para aprovecha r las amplias capacidades de escalado automático. Para obtener más informaci ón, consulte las tarifas del servicio de nube pública de CDP en el sitio web de Cloudera. • Cloudera Enterprise Data Hub se basa en Amazon Elastic Compute Cloud (Amazon EC2) y modela fielmente los clústeres tradicionales. Data Hub se puede personalizar, pero esto repercutirá en los costos. • CDP Public Cloud Data Warehouse, Cloudera Machine Learning y Cloudera Data Engineeri

		ng (CDE) están basados en contenedores y se pueden configurar para que se escalen automáticamente.
Marco y acuerdos de infraestructura	Requisitos del sistema	Consulte la sección Requisitos previos.
	SLA	Consulte el Acuerdo de nivel de servicio de Cloudera para la nube pública de CDP.
	DR	Consulte la recuperación de desastres en la documentación de Cloudera.
	Licencia y modelo operativo (para la cuenta de AWS objetivo)	Modelo Traiga su propia licencia (BYOL)
Conformidad	Requisitos de seguridad	Consulte la descripción general de seguridad de Cloudera en la documentación de Cloudera.
	Otras certificaciones de conformidad	Consulte la información en el sitio web de Cloudera sobre el cumplimiento del Reglamento General de Protección de Datos (GDPR) y el CDP Trust Center.

Requisitos previos y limitaciones

Requisitos previos

- Requisitos de las cuentas de AWS, incluidas las cuentas, los recursos, los servicios y los permisos, como la configuración de las políticas y los roles de AWS Identity and Access Management (IAM)

- Requisitos previos para la implementación de CDP desde el sitio web de Cloudera

La migración requiere los siguientes roles y experiencia:

Rol	Habilidades y responsabilidades
Líder de migración	Garantiza el apoyo ejecutivo, la colaboración en equipo, la planificación, la implementación y la evaluación
Cloudera SME	Conocimientos especializados en administración, administración de sistemas y arquitectura de CDH, HDP y CDP
Arquitecto de AWS	Habilidades en servicios, redes, seguridad y arquitecturas de AWS

Arquitectura

Construir según la arquitectura adecuada es un paso fundamental para garantizar que la migración y el rendimiento satisfagan sus expectativas. Para que su esfuerzo de migración cumpla con las suposiciones de este manual, su entorno de datos de destino en la nube de AWS, ya sea en instancias alojadas en la nube privada virtual (VPC) o en CDP, debe coincidir de manera equivalente con su entorno de origen en términos de versiones del sistema operativo y software, así como de las principales especificaciones de las máquinas.

El siguiente diagrama (reproducido con el permiso de la hoja de datos de Cloudera Shared Data Experience) muestra los componentes de infraestructura del entorno CDP y la forma en que interactúan los niveles o los componentes de la infraestructura.

La arquitectura incluye los siguientes componentes del CDP:

- Data Hub es un servicio para lanzar y gestionar clústeres de cargas de trabajo con tecnología Cloudera Runtime. Puede usar las definiciones de clústeres de Data Hub para aprovisionar clústeres de carga de trabajo y acceder a ellos para casos de uso personalizados y definir configuraciones de clústeres personalizadas. Para obtener más información, consulte el sitio web de Cloudera.

- El flujo y la transmisión de datos abordan los principales desafíos a los que se enfrentan las empresas con los datos en movimiento. Gestiona lo siguiente:
  - Procesamiento del flujo de datos en tiempo real a gran volumen y a gran escala
  - Seguimiento de la procedencia de los datos y del linaje de los datos de streaming
  - Gestión y supervisión de las aplicaciones periféricas y las fuentes de streaming

  Para obtener más información, consulte Cloudera DataFlow y CSP en el sitio web de Cloudera.
- La ingeniería de datos incluye la integración, la calidad y el gobierno de los datos, lo que ayuda a las organizaciones a crear y mantener flujos de trabajo y flujos de datos. Para obtener más información, consulte el sitio web de Cloudera. Aprenda sobre la compatibilidad con instancias de spot para facilitar el ahorro de costos en las cargas de trabajo de ingeniería de datos de AWS for Cloudera.
- Data Warehouse le permite crear data warehouses y data marts independientes que se escalan automáticamente para satisfacer las demandas de carga de trabajo. Este servicio proporciona instancias informáticas aisladas y una optimización automatizada para cada almacén de datos y mercado de datos, y le ayuda a ahorrar costes durante las reuniones. SLAs Para obtener más información, consulte el sitio web de Cloudera. Aprenda sobre la administración de costos y el autoscalamiento de Cloudera Data Warehouse en AWS.
- La base de datos operativa de CDP proporciona una base fiable y flexible para aplicaciones escalables y de alto rendimiento. Ofrece una base de datos escalable, siempre disponible y en tiempo real que proporciona datos estructurados tradicionales junto con datos nuevos y no estructurados dentro de una plataforma operativa y de almacenamiento unificada. Para obtener más información, consulte el sitio web de Cloudera.
- Machine Learning es una plataforma de machine learning nativa de la nube que combina las capacidades de autoservicio de ciencia de datos e ingeniería de datos en un único servicio portátil dentro de una nube de datos empresarial. Permite la implementación escalable del machine learning y la inteligencia artificial (IA) en los datos en cualquier lugar. Para obtener más información, consulte el sitio web de Cloudera.

CDP en AWS

El siguiente diagrama (adaptado con permiso del sitio web de Cloudera) muestra la arquitectura de alto nivel de CDP en AWS. CDP implementa su propio modelo de seguridad para administrar tanto las cuentas como el flujo de datos. Se integran con la IAM mediante el uso de roles entre cuentas.

El plano de control del CDP reside en una cuenta maestra de Cloudera en su propia VPC. Cada cuenta de cliente tiene su propia subcuenta y una VPC única. Los roles de IAM entre cuentas y las tecnologías SSL redirigen el tráfico de administración hacia y desde el plano de control a los servicios de atención al cliente que residen en las subredes públicas enrutables por Internet dentro de cada VPC del cliente. En la VPC del cliente, la experiencia de datos compartidos (SDX) de Cloudera proporciona una seguridad empresarial sólida con una gobernanza y un cumplimiento unificados para que pueda obtener información a partir de sus datos con mayor rapidez. La SDX es una filosofía de diseño que se incorpora a todos los productos de Cloudera. Para obtener más información sobre SDX y la arquitectura de red de nube pública CDP para AWS, consulte la documentación de Cloudera.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar Kubernetes en AWS sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Automatizar y herramientas

- Para obtener herramientas adicionales, puede usar Cloudera Backup Data Recovery (BDR), AWS Snowball y AWS Snowmobile para ayudar a migrar los datos del CDH, HDP y CDP en las instalaciones al CDP alojado en AWS.
- Para las nuevas implementaciones, le recomendamos que utilice la solución para socios de AWS para CDP.

Epics

Preparación para la migración

Tarea	Descripción	Habilidades requeridas
Involucre al equipo de Cloudera.	Cloudera sigue un modelo de interacción estandarizado con sus clientes y puede trabajar con su integrador de sistemas (SI) para promover el mismo enfoque. Póngase en contacto con el equipo de atención al cliente de Cloudera para que le brinden orientación y los recursos técnicos necesarios para iniciar el proyecto. Ponerse en contacto con el equipo de Cloudera garantiza que todos los equipos necesario s puedan prepararse para la migración a medida que se acerque su fecha. Puede ponerse en contacto con los servicios profesion ales de Cloudera para que su implementación de Cloudera pase de la fase piloto a la fase de producción rápidamente, a un costo menor y con el máximo rendimiento. Para obtener una lista completa de ofertas, consulte el sitio web de Cloudera.	Líder de migración

Tarea	Descripción	Habilidades requeridas
Cree un entorno de nube pública de CDP en AWS para su VPC.	Trabaje con Cloudera Professional Services o su SI para planificar e implement ar la nube pública de CDP en una VPC en AWS.	Arquitecto de la nube, Cloudera SME

Tarea	Descripción	Habilidades requeridas
Priorice y evalúe las cargas de trabajo para la migración.	Evalúe todas sus cargas de trabajo en las instalaciones para determinar cuáles son las más fáciles de migrar. Es mejor migrar primero a las aplicaciones que no son esenciales para la misión, ya que tendrán un impacto mínimo en sus clientes. Guarde las cargas de trabajo esenciales para el final, después de migrar correctam ente otras cargas de trabajo. **Note** Las cargas de trabajo transitorias (CDP Data Engineering) son más fáciles de migrar que las cargas de trabajo persistentes (CDP Data Warehouse). También es important e tener en cuenta el volumen y las ubicaciones de los datos al migrar. Los desafíos pueden incluir replicar los datos de forma continua desde un entorno en las instalaciones a la nube y cambiar	Líder de migración

Tarea	Descripción	Habilidades requeridas
	los procesos de ingesta de datos para importarlos directamente a la nube.	
Analice las actividades de migración de CDH, HDP, CDP y aplicaciones antiguas.	Considere y comience a planificar las siguientes actividades con Cloudera Workload Manager: • Datos y cargas de trabajo para copiar a su entorno de AWS • Datos listos para la nube • Vecinos ruidosos, que consumen recursos y crean problemas a otros inquilinos • Cargas de trabajo elásticas • Clústeres pequeños con una elevada sobrecarga operativa	Líder de migración

Tarea	Descripción	Habilidades requeridas
Complete los requisitos y recomendaciones de Cloudera Replication Manager.	Trabaje con Cloudera Professional Services y su SI para prepararse para migrar las cargas de trabajo a su entorno de nube pública de CDP en AWS. Comprender los siguientes requisitos y recomendaciones puede ayudarle a evitar problemas comunes durante y después de instalar el servicio Replication Manager. • Revise los documentos de respaldo de Replication Manager para confirmar que cumple con los requisitos del entorno y del sistema. Para obtener más información, consulte la matriz de soporte para CDP Public Cloud Replication Manager en el sitio web de Cloudera. • No necesita acceso root a los nodos en los que se instalarán la aplicación Replication Manager y el motor Data Lifecycle Manager (DLM). • Instale Apache Hive durante la instalación inicial de Replication Manager, a menos que esté seguro de que no utilizará la	Líder de migración

Tarea	Descripción	Habilidades requeridas
	replicación de Hive en el futuro. Si decide instalar Hive después de crear las políticas de replicación de HDFS en Replication Manager, tendrá que eliminar y volver a crear todas las políticas de replicación de HDFS después de agregar Hive. • Los clústeres utilizados en Replication Manager deben tener configuraciones simétricas. Cada clúster de una relación de replicación debe estar configurado exactamente de la misma manera en cuanto a seguridad (Kerberos), administración de usuarios (LDAP/AD) y Knox Proxy. Los servicios de clúster, como el Sistema de archivos distribuido de Hadoop (HDFS), Apache Hive, Apache Knox, Apache Ranger y Apache Atlas, pueden tener diferentes configuraciones para una alta disponibilidad (HA). Por ejemplo, los clústeres de origen y de destino pueden tener configuraciones de	

Tarea	Descripción	Habilidades requeridas
	alta y de baja disponibilidad independientes.	

Migración de CDP a AWS

Tarea	Descripción	Habilidades requeridas
Migre la primera carga de trabajo para dev/test los entornos con Cloudera Workload Manager.	Su SI puede ayudarlo a migrar su primera carga de trabajo a la nube de AWS. Debe ser una aplicación que no esté orientada al cliente ni sea esencial para la misión. Los candidatos ideales para dev/test la migración son las aplicaciones que tienen datos que la nube puede ingerir fácilmente, como las cargas de trabajo de ingeniería de datos de CDP. Se trata de una carga de trabajo transitoria a la que, por lo general, acceden menos usuarios, en comparación con una carga de trabajo persistente, como una carga de trabajo de CDP Data Warehouse, que podría tener muchos usuarios que necesitan un acceso ininterrumpido. Las cargas de trabajo de ingeniería de datos no son persistentes, lo que minimiza el impacto empresarial en caso de que algo vaya mal.	Líder de migración

Tarea	Descripción	Habilidades requeridas
	Sin embargo, estas tareas pueden ser fundamentales para los informes de producció n, así que priorice primero las cargas de trabajo de ingenierí a de datos de bajo impacto.	

Tarea	Descripción	Habilidades requeridas
Repita los pasos de migración según sea necesario.	Cloudera Workload Manager ayuda a identificar las cargas de trabajo que mejor se adaptan a la nube. Proporcio na métricas como las calificac iones de rendimiento de la nube, sizing/capacity los planes para el entorno objetivo y los planes de replicaci ón. Los mejores candidato s para la migración son las cargas de trabajo estaciona les, los informes ad hoc y los trabajos intermitentes que no consumen muchos recursos. Cloudera Replication Manager mueve los datos en las instalaciones a la nube y de la nube a las instalaciones. Optimice de forma proactiva las cargas de trabajo, las aplicaciones, el rendimiento y la capacidad de la infraestr uctura para el almacenam iento de datos, la ingenierí a de datos y el machine learning mediante Workload Manager. Para obtener una guía completa sobre cómo modernizar un data warehouse, consulte el sitio web de Cloudera.	Cloudera SME

Recursos relacionados

Documentación de Cloudera:

- Registro de clústeres clásicos con CDP, Cloudera Manager y Replication Manager:
  - Consola de administración
  - Replication en Hive de Replication Manager
- Replicación de Sentry
- Permisos de Sentry
- Lista de verificación para la planificación de clústeres de Data Hub
- Arquitectura de Workload Manager
- Requisitos de Replication Manager
- Observabilidad de la plataforma de datos de Cloudera
- Requisitos de AWS

Documentación de AWS:

- Migración de datos a la nube

Resolver los errores de conexión después de migrar Microsoft SQL Server a la nube de AWS

Premkumar Chelladurai, Amazon Web Services

Resumen

Tras migrar Microsoft SQL Server que se ejecuta en Windows Server 2008 R2, 2012 o 2012 R2 a instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la nube de Amazon Web Services (AWS), se produce un error en la conexión a SQL Server y aparecen los siguientes errores:

- `[Microsoft][ODBC SQL Server Driver][DBNETLIB] General Network error`
- `ERROR [08S01] [Microsoft][SQL Native Client]Communication link failure. System.Data.SqlClient.SqlException: A transport-level error has occurred when sending the request to the server. (provider: TCP Provider, error: 0 - An existing connection was forcibly closed by the remote host.)`
- `TCP Provider: The semaphore timeout period has expired`

Este patrón describe cómo puede resolver estos errores si desactiva las características del paquete de redes escalables (SNP) de Windows en el nivel del sistema operativo (SO) y de la interfaz de red para SQL Server que se ejecuta en Windows Server 2008 R2, 2012 o 2012 R2.

Requisitos previos y limitaciones

Requisitos previos

- Privilegios de administrador para Windows Server.
- Si utilizó AWS Application Migration Service como herramienta de migración, necesitará una de las siguientes versiones de Windows Server:
  - Windows Server 2008 R2 Service Pack 1, 2012 o 2012 R2
- Si utilizó CloudEndure Migration como herramienta de migración, necesitará una de las siguientes versiones de Windows Server:
  - Windows Server 2003 R2 Service Pack 3, 2008, 2008 R2 Service Pack 1, 2012 o 2012 R2.

Tools (Herramientas)

- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede utilizar Amazon EC2 para lanzar tantos o tan pocos servidores virtuales como necesite, y puede ampliarlos de forma horizontal o horizontal.
- Windows Server: Windows Server es una plataforma para crear una infraestructura de aplicaciones, redes y servicios web conectados.

Epics

Cómo desactivar las características de SNP a nivel del sistema operativo y de la interfaz de red elástica

Tarea	Descripción	Habilidades requeridas
Desactive las características de SNP a nivel del sistema operativo.	1. Inicie sesión en Windows Server y abra un símbolo del sistema como administrador. 2. Ejecute el comando `netsh int tcp show global`. 3. En el resultado, compruebe si `Receive-Side Scaling` o `Chimney Offload` está en modo `enabled`. Si alguno es `enabled`, ejecute los siguientes comandos: • `netsh int tcp set global chimney=disabled` • `netsh int tcp set global rss=disabled`	Administrador de AWS, administrador de sistemas de AWS, ingeniero de migraciones, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Desactive las características de SNP a nivel de la interface de red elástica.	1. Seleccione Inicio, introduzca `ncpa.cpl` y, a continuación, presione Intro. 2. Haga clic con el botón secundario en Elastic Network Adapter. 3. En el menú emergente, seleccione Properties. 4. En la ventana Ethernet Adapter Properties, seleccione Configure. 5. En la ventana emergente Amazon Elastic Network Adapter Properties, seleccione la pestaña Advanced. 6. En la sección Property, desactive todas las descargas y RSS.	Administrador de AWS, administrador de la nube, administrador de sistemas de AWS

Recursos relacionados

- Solución de problemas de características avanzadas de rendimiento de red, como RSS y NetDMA

Rediseñar

Temas

- Convierta VARCHAR2 (1) el tipo de datos de Oracle en un tipo de datos booleano para Amazon Aurora PostgreSQL
- Crear usuarios y roles de aplicaciones en Aurora compatible con PostgreSQL
- Emule Oracle DR mediante una base de datos global de Aurora compatible con PostgreSQL
- Implemente SHA1 el hash para los datos de PII al migrar de SQL Server a PostgreSQL
- Migración gradual de Amazon RDS para Oracle a Amazon RDS para PostgreSQL con Oracle SQL Developer y AWS SCT
- Cargar archivos BLOB en TEXT mediante la codificación de archivos en Aurora compatible con PostgreSQL
- Migre Amazon RDS for Oracle a Amazon RDS for PostgreSQL con y utilizando y AWS SCT AWS DMS AWS CLI CloudFormation
- Migración de Amazon RDS para Oracle a Amazon RDS para PostgreSQL en modo SSL mediante AWS DMS
- Migración de los paquetes pragma SERIALLY_REUTILIZABLE de Oracle a PostgreSQL
- Migración de tablas externas de Oracle a Amazon Aurora compatible con PostgreSQL
- Migración de índices basados en funciones de Oracle a PostgreSQL
- Migración de las funciones nativas de Oracle a PostgreSQL mediante extensiones
- Migre una base de datos Db2 de Amazon EC2 a Aurora compatible con MySQL mediante AWS DMS
- Migre una base de datos de Microsoft SQL Server de Amazon EC2 a Amazon DocumentDB mediante AWS DMS
- Migre una base de datos ThoughtSpot Falcon local a Amazon Redshift
- Migre de Oracle Database a Amazon RDS for PostgreSQL mediante Oracle GoldenGate
- Migración de una tabla particionada de Oracle a PostgreSQL mediante AWS DMS
- Migración de de Amazon RDS para Oracle a Amazon RDS para MySQL
- Migre de IBM Db2 en Amazon EC2 a Aurora compatible con PostgreSQL mediante AWS DMS y AWS SCT
- Migre de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante AWS DMS SharePlex

- Migración de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante la vista materializada y AWS DMS
- Migración de Oracle en Amazon EC2 a Amazon RDS para MySQL con AWS DMS y AWS SCT
- Migre una base de datos Oracle de Amazon EC2 a Amazon RDS para MariaDB con AWS DMS y AWS SCT
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para MySQL con AWS DMS y AWS SCT
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para PostgreSQL mediante Oracle Bystander y AWS DMS
- Migración de una base de datos de Oracle a Amazon Redshift con AWS DMS y AWS SCT
- Migración de una base de datos de Oracle a Aurora PostgreSQL con AWS DMS y AWS SCT
- Migración de datos de una base de datos de Oracle en las instalaciones a Aurora PostgreSQL
- Migración de SAP ASE a Amazon RDS para SQL Server utilizando AWS DMS
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon Redshift mediante AWS DMS
- Migración de una base de datos en las instalaciones de Microsoft SQL Server a Amazon Redshift mediante agentes de extracción de datos de AWS SCT
- Migración de aplicaciones heredadas de Oracle Pro*C a ECPG
- Migración de columnas generadas de forma virtual de Oracle a PostgreSQL
- Configure la funcionalidad UTL_FILE de Oracle en Aurora compatible con PostgreSQL
- Validar los objetos de la base de datos después de migrar de Oracle a Amazon Aurora PostgreSQL

Convierta VARCHAR2 (1) el tipo de datos de Oracle en un tipo de datos booleano para Amazon Aurora PostgreSQL

Naresh Damera, Amazon Web Services

Resumen

Durante una migración de Amazon Relational Database Service (Amazon RDS) para Oracle a una edición compatible con PostgreSQL de Amazon Aurora, es posible que se produzca una discrepancia de datos al validar la migración en (). AWS Database Migration Service AWS DMS Para evitar esta discrepancia, puede convertir VARCHAR2 (1) el tipo de datos en un tipo de datos booleano.

VARCHAR2 el tipo de datos almacena cadenas de texto de longitud variable y VARCHAR2 (1) indica que la cadena tiene una longitud de 1 carácter o 1 byte. Para obtener más información VARCHAR2, consulte los tipos de datos integrados de Oracle (documentación de Oracle).

En este patrón, en la columna de la tabla de datos fuente de muestra, los datos VARCHAR2 (1) son una Y, para Sí, o N, para No. Este patrón incluye instrucciones para usar AWS DMS y AWS Schema Conversion Tool (AWS SCT) para convertir este tipo de datos de los valores Y y N de VARCHAR2 (1) a valores verdaderos o falsos en booleano.

Destinatarios previstos

Este patrón se recomienda para quienes tengan experiencia en la migración de bases de datos de Oracle a una versión de Aurora compatible con PostgreSQL mediante AWS DMS. A medida que complete la migración, siga las recomendaciones de Cómo convertir Oracle a Amazon RDS for PostgreSQL o Amazon AWS SCT Aurora PostgreSQL (documentación).

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- Confirme que su entorno esté preparado para Aurora, incluida la configuración de credenciales, permisos y un grupo de seguridad. Para obtener más información, consulte Configuración del entorno para Amazon Aurora (documentación de Aurora).
- Una base de datos de Amazon RDS for Oracle de origen que contiene una columna de tabla VARCHAR2 con (1) datos.

- Instancia de base de datos compatible con Amazon Aurora PostgreSQL. Para obtener más información, consulte Creación de un clúster de base de datos y cómo conectarse a una base de datos en un clúster de base de datos de Aurora PostgreSQL (documentación de Aurora).

Versiones de producto

- Opciones de Amazon RDS para Oracle Versión 12.1.0.2 o posterior.
- AWS DMS versión 3.1.4 o posterior. Para obtener más información, consulte Uso de una base de datos Oracle como fuente AWS DMS y Uso de una base de datos PostgreSQL como destino AWS DMS(documentación).AWS DMS Le recomendamos que utilice la última versión de AWS DMS para obtener el soporte más completo de versiones y funciones.
- AWS Schema Conversion Tool (AWS SCT) versión 1.0.632 o posterior. Le recomendamos que utilice la última versión de AWS SCT para obtener el soporte más completo de versiones y funciones.
- Aurora es compatible con las versiones de PostgreSQL que figuran en Versiones del motor de base de datos para Aurora compatibles con PostgreSQL (documentación de Aurora).

Arquitectura

Pila de tecnología de origen

Recurso de instancia de base de datos de Amazon RDS para Oracle

Pila de tecnología de destino

Instancia de base de datos compatible con Amazon Aurora PostgreSQL

Arquitectura de origen y destino

Tools (Herramientas)

Servicios de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.
- AWS Database Migration Service (AWS DMS) le ayuda a migrar los almacenes de datos a una combinación de configuraciones locales y en la nube Nube de AWS o entre ellas.

- Amazon Relational Database Service (Amazon RDS) para Oracle lo ayuda a configurar, utilizar y escalar una base de datos relacional de Oracle en la Nube de AWS.
- AWS Schema Conversion Tool (AWS SCT) admite migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayoría del código personalizado a un formato compatible con la base de datos de destino.

Otros servicios

- Oracle SQL Developer es un entorno de desarrollo integrado que simplifica el desarrollo y la administración de bases de datos de Oracle, tanto en implementaciones tradicionales como en implementaciones basadas en la nube. En este patrón, utilice esta herramienta para conectarse a la instancia de base de datos Amazon RDS para Oracle y consultar los datos.
- pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos. En este patrón, utilice esta herramienta para conectarse a la instancia de base de datos Aurora y consultar los datos.

Epics

Preparación para la migración

Tarea	Descripción	Habilidades requeridas
Crear un informe de migración de bases de datos.	1. En AWS SCT, cree un informe de evaluación de la migración de la base de datos. Para obtener más información, consulte Creación de informes de evaluación de la migración. 2. Revise y lleve a cabo las acciones del informe de evaluación de la migración. Para obtener más informaci ón, consulte el informe de evaluación, consulte	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	Elementos de acción del informe de evaluación.	
Elimine las restricciones de clave externa en la base de datos de destino.	En PostgreSQL, las claves foráneas se implementan mediante activadores. Durante la fase de carga completa, AWS DMS carga cada tabla de una en una. Recomendamos encarecidamente que deshabilite las restricciones de clave externa durante una carga completa, utilizando uno de los siguientes métodos: • Deshabilite temporalmente todos los disparadores de la instancia y finalice la carga completa. • Utilice el parámetro `session_replication_role` en PostgreSQL. Si no es posible deshabilitar las restricciones de clave externa, cree una tarea de AWS DMS migración para los datos principales que sea específica de la tabla principal y la tabla secundaria.	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas

Deshabilite las claves principales y únicas en la base de datos de destino.	Con los siguientes comandos, deshabilite las claves y restricciones principales de la base de datos de destino. Esto ayuda a mejorar el rendimiento de la tarea de carga inicial.
	`ALTER TABLE <table> DISABLE PRIMARY KEY;`
	`ALTER TABLE <table> DISABLE CONSTRAINT <constraint_name>;`
		Administrador de base de datos, desarrollador

Cree la tarea de carga inicial.	En AWS DMS, cree la tarea de migración para la carga inicial. Para obtener instrucciones, consulte Creación de tareas. En Migration type (Tipo de migración), elija Migrate existing data (Migración de datos existentes). Este método de migración se llama `Full Load` en la API. No inicie esta tarea todavía.	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
Edite la configuración de la tarea de carga inicial.	Edite la configuración de la tarea para añadir la validación de datos. Estos ajustes de validación se deben crear en un archivo JSON. Para obtener instrucciones y ejemplos, consulte Especificar la configuración de las tareas. Añada las siguientes validaciones: • Para comprobar que los VARCHAR2 (1) datos se han convertido correctamente a booleanos en la base de datos de destino, añada el código en el script de validación de datos de la sección de información adicional de este patrón. El script de validación convierte los valores booleanos de 1 en Y y de 0 en N de la tabla de destino y, a continuación, compara los valores de la tabla de destino con la tabla de origen. Para validar el resto de la migración de datos, habilite la validación de datos en la tarea. Para obtener más información consulte	Administrador de AWS, Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Configuración de tareas de validación de datos.	
Creación de una tarea de replicación continua.	En AWS DMS, cree la tarea de migración que mantenga la base de datos de destino sincronizada con la base de datos de origen. Para obtener instrucciones, consulte Creación de tareas. Para el método de migración, elija Replicar solo los cambios de datos. No inicie esta tarea todavía.	Administrador de base de datos

Probar las tareas de migración

Tarea	Descripción	Habilidades requeridas
Cree datos de muestra para realizar pruebas.	En la base de datos de origen, cree una tabla de muestra con datos para realizar pruebas.	Desarrollador
Confirme que no haya actividades conflictivas.	Utilice `pg_stat_activity` para comprobar si hay alguna actividad en el servidor que pueda afectar a la migración . Para obtener más informaci ón, consulte Recopilador de estadísticas (documentación de PostgreSQL).	Administrador de AWS
Inicie las tareas de AWS DMS migración.	En la AWS DMS consola, en la página del panel de control, inicie la carga inicial	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	y las tareas de replicación en curso que creó en la epopeya anterior.	
Supervise las tareas y los estados de carga de la tabla.	Durante la migración, supervise el estado de las tareas y los estados de la tabla. Cuando se complete la tarea de carga inicial, en la pestaña Estadísticas de la tabla: • El Estado de carga debe ser Tabla completada. • El Estado de validación debe estar Validado.	Administrador de AWS
Compruebe los resultados de la migración.	Con pgAdmin, consulte la tabla en la base de datos de destino. Una consulta correcta indica que los datos se migraron correctamente.	Desarrollador
Agregue claves principales y claves externas a la base de datos de destino.	Cree la clave principal y la clave externa en la base de datos de destino. Para obtener más información, consulte ALTER TABLE (sitio web de PostgreSQL).	Administrador de base de datos
Elimine los datos de la prueba.	En las bases de datos de origen y destino, limpie los datos que se crearon para las pruebas unitarias.	Desarrollador

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Completar la migración.	Repita la epopeya anterior, pruebe las tareas de migración utilizando los datos de origen reales. De este modo, se migran los datos desde la base de datos de origen a la base de datos de destino.	Desarrollador
Valide que las bases de datos de origen y destino estén sincronizadas.	Valide que las bases de datos de origen y destino estén sincronizadas. Para obtener más información e instrucciones, consulte Validación de datos de AWS DMS.	Desarrollador
Detenga la base de datos de origen.	Detenga la base de datos de Amazon RDS para Oracle. Para obtener instrucciones, consulte Detener temporalmente una instancia de base de datos de Amazon RDS. Al detener la base de datos de origen, la carga inicial y las tareas de replicación en curso AWS DMS se detienen automáticamente. No es necesario realizar ninguna acción adicional para detener estas tareas.	Desarrollador

Recursos relacionados

AWS referencias

- Migre una base de datos Oracle a Aurora PostgreSQL AWS DMS mediante AWS SCT y AWS (Guía prescriptiva)
- Conversión de Oracle a Amazon RDS para PostgreSQL o Amazon AWS SCT Aurora PostgreSQL (documentación)
- Cómo funciona (documentación) AWS DMSAWS DMS

Otras referencias

- Tipo de datos booleano (documentación de PostgreSQL)
- Tipos de datos integrados de Oracle (documentación de Oracle)
- pgAdmin (sitio web de pgAdmin)
- SQL Developer (sitio web de Oracle)

Tutoriales y videos

- Cómo empezar con AWS DMS
- Introducción a Amazon RDS
- Introduction to AWS DMS (video)
- Descripción de Amazon RDS (video)

Información adicional

Script de validación de datos

El siguiente script de validación de datos convierte 1 en Y y 0 en N. Esto ayuda a que la AWS DMS tarea se complete correctamente y supere la validación de la tabla.

```
{
"rule-type": "validation",
"rule-id": "5",
"rule-name": "5",
"rule-target": "column",
"object-locator": {
```

```
"schema-name": "ADMIN",
"table-name": "TEMP_CHRA_BOOL",
"column-name": "GRADE"
},
"rule-action": "override-validation-function",
"target-function": "case grade when '1' then 'Y' else 'N' end"
        }
```

La sentencia `case` del script realiza la validación. Si la validación falla, AWS DMS inserta un registro en la tabla public.awsdms_validation_failures_v1 de la instancia de base de datos de destino. Este registro incluye el nombre de la tabla, el tiempo de error y detalles sobre los valores que no coinciden en las tablas de origen y destino.

Si no agrega este script de validación de datos a la tarea y los datos se insertan en la tabla de destino, la AWS DMS tarea mostrará el estado de validación como Registros no coincidentes. AWS DMS

Durante la AWS SCT conversión, la tarea de AWS DMS migración cambia el tipo de datos de VARCHAR2 (1) a booleano y añade una restricción de clave principal a la columna. `''N0''`

Crear usuarios y roles de aplicaciones en Aurora compatible con PostgreSQL

Abhishek Verma, Amazon Web Services

Resumen

Al migrar a la edición compatible con PostgreSQL de Amazon Aurora, los usuarios y roles de la base de datos que existen en la base de datos de origen deben crearse en la base de datos de Aurora compatible con PostgreSQL. Puede crear los usuarios y los roles en Aurora compatibles con PostgreSQL mediante dos enfoques diferentes:

- Utilice usuarios y roles similares en la base de datos de destino y en la base de datos de origen. En este enfoque, los lenguajes de definición de datos (DDLs) se extraen para los usuarios y las funciones de la base de datos de origen. A continuación, se transforman y se aplican a la base de datos Aurora compatible con PostgreSQL de destino. Por ejemplo, la entrada del blog Usar SQL para asignar usuarios, roles y concesiones de Oracle a PostgreSQL trata sobre el uso de la extracción de un motor de base de datos de origen de Oracle.
- Utilice usuarios y roles estandarizados que se utilizan habitualmente durante el desarrollo, la administración y para realizar otras operaciones relacionadas en la base de datos. Esto incluye las operaciones de solo lectura, lectura/escritura, desarrollo, administración e implementación realizadas por los respectivos usuarios.

Este patrón contiene las concesiones necesarias para la creación de usuarios y roles en Aurora, compatible con PostgreSQL, necesarias para el enfoque estandarizado de usuarios y roles. Los pasos de creación de usuarios y roles están alineados con la política de seguridad de conceder el privilegio mínimo a los usuarios de la base de datos. La siguiente tabla muestra los usuarios, sus funciones correspondientes y sus detalles en la base de datos.

Users	Roles	Finalidad
`APP_read`	`APP_RO`	Se utiliza para el acceso de solo lectura al esquema APP
`APP_WRITE`	`APP_RW`	Se utiliza para las operaciones de escritura y lectura del esquema APP

`APP_dev_user`	`APP_DEV`	Se utiliza con fines de desarrollo en el esquema `APP_DEV`, con acceso de solo lectura al esquema `APP`
`Admin_User`	`rds_superuser`	Se utiliza para realizar operaciones de administrador en la base de datos
`APP`	`APP_DEP`	Se utiliza para crear los objetos del esquema `APP` y para la implementación de objetos en el esquema `APP`

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa
- Una base de datos PostgreSQL, una base de datos Amazon Aurora de edición compatible con PostgreSQL o una base de datos Amazon Relational Database Service (Amazon RDS) para PostgreSQL

Versiones de producto

- Todas las versiones de PostgreSQL

Arquitectura

Pila de tecnología de origen

- Cualquier base de datos

Pila de tecnología de destino

- Amazon Aurora compatible con PostgreSQL

Arquitectura de destino

El siguiente diagrama muestra los roles de usuario y la arquitectura del esquema en la base de datos Aurora compatible con PostgreSQL.

Automatizar y escalar

Este patrón contiene los usuarios, los roles y el script de creación del esquema, que puede ejecutar varias veces sin que ello afecte a los usuarios actuales de la base de datos de origen o destino.

Tools (Herramientas)

Servicios de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.

Otros servicios

- psql es una herramienta frontend basada en un terminal que se instala con todas las instalaciones de PostgreSQL Database. Cuenta con una interfaz de la línea de comandos para ejecutar comandos de SQL, PL-PGSQL y del sistema operativo.
- pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.

Epics

Crear los usuarios y los roles

Tarea	Descripción	Habilidades requeridas
Cree el usuario de implement ación.	El usuario de implementación APP se utilizará para crear y modificar los objetos de la base de datos durante las	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	implementaciones. Utilice los siguientes scripts para crear el rol de usuario de implement ación APP_DEP en el esquema APP. Valide los derechos de acceso para asegurarse de que este usuario solo tiene el privilegio de crear objetos en el esquema APP requerido.
	
	1. Conéctese al usuario administrador y cree el esquema.
	
	`CREATE SCHEMA APP;`
	
	2. Cree el usuario.
	
	`CREATE USER APP WITH PASSWORD <password> ;`
	
	3. Creación del rol.
	
	`CREATE ROLE APP_DEP ;`
	`GRANT all on schema APP to APP_DEP ;`
	`GRANT USAGE ON SCHEMA APP to APP_DEP ;`
	`GRANT connect on database <db_name> to APP_DEP ;`
	`GRANT APP_DEP to APP;`
	
	4. Para probar los privilegios, conéctese a las tablas APP y cree las tablas.	

Tarea	Descripción	Habilidades requeridas

	`set search_path to APP;`
	`SET`
	`CREATE TABLE test(id integer ) ;`
	`CREATE TABLE`
	5. Compruebe los privilegios.
	`select schemaname , tablename , tableowner from pg_tables where tablename like 'test' ;`
	`schemaname | tablename | tableowner`
	`APP | test | APP`	

Tarea	Descripción	Habilidades requeridas

Cree el usuario de solo lectura.	El usuario de solo lectura `APP_read` se utilizará para realizar la operación de solo lectura en el esquema APP. Utilice los siguientes scripts para crear el usuario de solo lectura. Valide los derechos de acceso para asegurars e de que este usuario tiene privilegios para leer únicament e los objetos del esquema APP y para conceder automátic amente el acceso de lectura a cualquier objeto nuevo creado en el esquema APP.
	
	1. Cree el usuario `APP_read`.
	
	`create user APP_read ; alter user APP_read with password 'your_password' ;`
	
	2. Creación del rol.
	
	`CREATE ROLE APP_ro ; GRANT SELECT ON ALL TABLES IN SCHEMA APP TO APP_RO ; GRANT USAGE ON SCHEMA APP TO APP_RO GRANT CONNECT ON DATABASE testdb TO APP_RO ; GRANT APP_RO TO APP_read;`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	3. Para probar los privilegios, inicie sesión con el usuario `APP_read`.
	
	`set search_path to APP ;`
	`create table test1( id integer) ;`
	`ERROR: permission denied for schema APP`
	`LINE 1: create table test1( id integer) ;`
	`insert into test values (34) ;`
	`ERROR: permission denied for table test`
	`SQL state: 42501`
	`select from test`
	`no rows selected`	

Tarea	Descripción	Habilidades requeridas

Cree el read/write usuario.	El read/write usuario se `APP_WRITE` utilizará para realizar operaciones de lectura y escritura en el esquemaAPP. Utilice los siguientes scripts para crear el read/write usuario y asignarle el `APP_RW` rol. Valide los derechos de acceso para asegurarse de que este usuario solo tiene privilegios de lectura y escritura en los objetos del esquema APP y para conceder automáticamente el acceso de lectura y escritura a cualquier objeto nuevo creado en el esquema APP.
	
	1. Cree el usuario.
	
	`CREATE USER APP_WRITE ; alter user APP_WRITE with password 'your_password' ;`
	
	2. Creación del rol.
	
	`CREATE ROLE APP_RW; GRANT SELECT, INSERT, UPDATE, DELETE ON ALL TABLES IN SCHEMA APP TO APP_RW ; GRANT CONNECT ON DATABASE postgres to APP_RW ; GRANT USAGE ON SCHEMA APP to APP_RW ;`	

Tarea	Descripción	Habilidades requeridas
	ALTER DEFAULT PRIVILEGES IN SCHEMA APP GRANT SELECT, INSERT, UPDATE, DELETE ON TABLES TO APP_RW ; GRANT APP_RW to APP_WRITE 3. Para probar los privilegios, inicie sesión con el usuario `APP_WRITE` . SET SEARCH_PATH to APP; CREATE TABLE test1(id integer) ; ERROR: permission denied for schema APP LINE 1: create table test1(id integer) ; SELECT * FROM test ; id ---- 12 INSERT INTO test values (31) ; INSERT 0 1	

Tarea	Descripción	Habilidades requeridas

Cree el usuario administrador.	El usuario administrador `Admin_User` se utilizará para realizar operaciones de administración en la base de datos. Algunos ejemplos de estas operaciones son `CREATE ROLE` y `CREATE DATABASE`. `Admin_User` utiliza la función integrada `rds_superuser` para realizar operaciones de administración en la base de datos. Utilice los siguientes scripts para crear y probar el privilegio del usuario administrador `Admin_User` en la base de datos.
	
	1. Cree el usuario y conceda el rol.
	
	`create user Admin_User WITH PASSWORD ‘Your password’ ALTER user Admin_user CREATEDB; ALTER user Admin_user CREATEROLE;`
	
	2. Para probar el privilegio, inicie sesión desde el usuario `Admin_User` .
	
	`SELECT * FROM APP.test ; id ----`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	31 CREATE ROLE TEST ; CREATE DATABASE test123 ;	

Tarea	Descripción	Habilidades requeridas

Cree el usuario de desarrollo.	El usuario de desarrollo `APP_dev_user` tendrá derechos para crear los objetos en su esquema local APP_DEV y acceso de lectura en el esquema APP. Utilice los siguientes scripts para crear y probar los privilegios del usuario `APP_dev_user` en la base de datos.
	1. Cree el usuario.
	`CREATE USER APP1_dev_ user with password ‘your password’;`
	2. Cree el esquema APP_DEV para el `App_dev_user` .
	`CREATE SCHEMA APP1_DEV ;`
	3. Cree el rol APP_DEV.
	`CREATE ROLE APP1_DEV ; GRANT APP1_RO to APP1_DEV ; GRANT SELECT ON ALL TABLES IN SCHEMA APP1_DEV to APP1_dev_ user GRANT USAGE, CREATE ON SCHEMA APP1_DEV to APP1_DEV_USER GRANT APP1_DEV to APP1_DEV_USER ;`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	4. Para probar los privilegios, inicie sesión desde `APP_dev_user` .
	
	`CREATE TABLE APP1_dev.test1( id integer ) ;`
	`CREATE TABLE`
	`INSERT into APP1_dev.test1 ( select * from APP1.test );`
	`INSERT 0 1`
	`CREATE TABLE APP1.test4 ( id int) ;`
	`ERROR: permission denied for schema APP1`
	`LINE 1: create table APP1.test4 ( id int) ;`	

Recursos relacionados

Documentación de PostgreSQL

- CREAR ROL
- CREAR USUARIO
- Roles predefinidos

Información adicional

Mejora de PostgreSQL 14

PostgreSQL 14 proporciona un conjunto de roles predefinidos que dan acceso a determinadas capacidades e información privilegiadas que se necesitan con frecuencia. Los administradores (incluidos roles con privilegios `CREATE ROLE`) pueden conceder estos roles u otros roles de su entorno a los usuarios, proporcionándoles acceso a la información y las capacidades especificadas.

Los administradores pueden conceder a los usuarios el acceso a estos roles mediante el comando `GRANT`. Por ejemplo, para conceder el rol `pg_signal_backend` al `Admin_User`, puede ejecutar el siguiente comando.

```
GRANT pg_signal_backend TO Admin_User;
```

El objetivo del rol `pg_signal_backend` es permitir a los administradores habilitar roles de confianza que no son de superusuario para enviar señales a otros backends. Para obtener más información, consulte Mejora de PostgreSQL 14.

Afinar el acceso

En algunos casos, puede ser necesario proporcionar un acceso más detallado a los usuarios (por ejemplo, acceso basado en tablas o en columnas). En esos casos, se pueden crear roles adicionales para conceder esos privilegios a los usuarios. Para obtener información, consulte Concesiones de PostgreSQL.

Emule Oracle DR mediante una base de datos global de Aurora compatible con PostgreSQL

HariKrishna Boorgadda, Amazon Web Services

Resumen

Las prácticas recomendadas para la recuperación de desastres (DR) a nivel empresarial consisten, básicamente, en diseñar e implementar sistemas de hardware y software tolerantes a fallos que puedan sobrevivir a un desastre (continuidad de la actividad empresarial) y reanudar las operaciones normales (reanudación de la actividad empresarial) con una intervención mínima e, idealmente, sin pérdida de datos. Crear entornos tolerantes a fallos para cumplir los objetivos de la DR empresarial puede ser una empresa larga y costosa, y requiere un firme compromiso por parte de la empresa.

Oracle Database ofrece tres enfoques diferentes de recuperación de desastres que proporcionan el nivel más alto de protección y disponibilidad de datos en comparación con cualquier otro enfoque para proteger datos de Oracle.

- Dispositivo de recuperación sin pérdida de datos de Oracle
- Oracle Active Data Guard
- Oráculo GoldenGate

Este patrón proporciona una forma de emular la recuperación ante GoldenGate desastres de Oracle mediante una base de datos global de Amazon Aurora. La arquitectura de referencia utiliza Oracle GoldenGate for DR en tres regiones de AWS. El patrón redefine la plataforma de la arquitectura de origen a la base de datos global de Aurora, nativa en la nube y basada en la edición compatible con PostgreSQL de Amazon Aurora.

Las bases de datos globales de Aurora están diseñadas para aplicaciones con una huella global. Una única base de datos de Aurora puede abarcar varias regiones de AWS con hasta cinco regiones secundarias. Las bases de datos globales de Aurora ofrecen las siguientes características:

- Replicación física a nivel de almacenamiento
- Lecturas globales de baja latencia
- Recuperación de desastres rápida tras interrupciones en toda la región
- Migraciones rápidas entre regiones
- Bajo retraso de replicación en todas las regiones

- Little-to-no impacto en el rendimiento de su base de datos

Para obtener más información sobre las características y ventajas de las bases de datos globales de Aurora, consulte Uso de las bases de datos globales de Amazon Aurora. Para obtener más información sobre las conmutaciones por error gestionadas y no planificadas, consulte Uso de la conmutación por error en una base de datos global de Amazon Aurora.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un controlador PostgreSQL de Java Database Connectivity (JDBC) para conectividad de aplicaciones
- Una base de datos global de Aurora basada en Amazon Aurora compatible con PostgreSQL
- Una base de datos de Oracle Real Application Clusters (RAC) migrada a la base de datos global de Aurora basada en Aurora compatible con PostgreSQL

Limitaciones de las bases de datos globales de Aurora

- Las bases de datos globales de Aurora no están disponibles en todas las regiones de AWS. Para obtener una lista de las regiones compatibles, consulte Bases de datos globales de Aurora con Aurora PostgreSQL.
- Para obtener información sobre las características no compatibles y otras limitaciones de las bases de datos globales de Aurora, consulte Limitaciones de las bases de datos globales de Amazon Aurora.

Versiones de producto

- Amazon Aurora, edición compatible con PostgreSQL, versión 10.14 o posterior

Arquitectura

Pila de tecnología de origen

- Base de datos de Oracle RAC de cuatro nodos
- Oracle GoldenGate

Arquitectura de origen

El siguiente diagrama muestra tres clústeres con Oracle RAC de cuatro nodos en diferentes regiones de AWS replicados mediante Oracle. GoldenGate

Pila de tecnología de destino

- Una base de datos global de Amazon Aurora de tres clústeres basada en Aurora compatible con PostgreSQL, con un clúster en la región principal y dos clústeres en diferentes regiones secundarias

Arquitectura de destino

Tools (Herramientas)

Servicios de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.
- Las bases de datos globales de Amazon Aurora abarcan varias regiones de AWS, lo que permite lecturas globales de baja latencia y proporcionan una recuperación rápida de cualquier interrupción que pueda afectar a toda una región de AWS.

Epics

Agregue regiones con instancias de base de datos de lectura

Tarea	Descripción	Habilidades requeridas
Adjunte uno o varios clústeres de Aurora secundarios.	En la Consola de administr ación de AWS, seleccione Amazon Aurora. Seleccione el clúster principal, elija Acciones y seleccione Añadir región en la lista desplegable.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Seleccione la clase de instancia.	Puede cambiar la clase de instancia del clúster secundario. Sin embargo, le recomendamos mantenerla igual que la clase de instancia del clúster principal.	Administrador de base de datos
Añada la tercera región.	Repita los pasos de esta épica para añadir un clúster en la tercera región.	Administrador de base de datos

Error en la base de datos global Aurora

Tarea	Descripción	Habilidades requeridas
Elimine el clúster secundario de la base de datos global de Aurora.	1. Seleccione el clúster principal en la página de Bases de datos. 2. Seleccione Eliminar de global para conmutar por error a un clúster secundario.	Administrador de base de datos
Puede volver a configurar la aplicación para desviar el tráfico de escritura al clúster que acaba de promover.	Cambie el punto de conexión de la aplicación por el del clúster recién promocionado.	Administrador de base de datos
Detenga la ejecución de cualquier operación de escritura en el clúster no disponible.	Detenga la aplicación y cualquier actividad del lenguaje de manipulación de datos (DML) en el clúster que ha eliminado.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Crear una base de datos global de Aurora.	Ahora puede crear una base de datos global de Aurora con el clúster recién promovido como clúster principal.	Administrador de base de datos

Inicie el clúster principal

Tarea	Descripción	Habilidades requeridas
Seleccione el clúster principal que se va a iniciar desde la base de datos global.	En la consola de Amazon Aurora, en la configuración de la base de datos global, elija el clúster principal.	Administrador de base de datos
Iniciar el clúster.	En la lista desplegable Acciones, seleccione Iniciar. Este proceso puede tardar algún tiempo. Actualice la pantalla para ver el estado o compruebe, en la columna Estado, el estado actual del clúster una vez finalizada la operación.	Administrador de base de datos

Limpie los recursos

Tarea	Descripción	Habilidades requeridas
Elimine los clústeres secundarios restantes.	Tras completar el piloto de conmutación por error, elimine los clústeres secundarios de la base de datos global.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Elimine el clúster principal.	Eliminar el clúster.	Administrador de base de datos

Recursos relacionados

- Uso de bases de datos globales de Amazon Aurora
- Soluciones de recuperación de desastres de Aurora PostgreSQL mediante Base de datos global de Amazon Aurora (publicación de blog)

Implemente SHA1 el hash para los datos de PII al migrar de SQL Server a PostgreSQL

Rajkumar Raghuwanshi y Jagadish Kantubugata, Amazon Web Services

Resumen

Este patrón describe cómo implementar el hash del algoritmo de hash seguro 1 (SHA1) para las direcciones de correo electrónico al migrar de SQL Server a Amazon RDS for PostgreSQL o Amazon Aurora compatible con PostgreSQL. Una dirección de correo electrónico es un ejemplo de información de identificación personal (PII). La PII es información que, vista directamente o combinada con otros datos relacionados, puede utilizarse para deducir de manera razonable la identidad de una persona.

Este patrón cubre los desafíos de mantener valores hash coherentes en diferentes intercalaciones de bases de datos y codificaciones de caracteres, y proporciona una solución con funciones y desencadenadores de PostgreSQL. Si bien este patrón se centra en el uso de SHA1 hash, se puede adaptar a otros algoritmos de hash compatibles con el módulo de PostgreSQL. `pgcrypto` Tenga siempre en cuenta las implicaciones de seguridad de su estrategia de hash y consulte con expertos en seguridad si maneja información confidencial.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- La base de datos de SQL Server de origen
- La base de datos de PostgreSQL de destino (Amazon RDS para PostgreSQL o Aurora compatible con PostgreSQL)
- Experiencia en codificación PL/pgSQL

Limitaciones

- Este patrón requiere cambios en la intercalación en el nivel de base de datos en función de los casos de uso.
- No se ha evaluado el impacto en el rendimiento de conjuntos de datos de gran tamaño.
- Algunos Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver

los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- Microsoft SQL Server 2012 o posterior

Arquitectura

Pila de tecnología de origen

- SQL Server
- .NET Framework

Pila de tecnología de destino

- PostgreSQL
- Extensión `pgcrypto`

Automatización y escala

- Considere la posibilidad de implementar la función de hash como un procedimiento almacenado para facilitar el mantenimiento.
- Para conjuntos de datos grandes, evalúe el rendimiento y considere el procesamiento por lotes o las estrategias de indexación.

Tools (Herramientas)

Servicios de AWS

- Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, totalmente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.
- AWS Database Migration Service (AWS DMS) le ayuda a migrar los almacenes de datos a una combinación de configuraciones locales y en la nube Nube de AWS o entre ellas.

- Amazon Relational Database Service (Amazon RDS) para PostgreSQL lo ayuda a configurar, utilizar y escalar una base de datos relacional de PostgreSQL en la Nube de AWS.
- AWS Schema Conversion Tool (AWS SCT) admite migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayoría del código personalizado a un formato compatible con la base de datos de destino.

Otras herramientas

- pgAdmin es una herramienta de administración de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.
- SQL Server Management Studio (SSMS) es un entorno integrado para administrar infraestructuras de SQL Server.

Prácticas recomendadas

- Utilice la configuración de intercalación adecuada para gestionar los caracteres especiales en la base de datos de destino.
- Haga pruebas exhaustivas con una variedad de direcciones de correo electrónico, incluidas las direcciones con caracteres que no sean ASCII.
- Mantenga la coherencia en la gestión de mayúsculas y minúsculas entre las capas de aplicación y base de datos.
- Compare el rendimiento de las consultas utilizando los valores con hash.

Epics

Análisis de la implementación del hash de origen

Tarea	Descripción	Habilidades requeridas
Revisar el código de SQL Server.	Para revisar el código de SQL Server que genera SHA1 hashes, haga lo siguiente: • Analice la implementación actual del SHA1 hash en SQL Server.	Ingeniero de datos, administrador de base de datos, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	• Identifique los métodos exactos utilizados para la generación del hash. • Documente los parámetros de entrada y el formato de salida. • Revise cualquier conversión o transformación de tipo de datos. • Examine la configuración de intercalación y su impacto.	
Documentar el algoritmo de hash y las transformaciones de los datos.	Para documentar el algoritmo de hash exacto y las transformaciones de los datos, haga lo siguiente: • Cree documentación técnica detallada del proceso de hash. • Documente la lógica step-by-step de transformación. • Especifique los formatos de entrada y salida y los tipos de datos. • Incluya casos extremos y la gestión de caracteres especiales.	Desarrollador de aplicaciones, ingeniero de datos, administrador de base de datos

Creación de la función de hash de PostgreSQL

Tarea	Descripción	Habilidades requeridas
Crear la extensión `pgcrypto`.	Para crear la extensión `pgcrypto`, use `pgAdmin/psql` para ejecutar el siguiente comando: `CREATE EXTENSION pgcrypto;`	Administrador de base de datos, ingeniero de datos
Implementar una función de PostgreSQL.	Implemente la siguiente función de PostgreSQL para replicar la lógica de hash de SQL Server. En líneas generales, esta función utiliza los pasos siguientes: 1. Si lo desea, convierte la entrada a mayúsculas. 2. Crea un SHA1 hash de la entrada. 3. Toma los últimos 10 bytes (80 bits) de este hash. 4. Convierte estos bytes en un entero de 64 bits. `CREATE OR REPLACE FUNCTION utility.hex_to_bigint ( par_val character varying, par_upper character varying DEFAULT 'lower'::character varying)`	Ingeniero de datos, administrador de base de datos, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	RETURNS bigint
	LANGUAGE 'plpgsql'
	AS $BODY$
	DECLARE
	    retnumber bigint;
	    digest_bytes bytea;
	BEGIN
	    if lower(par_upper)
	 = 'upper'
	    then
	        digest_bytes :=
	 digest(upper(par_v
	al), 'sha1');
	    else
	        digest_bytes :=
	 digest((par_val),
	 'sha1');
	    end if;
	    retnumber := ('x'
	 || encode(substring(d
	igest_bytes, length(di
	gest_bytes)-10+1),
	 'hex'))::bit(64)::
	bigint;
	    RETURN retnumber;
	END;
	$BODY$;	

Tarea	Descripción	Habilidades requeridas

Pruebe la función.	Para probar la función, utilice datos de ejemplo de SQL Server para comprobar que los valores de hash coincidan. Use el siguiente comando:
	`select 'alejandro_rosalez@example.com' as Email, utility.hex_to_bigint('alejandro_rosalez@example.com', 'upper') as HashValue;`
	`--OUTPUT`
	`/*`
	`email hashvalue`
	`"alejandro_rosalez@example.com" 451397011176045063`
	`*/`
		Desarrollador de aplicaciones, administrador de base de datos, ingeniero de datos

Implementación de desencadenadores para el hash automático

Tarea	Descripción	Habilidades requeridas
Crear desencadenadores en las tablas pertinentes.	Para crear desencadenadores en las tablas pertinentes para generar automáticamente valores de hash al insertar o actualizar, ejecute el siguiente comando: `CREATE OR REPLACE FUNCTION update_email_hash()`	Desarrollador de aplicaciones, ingeniero de datos, administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	RETURNS TRIGGER
	AS $$
	BEGIN
	    NEW.email_hash =
	 utility.hex_to_big
	int(NEW.email,
	 'upper');
	    RETURN NEW;
	END;
	$$ LANGUAGE plpgsql;
	
	CREATE TRIGGER email_has
	h_trigger BEFORE INSERT
	 OR UPDATE ON users
	 FOR EACH ROW EXECUTE
	 FUNCTION update_em
	ail_hash();	

Migración de los datos existentes

Tarea	Descripción	Habilidades requeridas
Desarrolle o utilice un script de migración AWS DMS.	Desarrolle un script de migración o AWS DMS utilícelo para rellenar los valores hash de los datos existentes (incluidos los valores hash almacenados `BIGINT` en el sistema de origen). Realice los siguientes pasos: • Cree scripts de migración para la transferencia de datos con valores de hash.	Ingeniero de datos, desarrollador de aplicaciones, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	• Configure AWS DMS las tareas con las reglas de transformación adecuadas. • Configure los puntos finales de origen y destino en AWS DMS. • Implemente mecanismo s de gestión y registro de errores. • Diseñe una estrategia de procesamiento por lotes para conjuntos de datos grandes. • Cree consultas de validació n para la verificación de los datos.	

Tarea	Descripción	Habilidades requeridas
Utilizar la nueva función de hash de PostgreSQL.	Para utilizar la nueva función de hash de PostgreSQL y garantizar la coherencia, haga lo siguiente: • Implemente procedimientos de validación para verificar la coherencia del hash. • Cree scripts de comparación entre los sistemas de origen y destino. • Configure pruebas automatizadas para la verificación del valor de hash. • Documente cualquier discrepancia y los pasos para resolverlas.	Desarrollador de aplicaciones, administrador de bases de datos, ingeniero DevOps

Actualización de consultas de aplicaciones

Tarea	Descripción	Habilidades requeridas
Identificar las consultas de aplicaciones.	Para identificar las consultas de la aplicación que utilizan valores de hash, haga lo siguiente: • Analice la base de código de la aplicación en busca de consultas que utilicen valores de hash. • Revise los procedimientos y funciones almacenados	Desarrollador de aplicaciones, administrador de base de datos, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	que hacen referencia a las operaciones de hash. • Documente las métricas de rendimiento y los planes de ejecución de las consultas. • Identifique las dependencias en las búsquedas basadas en hash. • Planifique los componentes de la aplicación afectados.	
Modificar consultas.	Si es necesario, modifique las consultas para usar la nueva función de hash de PostgreSQL. Haga lo siguiente: • Refactorice las consultas existentes para usar la función de hash de PostgreSQL. • Actualice los procedimientos y las funciones almacenados. • Implemente y pruebe nuevos patrones de consulta. • Optimice el rendimiento de las consultas modificadas.	Desarrollador de aplicaciones, administrador de base de datos, ingeniero de datos

Prueba y validación

Tarea	Descripción	Habilidades requeridas
Hacer pruebas.	Para llevar a cabo pruebas exhaustivas con un subconjunto de datos de producción, haga lo siguiente: • Cree un plan de pruebas para la validación del subconjunto de datos. • Extraiga una muestra representativa de los datos de producción. • Configure un entorno de prueba con las configuraciones adecuadas. • Ejecute pruebas de carga y transformación de datos. • Haga pruebas de volumen y estrés.	Desarrollador de aplicaciones, ingeniero de datos, administrador de base de datos
Validar que los valores de hash coincidan.	Para validar que los valores de hash coincidan entre SQL Server y PostgreSQL, haga lo siguiente: • Desarrolle scripts de comparación para valores de hash. • Cree informes de validación para la coincidencia del hash.	Desarrollador de aplicaciones, ingeniero de datos, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	• Implemente procedimientos de verificación automatiz ados. • Documente cualquier discrepancia encontrada. • Analice y resuelva las faltas de coincidencia del hash.	
Verificar la funcionalidad de la aplicación.	Para verificar la funcionalidad de la aplicación mediante los datos migrados y la nueva implementación de hash, haga lo siguiente: • Ejecute las pruebas end-to-end de aplicaciones. • Valide todas las caracterí sticas de la aplicación mediante datos con hash. • Pruebe el rendimiento de la aplicación con la nueva implementación. • Verifique las integraciones y dependencias de las API.	Desarrollador de aplicacio nes, administrador de base de datos, ingeniero de datos

Resolución de problemas

Problema	Solución
Los valores de hash no coinciden.	Compruebe las codificaciones de caracteres y las intercalaciones entre el origen y el destino. Para obtener más información, consulte Administrar los cambios de intercalación en

Problema	Solución
	PostgreSQL en Amazon Aurora y Amazon AWS RDS (blog).

Recursos relacionados

AWS Blogs

- Manage collation changes in PostgreSQL on Amazon Aurora and Amazon RDS
- Migrate SQL Server to Amazon Aurora PostgreSQL using best practices and lessons learned from the field

Otros recursos

- PostgreSQL pgcrypto module (documentación de PostgreSQL)
- PostgreSQL trigger functions (documentación de PostgreSQL)
- SQL Server HASHBYTES function (documentación de Microsoft)

Migración gradual de Amazon RDS para Oracle a Amazon RDS para PostgreSQL con Oracle SQL Developer y AWS SCT

Pinesh Singal, Amazon Web Services

Resumen

Muchas estrategias y enfoques de migración se ejecutan en varias fases y pueden durar desde unas semanas hasta varios meses. Durante este tiempo, puede experimentar retrasos debido a la aplicación de parches o actualizaciones en las instancias de base de datos de Oracle de origen que desee migrar a las instancias de base de datos de PostgreSQL. Para evitar esta situación, le recomendamos que migre de forma incremental el código de base de datos de Oracle restante al código de base de datos de PostgreSQL.

Este patrón proporciona una estrategia de migración incremental sin tiempo de inactividad para una instancia de base de datos de Oracle de varios terabytes que tiene un número elevado de transacciones realizadas después de la migración inicial y que debe migrarse a una base de datos PostgreSQL. Puede utilizar el step-by-step enfoque de este patrón para migrar de forma incremental una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para Oracle a una instancia de base de datos de Amazon RDS for PostgreSQL sin iniciar sesión en la consola de administración de Amazon Web Services (AWS).

El patrón utiliza Oracle SQL Developer para encontrar las diferencias entre dos esquemas de la base de datos de Oracle de origen. A continuación, utilice la herramienta de conversión de esquemas de AWS (AWS SCT) para convertir los objetos de esquema de base de datos de Amazon RDS para Oracle en objetos de esquema de base de datos de Amazon RDS para PostgreSQL. A continuación, puede ejecutar un script de Python en la línea de comandos de Windows para crear objetos SCT de AWS para los cambios incrementales en los objetos de la base de datos de origen.

> **Note**
>
> Antes de migrar sus cargas de trabajo de producción, le recomendamos que ejecute una prueba de concepto (PoC) para el enfoque de este patrón en un entorno de pruebas o que no sea de producción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una instancia existente de base de datos de Amazon RDS para Oracle.
- Una instancia de base de datos de Amazon RDS para PostgreSQL.
- AWS SCT, instalado y configurado con controladores JDBC para motores de bases de datos de Oracle y PostgreSQL. Para obtener más información al respecto, consulte Instalación de AWS SCT e Instalación de los controladores de base de datos necesarios en la documentación de AWS SCT.
- Oracle SQL Developer, instalado y configurado. Para obtener más información acerca de estos componentes, consulte la documentación de Oracle SQL Developer.
- El archivo (adjunto) `incremental-migration-sct-sql.zip`, descargado en su equipo local.

Limitaciones

- Los requisitos mínimos para la instancia de base de datos de Amazon RDS para Oracle son:
  - Oracle versiones 10.2 y posteriores (para las versiones 10.x), 11g (versiones 11.2.0.3.v1 y posteriores) y hasta 12.2 y 18c para las ediciones Enterprise, Standard, Standard One y Standard Two
- Los requisitos mínimos para su instancia de base de datos de Amazon RDS para PostgreSQL de destino son:
  - PostgreSQL versiones 9.4 y posteriores (para las versiones 9.x), 10.x y 11.x
- En este patrón, se utiliza Oracle SQL Developer. Los resultados pueden variar si utiliza otras herramientas para buscar y exportar las diferencias de esquema.
- Los scripts SQL generados por Oracle SQL Developer pueden generar errores de transformación, lo que significa que es necesario realizar una migración manual.
- Si las conexiones de prueba de origen y destino de AWS SCT fallan, asegúrese de configurar las versiones del controlador JDBC y las reglas de entrada para que el grupo de seguridad de la nube privada virtual (VPC) acepte el tráfico entrante.

Versiones de producto

- Instancia de base de datos Amazon RDS para Oracle, versión 12.1.0.2 (versión 10.2 y posteriores)
- Instancia de base de datos Amazon RDS para PostgreSQL versión 11.5 (versión 9.4 y posteriores)
- Oracle SQL Developer, versión 19.1 y posteriores
- AWS SCT versión 1.0.632 y versiones posteriores

Arquitectura

Pila de tecnología de origen

- Instancia de base de datos de Amazon RDS para Oracle

Pila de tecnología de destino

- Amazon RDS para instancia de base de datos para PostgreSQL

Arquitectura de origen y destino

El siguiente diagrama muestra la migración de una instancia de base de datos Amazon RDS para Oracle a una instancia de base de datos Amazon RDS para PostgreSQL.

En el diagrama, se muestra el siguiente flujo de migración:

1. Abra Oracle SQL Developer y conéctese a las bases de datos de origen y destino.
2. Genere un informe de diferencias y, a continuación, genere el archivo de scripts SQL para los objetos de diferencias de esquema. Para obtener más información acerca de los informes de diferencias, consulte Informes de diferencias detallados en la documentación de Oracle.
3. Configure AWS SCT y ejecute el código de Python.
4. El archivo de scripts SQL se convierte de Oracle a PostgreSQL.
5. Ejecute el archivo de scripts SQL en la instancia de base de datos PostgreSQL de destino.

Automatizar y escalar

Para automatizar esta migración se pueden agregar parámetros adicionales y cambios relacionados con la seguridad para múltiples funcionalidades de un solo programa al Script de Python.

Tools (Herramientas)

- AWS SCT: la herramienta de conversión de esquemas de AWS (AWS SCT) convierte el esquema de base de datos existente de un motor de base de datos a otro.
- Desarrollador de Oracle SQL: Oracle SQL Developer es un entorno de desarrollo integrado (IDE) que simplifica el desarrollo y la administración de las bases de datos de Oracle, tanto en las implementaciones tradicionales como en las basadas en la nube.

Código

El archivo (adjunto) `incremental-migration-sct-sql.zip` contiene el código fuente completo de este patrón.

Epics

Cree el archivo de scripts SQL para las diferencias del esquema de la base de datos de origen

Tarea	Descripción	Habilidades requeridas
Ejecute Database Diff en Oracle SQL Developer.	1. Inicie sesión en la instancia de base de datos de Oracle de origen, seleccione Herramientas y, a continuación, elija Diferencias en base de datos. 2. Elija la base de datos de origen en Conexión con origen. 3. Elija la base de datos de origen actualizada o parcheada en Conexión de destino. 4. Configure las opciones restantes según sus requisitos, seleccione Siguiente y, a continuación, elija Finalizar para generar el informe de diferencias.	Administrador de base de datos
Genere el archivo de scripts SQL.	Elija Generar script para generar las diferencias en los archivos SQL. Esto genera el archivo de scripts SQL que AWS SCT utiliza para convertir la	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	base de datos de Oracle a PostgreSQL.	

Use el script de Python para crear los objetos de base de datos de destino en AWS SCT

Tarea	Descripción	Habilidades requeridas
Configure AWS SCT con la línea de comandos de Windows.	1. Copie el archivo `AWSSchemaConversionToolBatch.jar` de la carpeta AWS SCT preinstalada y péguelo en su directorio de trabajo. 2. Implemente el código Python desde el archivo `run_aws_sct_sql.py` de la carpeta (adjunto) `incremental-migration-sct-sql.zip` . Esto crea archivos.xml y archivos.sct en el directorio `projects` con los detalles de configuración del entorno de base de datos de origen y destino. También lee el archivo de scripts SQL que generó en Oracle SQL Developer. Por último, crea objetos de archivo.sql en el directorio `output`. 3. Configure los detalles de configuración del entorno de origen y destino en	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	el archivo `database_migration.txt` con el formato siguiente:
	
	`#source_vendor,source_hostname,source_dbname,source_user,source_pwd,source_schema,source_port,source_sid,target_vendor,target_hostname,target_user,target_pwd,target_dbname,target_port`
	
	`ORACLE,myoracledb.cokmvis0v46q.us-east-1.rds.amazonaws.com,ORCL,orcl,orcl1234,orcl,1521,ORCL,POSTGRESQL,mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com,pguser,pgpassword,pgdb,5432`
	
	4. Modifique los parámetros de configuración de AWS SCT según sus requisitos y, a continuación, copie el archivo de scripts SQL en el directorio de trabajo del subdirectorio `input`.	

Tarea	Descripción	Habilidades requeridas
Ejecutar el script de Python .	1. Ejecute el script de Python mediante el comando siguiente: `$ python run_aws_sct_sql.py database_migration.txt` 2. Esto crea el archivo SQL de los objetos de base de datos. Los códigos no convertidos con errores de transformación se pueden convertir manualmente.	Administrador de base de datos
Cree los objetos en Amazon RDS para PostgreSQL	Ejecute los archivos SQL y cree objetos en su instancia de base de datos de Amazon RDS para PostgreSQL.	Administrador de base de datos

Recursos relacionados

- Oracle en Amazon RDS
- PostgreSQL en Amazon RDS
- Uso de la interfaz de usuario de AWS SCT
- Uso de Oracle como origen para AWS SCT

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Cargar archivos BLOB en TEXT mediante la codificación de archivos en Aurora compatible con PostgreSQL

Bhanu Ganesh Gudivada y Jeevan Shetty, Amazon Web Services

Resumen

A menudo, durante la migración, hay casos en los que hay que procesar datos estructurados y no estructurados que se cargan desde archivos de un sistema de archivos local. Los datos también pueden estar en un juego de caracteres diferente del juego de caracteres de la base de datos.

Estos archivos contienen los siguientes tipos de datos:

- Metadatos – Estos datos describen la estructura del archivo.
- Datos semiestructurados – Son cadenas de texto en un formato específico, como JSON o XML. Es posible que pueda hacer afirmaciones sobre dichos datos, como "siempre empezará por '<' " o "no contiene caracteres de nueva línea".
- Texto completo – Estos datos suelen contener todos los tipos de caracteres, incluyendo los caracteres de nueva línea y comillas. También puede consistir en caracteres multibyte en UTF-8.
- Datos binarios: estos datos pueden contener bytes o combinaciones de bytes, incluidos valores nulos y end-of-file marcadores.

Cargar una combinación de estos tipos de datos puede ser complicado.

El patrón se puede utilizar con bases de datos Oracle locales, bases de datos Oracle que se encuentran en instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la nube de Amazon Web Services (AWS) y Amazon Relational Database Service (Amazon RDS) para bases de datos Oracle. Por ejemplo, este patrón utiliza Amazon Aurora de edición compatible con PostgreSQL.

En la base de datos de Oracle, con la ayuda de un puntero `BFILE` (archivo binario), el paquete `DBMS_LOB` y las funciones del sistema Oracle, puede cargar desde un archivo y convertirlo a CLOB con codificación de caracteres. Como PostgreSQL no admite el tipo de datos BLOB al migrar a una base de datos de Amazon Aurora de edición compatible con PostgreSQL, estas funciones deben convertirse en scripts compatibles con PostgreSQL.

Este patrón proporciona dos enfoques para cargar un archivo en una base de datos de una sola columna en una base de datos de Amazon Aurora compatible con PostgreSQL:

- Método 1: Usted importa datos de su bucket de Amazon Simple Storage Service (Amazon S3) utilizando la función `table_import_from_s3` de la extensión `aws_s3` con la opción de codificación.
- Método 2: Usted codifica en formato hexadecimal fuera de la base de datos y, a continuación, decodifica para ver `TEXT` dentro de la base de datos.

Recomendamos usar el Método 1 porque Aurora, compatible con PostgreSQL, tiene una integración directa con la extensión `aws_s3`.

Este patrón utiliza el ejemplo de cargar un archivo plano que contiene una plantilla de correo electrónico, que tiene caracteres multibyte y formatos distintos, en una base de datos de Amazon Aurora compatible con PostgreSQL.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una instancia de Amazon RDS o una instancia de Aurora compatible con PostgreSQL
- Conocimientos básicos de SQL y del sistema de administración de base de datos relacional (RDBMS)
- Un bucket de Amazon Simple Storage Service (Amazon S3)
- Conocimiento de las funciones del sistema en Oracle y PostgreSQL
- Paquete RPM HexDump -XXD-0.1.1 (incluido con Amazon Linux 2)

> **Note**
>
> Se acerca el fin de la compatibilidad de Amazon Linux 2. Para obtener más información, consulte Amazon Linux 2 FAQs.

Limitaciones

- Para el tipo de datos `TEXT`, la cadena de caracteres más larga posible que se puede almacenar es de aproximadamente 1 GB.

Versiones de producto

- Aurora es compatible con las versiones de PostgreSQL que aparecen en las actualizaciones de PostgreSQL de Amazon Aurora.

Arquitectura

Pila de tecnología de destino

- Aurora compatible con PostgreSQL

Arquitectura de destino

Método 1: Uso de aws_s3.table_import_from_s3

Desde un servidor en las instalaciones, se transfiere a Amazon S3 un archivo que contiene una plantilla de correo electrónico con caracteres multibyte y un formato personalizado. La función de base de datos personalizada que proporciona este patrón utiliza la función `aws_s3.table_import_from_s3` con `file_encoding` para cargar archivos en la base de datos y regresar los resultados de las consultas como tipo de datos `TEXT`.

1. Los archivos se transfieren al bucket de S3 de almacenamiento temporal.
2. Los archivos se cargan en la base de datos Amazon Aurora compatible con PostgreSQL.
3. Mediante el cliente pgAdmin, la función `load_file_into_clob` personalizada se implementa en la base de datos Aurora.
4. La función personalizada usa internamente `table_import_from_s3` con file_encoding. El resultado de la función se obtiene utilizando `array_to_string` y `array_agg` como salida `TEXT`.

Método 2: Codificar en hexadecimal fuera de la base de datos y decodificar para ver el TEXTO dentro de la base de datos

Un archivo de un servidor en las instalaciones o de un sistema de archivos local se convierte en un volcado hexadecimal. A continuación, el archivo se importa a PostgreSQL como un campo `TEXT`.

1. Convierta el archivo en un volcado hexadecimal en la línea de comandos mediante la opción `xxd -p`.

2. Cargue los archivos de volcado hexadecimales en una versión de Aurora compatible con PostgreSQL mediante la opción `\copy` y, a continuación, decodifique los archivos de volcado hexadecimales en binarios.
3. Codifique los datos binarios para regresarlos como `TEXT`.

Tools (Herramientas)

Servicios de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.

Otras herramientas

- pgAdmin4 es una plataforma de administración y desarrollo de código abierto para PostgreSQL. pgAdmin4 se puede usar en Linux, Unix, mac OS y Windows para administrar PostgreSQL.

Epics

Método 1: Importación de datos de Amazon S3 a Aurora compatible con PostgreSQL

Tarea	Descripción	Habilidades requeridas
Lance una EC2 instancia.	Para obtener instrucciones sobre cómo lanzar una instancia, consulte Lanzar su instancia.	Administrador de base de datos
Instale la herramien ta pgAdmin del cliente PostgreSQL.	Descargue e instale pgAdmin.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree una política de IAM.	Cree una de política AWS Identity and Access Management (IAM) denominada `aurora-s3-access-pol` que conceda acceso al bucket de S3 en el que se almacenar án los archivos. Use el siguiente código, sustituye ndo `<bucket-name>` por el nombre de su bucket de S3. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "s3:GetObject", "s3:AbortMultipartUpload", "s3:DeleteObject", "s3:ListMultipartUploadParts", "s3:PutObject", "s3:ListBucket" ], "Resource": [`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	<pre>"arn:aws:s3:::<bucket-name>/*",
	
	"arn:aws:s3:::<bucket-name>"
	]
	}
	]
	}</pre>	

Cree un rol de IAM para la importación de objetos de Amazon S3 a Aurora compatible con PostgreSQL.	Usa el siguiente código para crear un rol de IAM denominado `aurora-s3-import-role` con la relación de AssumeRole confianza. `AssumeRole` permite a Aurora acceder a otros servicios de AWS en su nombre.
	
	<pre>{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Effect": "Allow","Principal": {
	"Service": "rds.amazonaws.com"
	},"Action": "sts:AssumeRole"
	}
	]
	}</pre>
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Asocie el rol de IAM al clúster.	Para asociar el rol de IAM al clúster de base de datos compatible con Aurora PostgreSQL, ejecute el siguiente comando de la CLI de AWS. Cambie `<Account-ID>` al ID de la cuenta de AWS que aloja la base de datos Aurora compatible con PostgreSQL. Esto permite que la base de datos Aurora compatible con PostgreSQL acceda al bucket de S3. `aws rds add-role-to-db-cluster --db-cluster-identifier aurora-postgres-cl --feature-name s3Import --role-arn arn:aws:iam::<Account-ID>:role/aurora-s3-import-role`	Administrador de base de datos
Cargue el ejemplo en Amazon S3.	1. En la sección de Información adicional de este patrón, copie el código de la plantilla de correo electrónico en un archivo denominado `salary.event.notification.email.vm` . 2. Cargue el archivo en el bucket de S3.	Administrador de base de datos, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Implemente la función personalizada.	1. En la sección Información adicional, copie el contenido del archivo SQL `load_file_into_clob` de la función personalizada en una tabla temporal. 2. Inicie sesión en la base de datos Aurora compatible con PostgreSQL e impleméntela en el esquema de la base de datos mediante el cliente pgAdmin.	Administrador de base de datos, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas

Ejecute la función personalizada para importar los datos en la base de datos.	Ejecute el siguiente comando SQL y sustituya los elementos entre paréntesis angulares por los valores adecuados.
	`select load_file _into_clob('aws-s3 -import-test'::tex t,'us-west-1'::tex t,'employee.salary .event.notificatio n.email.vm'::text);`
	Sustituya los elementos entre paréntesis angulares por los valores adecuados, como se muestra en el siguiente ejemplo, antes de ejecutar el comando.
	`Select load_file _into_clob('aws-s3 -import-test'::tex t,'us-west-1'::tex t,'employee.salary .event.notificatio n.email.vm'::text);`
	El comando carga el archivo desde Amazon S3 y regresa el resultado como TEXT.
		Administrador de base de datos, propietario de la aplicación

Método 2: Convertir el archivo de plantilla en un volcado hexadecimal en un sistema Linux local

Tarea	Descripción	Habilidades requeridas
Convierta el archivo de plantilla en un volcado hexadecimal.	**Note** La utilidad Hexdump muestra el contenido de los archivos binarios en formato hexadecimal, decimal, octal o ASCII. El comando `hexdump` forma parte del paquete `util-linux` y viene preinstalado en las distribuciones de Linux. El paquete RPM Hexdump también forma parte de Amazon Linux 2. (: Amazon Linux 2 está a punto de finalizar el soporte. Para obtener más información, consulte Amazon Linux 2 FAQs.) Para convertir el contenido del archivo en un volcado hexadecimal, ejecute el siguiente comando del intérprete de comandos.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	`xxd -p </path/file.vm> | tr -d '\n' > </path/file.hex>`
	
	Sustituya la ruta y el archivo por los valores adecuados, como se muestra en el siguiente ejemplo.
	
	`xxd -p employee.salary.event.notification.email.vm | tr -d '\n' > employee.salary.event.notification.email.vm.hex`	

Tarea	Descripción	Habilidades requeridas
Cargue el archivo hexdump en el esquema de la base de datos.	Utilice los siguientes comandos para cargar el archivo hexdump en la base de datos Aurora compatible con PostgreSQL. 1. Inicie sesión en la base de datos PostgreSQL de Aurora y cree una tabla nueva llamada `email_template_hex` . ``` CREATE TABLE email_template_hex(hex_data TEXT); ``` 2. Cargue los archivos del sistema de archivos local en el esquema de base de datos mediante el siguiente comando. ``` \copy email_template_hex FROM '/path/file.hex'; ``` Sustituya la ruta por la ubicación del sistema de archivos local. ``` \copy email_template_hex FROM '/tmp/employee.salary.event.notification.email.vm.hex'; ```	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	3. Cree una tabla más llamada `email_template_bytea` .
	
	`CREATE TABLE email_template_bytea(hex_data bytea);`
	
	4. Inserte los datos desde `email_template_hex` a `email_template_bytea` .
	
	`INSERT INTO email_template_bytea (hex_data)`
	
	`(SELECT decode(hex_data, 'hex') FROM email_template_hex limit 1);`
	
	5. Para devolver el código de bytes hexadecimales como datos TEXT, ejecute el siguiente comando.
	
	`SELECT encode(hex_data::bytea, 'escape') FROM email_template_bytea;`	

Recursos relacionados

Referencias

- Utilizar una base de datos PostgreSQL como objetivo para el servicio de migración de bases de datos de AWS
- Manual de migración de la base de datos de Oracle 19c a Amazon Aurora con compatibilidad con PostgreSQL (12.4)
- Crear políticas de IAM
- Asociación de un rol de IAM con un clúster de base de datos Amazon Aurora MySQL
- pgAdmin

Tutoriales

- Introducción a Amazon RDS
- Migración de Oracle a Amazon Aurora

Información adicional

Función personalizada load_file_into_clob

```
CREATE OR REPLACE FUNCTION load_file_into_clob(
    s3_bucket_name text,
    s3_bucket_region text,
    file_name text,
    file_delimiter character DEFAULT '&'::bpchar,
    file_encoding text DEFAULT 'UTF8'::text)
    RETURNS text
    LANGUAGE 'plpgsql'
    COST 100
    VOLATILE PARALLEL UNSAFE
AS $BODY$
DECLARE
    blob_data BYTEA;
    clob_data TEXT;
    l_table_name CHARACTER VARYING(50) := 'file_upload_hex';
    l_column_name CHARACTER VARYING(50) := 'template';
    l_return_text TEXT;
    l_option_text CHARACTER VARYING(150);
    l_sql_stmt CHARACTER VARYING(500);

BEGIN
```

```
   EXECUTE format ('CREATE TEMPORARY TABLE %I (%I text, id_serial serial)',
 l_table_name, l_column_name);

   l_sql_stmt := 'select ''(format text, delimiter ''''' || file_delimiter || ''''',
 encoding ''''' || file_encoding ||  ''''')'' ';

   EXECUTE FORMAT(l_sql_stmt)
   INTO l_option_text;

   EXECUTE FORMAT('SELECT aws_s3.table_import_from_s3($1,$2,$6,
 aws_commons.create_s3_uri($3,$4,$5))')
   INTO l_return_text
   USING l_table_name, l_column_name, s3_bucket_name,
 file_name,s3_bucket_region,l_option_text;

   EXECUTE format('select array_to_string(array_agg(%I order by id_serial),E''\n'')
 from %I', l_column_name, l_table_name)
   INTO clob_data;

   drop table file_upload_hex;

   RETURN clob_data;
END;
$BODY$;
```

Plantilla de correo electrónico

```
##############################################################################################
##
 ##
##    johndoe Template Type: email
 ##
##    File: johndoe.salary.event.notification.email.vm
 ##
##    Author: Aimée Étienne    Date 1/10/2021
      ##
##  Purpose: Email template used by EmplmanagerEJB to inform a johndoe they         ##
##        have been given access to a salary event
 ##
##    Template Attributes:
 ##
```

```
##        invitedUser - PersonDetails object for the invited user
  ##
##        salaryEvent - OfferDetails object for the event the user was given access
 ##
##        buyercollege - CompDetails object for the college owning the salary event
 ##
##        salaryCoordinator - PersonDetails of the salary coordinator for the event
 ##
##        idp - Identity Provider of the email recipient
 ##
##        httpWebRoot - HTTP address of the server
 ##
##
 ##
#################################################################################

$!invitedUser.firstname $!invitedUser.lastname,

Ce courriel confirme que vous avez ete invite par $!salaryCoordinator.firstname $!
salaryCoordinator.lastname de $buyercollege.collegeName a participer a l'evenement
 "$salaryEvent.offeringtitle" sur johndoeMaster Sourcing Intelligence.

Votre nom d'utilisateur est $!invitedUser.username

Veuillez suivre le lien ci-dessous pour acceder a l'evenement.

${httpWebRoot}/myDashboard.do?idp=$!{idp}

Si vous avez oublie votre mot de passe, utilisez le lien "Mot de passe oublie" situe
 sur l'ecran de connexion et entrez votre nom d'utilisateur ci-dessus.

Si vous avez des questions ou des preoccupations, nous vous invitons a
 communiquer avec le coordonnateur de l'evenement $!salaryCoordinator.firstname $!
salaryCoordinator.lastname au ${salaryCoordinator.workphone}.

*******

johndoeMaster Sourcing Intelligence est une plateforme de soumission en ligne pour les
 equipements, les materiaux et les services.

Si vous avez des difficultes ou des questions, envoyez un courriel a
 support@johndoeMaster.com pour obtenir de l'aide.
```

Migre Amazon RDS for Oracle a Amazon RDS for PostgreSQL con y utilizando y AWS SCT AWS DMS AWS CLI CloudFormation

Pinesh Singal, Amazon Web Services

Resumen

Este patrón muestra cómo migrar una instancia de base de datos Amazon Relational Database Service (Amazon RDS) para Oracle de varios terabytes a una instancia de base de datos Amazon RDS for PostgreSQL mediante (). AWS Command Line Interface AWS CLI Este enfoque proporciona un tiempo de inactividad mínimo y no requiere iniciar sesión en la Consola de administración de AWS.

Este patrón ayuda a evitar las configuraciones manuales y las migraciones individuales mediante el uso de las consolas () y (). AWS Schema Conversion Tool AWS SCT AWS Database Migration Service AWS DMS La solución establece una configuración única para varias bases de datos y realiza las migraciones utilizando AWS SCT y AWS DMS en. AWS CLI

El patrón se utiliza AWS SCT para convertir los objetos del esquema de la base de datos de Amazon RDS for Oracle a Amazon RDS para PostgreSQL y, a continuación, AWS DMS se utiliza para migrar los datos. Al utilizar scripts de Python AWS CLI, se crean AWS SCT objetos y AWS DMS tareas con una CloudFormation plantilla.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.
- Una instancia existente de base de datos de Amazon RDS para Oracle.
- Una instancia de base de datos de Amazon RDS para PostgreSQL.
- Una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o una máquina local con sistema operativo Windows o Linux para ejecutar scripts.
- Comprensión de los siguientes tipos de tareas de AWS DMS migración:`full-load`,`cdc`,`full-load-and-cdc`. Para obtener más información, consulte Crear una tarea en la AWS DMS documentación.
- AWS SCT instalado y configurado con controladores JDBC (Java Database Connectivity) para motores de bases de datos de Oracle y PostgreSQL. Para obtener más información, consulte Instalación y configuración AWS SCT en la AWS SCT documentación.

- El `AWSSchemaConversionToolBatch.jar` archivo de la AWS SCT carpeta instalada, copiado en su directorio de trabajo.
- El archivo `cli-sct-dms-cft.zip` (adjunto), descargado y extraído en el directorio de trabajo.
- La versión más reciente AWS DMS del motor de instancias de replicación. Para obtener más información, consulte Cómo crear una instancia de AWS DMS replicación en la AWS Support documentación y las notas de la AWS DMS versión.
- AWS CLI versión 2, instalada y configurada con el identificador de la clave de acceso, la clave de acceso secreta y el Región de AWS nombre predeterminado de la EC2 instancia o el sistema operativo en el que se ejecutan los scripts. Para obtener más información, consulte Instalación o actualización a la versión más reciente AWS CLI y Configuración de los ajustes AWS CLI de la AWS CLI documentación.
- Familiaridad con las CloudFormation plantillas. Para obtener más información, consulte Cómo CloudFormation funciona en la CloudFormation documentación.
- Python versión 3, instalado y configurado en la EC2 instancia o el sistema operativo donde se ejecutan los scripts. Para obtener más información, consulte la documentación de Python.

Limitaciones

- Los requisitos mínimos para la instancia de base de datos de Amazon RDS para Oracle son:
  - Versiones 12c (12.1.0.2, 12.2.0.1), 18c (18.0.0.0) y 19c (19.0.0.0) de Oracle para las ediciones Enterprise, Standard, Standard One y Standard Two.
  - Aunque Amazon RDS es compatible con Oracle 18c (18.0.0.0), esta versión está en desuso porque Oracle ya no proporciona parches para 18c después de esa fecha. end-of-support Para obtener más información, consulte Amazon RDS para Oracle en la documentación de Amazon RDS.
  - Amazon RDS para Oracle 11g ya no se admite.
- Los requisitos mínimos para la instancia de base de datos de Amazon RDS para PostgreSQL son:
  - Versiones 9 (9.5 y 9.6), 10.x, 11.x, 12.x y 13.x de PostgreSQL.

Versiones de producto

- Instancia de Amazon RDS para Oracle DB versión 12.1.0.2 y posterior
- Instancia de Amazon RDS para PostgreSQL DB versión 11.5 y posterior
- AWS CLI versión 2

- La última versión de AWS SCT
- La versión más reciente de Python 3

Arquitectura

Pila de tecnología de origen

- Amazon RDS para Oracle

Pila de tecnología de destino

- Amazon RDS para PostgreSQL

Arquitectura de origen y destino

El siguiente diagrama muestra la migración de una instancia de base de datos de Amazon RDS for Oracle a una instancia de base de datos de Amazon RDS for PostgreSQL AWS DMS mediante scripts de Python.

En el diagrama, se muestra el siguiente flujo de trabajo de migración:

1. El script de Python se utiliza AWS SCT para conectarse a las instancias de base de datos de origen y destino.
2. El usuario comienza AWS SCT con el script de Python, convierte el código de Oracle en código PostgreSQL y lo ejecuta en la instancia de base de datos de destino.
3. El script de Python crea tareas de AWS DMS replicación para las instancias de base de datos de origen y destino.
4. El usuario despliega scripts de Python para iniciar las AWS DMS tareas y, a continuación, las detiene una vez finalizada la migración de datos.

Automatización y escala

Para automatizar esta migración, se pueden agregar parámetros y cambios relacionados con la seguridad al script de Python a fin de proporcionar funcionalidad adicional.

Tools (Herramientas)

- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar con los servicios de AWS mediante comandos en el shell de la línea de comandos.
- CloudFormationle ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y administrarlos a lo largo de su ciclo de vida en todas Cuentas de AWS las regiones. Este patrón convierte el archivo de entrada `.csv` en un archivo de entrada `.json` mediante un script de Python. El `.json` archivo se utiliza en AWS CLI los comandos para crear una CloudFormation pila que cree varias tareas de AWS DMS replicación con los nombres de los recursos de Amazon (ARNs), los tipos de migración, la configuración de las tareas y las asignaciones de tablas.
- AWS Database Migration Service (AWS DMS) le ayuda a migrar los almacenes de datos a una combinación de configuraciones locales y en la nube Nube de AWS o entre ellas. Este patrón se utiliza AWS DMS para crear, iniciar y detener tareas con un script de Python que se ejecuta en la línea de comandos y para crear la CloudFormation plantilla.
- AWS Schema Conversion Tool (AWS SCT) admite migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayoría del código personalizado a un formato compatible con la base de datos de destino. Este patrón requiere el `AWSSchemaConversionToolBatch.jar` archivo del directorio instalado AWS SCT .

Código

El archivo `cli-sct-dms-cft.zip` (adjunto) contiene el código fuente completo de este patrón.

Epics

Configure AWS SCT y cree objetos de base de datos en el AWS CLI

Tarea	Descripción	Habilidades requeridas
Configure AWS SCT para ejecutarse desde AWS CLI.	1. Configure los detalles de configuración del entorno de origen y destino en el archivo `database_migration.txt` con el formato siguiente:	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	<pre>#source_vendor,source_hostname,source_dbname,source_user,source_pwd,source_schema,source_port,source_sid,target_vendor,target_hostname,target_user,target_pwd,target_dbname,target_port
	ORACLE,myoracledb.cokmvis0v46q.us-east-1.rds.amazonaws.com,ORCL,orcl,orcl1234,orcl,1521,ORCL,POSTGRESQL,mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com,pguser,pgpassword,pgdb,5432</pre> 2. Modifique los parámetros de AWS SCT configuración según sus requisitos en los siguientes archivos: `project_settings.xml` `Oracle_PG_Test_Batch.xml` , y `ORACLE-orcl-to-POSTGRESQL.xml` .	

Tarea	Descripción	Habilidades requeridas
Ejecutar el script de Python `run_aws_sct.py` .	Ejecute el script de Python `run_aws_sct.py` mediante el comando siguiente: `$ python run_aws_sct.py database_migration.txt` El script de Python convierte los objetos de la base de datos de Oracle a PostgreSQL y crea archivos SQL en formato PostgreSQL. El script también crea el archivo `Database migration assessment report` PDF, que proporciona recomendaciones detalladas y estadísticas de conversión para los objetos de la base de datos.	Administrador de base de datos
Cree objetos en Amazon RDS para PostgreSQL.	1. Modifique manualmente los archivos SQL generados por AWS SCT, si es necesario. 2. Ejecute los archivos SQL y cree objetos en su instancia de base de datos de Amazon RDS para PostgreSQL.	Administrador de base de datos

Configure y cree AWS DMS tareas mediante el comando AWS CLI y CloudFormation

Tarea	Descripción	Habilidades requeridas
Cree una instancia AWS DMS de replicación.	Inicie sesión en Consola de administración de AWS, abra la AWS DMS consola y cree una instancia de replicaci ón que esté configurada de acuerdo con sus requisitos. Para obtener más información, consulte Crear una instancia de replicación en la AWS DMS documentación y Cómo crear una instancia de AWS DMS replicación en la AWS Support documentación.	Administrador de base de datos
Cree el punto de conexión de origen.	En la AWS DMS consola, elija Endpoints y, a continuación, cree un punto final de origen para la base de datos Oracle según sus necesidades. **Note** El atributo de conexión adicional debe ser `numberDat aTypeScale` con el valor `-2`. Para obtener más información, consulte Creación de puntos	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	finales de origen y destino en la AWS DMS documentación.	
Cree el punto de conexión de destino.	En la AWS DMS consola, elija Endpoints y, a continuación, cree un punto final de destino para la base de datos PostgreSQL según sus necesidades. Para obtener más información, consulte Crear puntos de enlace de origen y destino en la documentación. AWS DMS	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Configure los detalles de la AWS DMS replicación para que se ejecuten desde AWS CLI.	Configure los puntos finales de AWS DMS origen y destino y los detalles de la replicación en el `dms-arn-list.txt` archivo con el ARN del punto final de origen, el ARN del punto final de destino y el ARN de la instancia de replicación mediante el siguiente formato:
	`#sourceARN,targetARN,repARN`
	`arn:aws:dms:us-east-1:123456789012:endpoint:EH7AINRUDZ5GOYIY6HVMXECMCQ`
	`arn:aws:dms:us-east-1:123456789012:endpoint:HHJVUV57N7O3CQF4PJZKGIOYY5`
	`arn:aws:dms:us-east-1:123456789012:rep:LL57N77AQQAHHJF4PJFHNEDZ5G`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Ejecute el script de `dms-create-task.py` Python para crear las AWS DMS tareas.	1. Ejecute el script de Python `dms-create-task.py` mediante el comando siguiente: `$ python dms-create-task.py database_migration.txt dms-arn-list.txt <cft-stack-name> <migration-type>` donde: • `database_migration.txt` es el archivo de texto de migración de la base de datos. • `dms-arn-list.txt` es la lista de ARN de. AWS DMS • `<cft-stack-name>`es el nombre de la CloudFormation pila definido por el usuario. • `<migration-type>` es `full-load` , `cdc` o `full-load-and-cdc` . 2. Según el tipo de migración , puede usar los siguientes comandos para crear tres tipos de AWS DMS tareas: • `$ python dms-create-task.py database_migration`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`.txt dms-arn-list.txt dms-cli-cft-stack full-load` • `$ python dms-create-task.py database_migration.txt dms-arn-list.txt dms-cli-cft-stack cdc` • `$ python dms-create-task.py database_migration.txt dms-arn-list.txt dms-cli-cft-stack full-load-and-cdc`	
Compruebe que AWS DMS las tareas estén listas.	En la AWS DMS consola, comprueba que AWS DMS las tareas estén en `Ready` estado en la sección Estado.	Administrador de base de datos

Inicie y detenga las AWS DMS tareas mediante el AWS CLI

Tarea	Descripción	Habilidades requeridas
Inicie las AWS DMS tareas.	Ejecute el script de Python `dms-start-task.py` mediante el comando siguiente:	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`$ python dms-start-task.py start '<cdc-start-datetime>'` **Note** La fecha y la hora de inicio deben estar en los formatos `'DD-MON-YYYY'` o `'YYYY-MM-DDTHH:MI:SS'` (por ejemplo, `'01-Dec-2019'` o `'2018-03-08T12:12:12'`). Puede revisar el estado de la AWS DMS tarea en la pestaña de estadísticas de la tabla de la página Tareas de la AWS DMS consola.	

Tarea	Descripción	Habilidades requeridas
Valide los datos.	1. Una vez completada la migración de carga completa, la tarea se mantiene en ejecución de forma continua para CDC. 2. Cuando se complete el CDC o no sea necesario migrar más cambios, revise y valide los resultados y los datos de las tareas de migración en sus bases de datos de Oracle y PostgreSQL. Puede validar sus datos comprobando las columnas de estado y recuento (`Validation state`, `Validation pending` `Validation failed` `Validation suspended` , y `Validation details`) en la pestaña Estadísticas de la tabla de la tarea de migración de la base de datos de la página Tareas de la AWS DMS consola. Para obtener más información, consulte la validación de AWS DMS datos en la AWS DMS documentación.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Detenga las AWS DMS tareas.	Ejecute el script de Python mediante el comando siguiente: `$ python dms-start-task.py stop` **Note** AWS DMS es posible que las tareas se detengan con un `failed` estado, en función del estado de la validación. Para obtener más información, consulte la siguiente sección.	Administrador de base de datos

Resolución de problemas

Problema	Solución
AWS SCT las conexiones de prueba de origen y destino fallan.	Configure las versiones del controlador JDBC y las reglas de entrada del grupo de seguridad de VPC para que acepten el tráfico entrante.
La prueba del punto de conexión de origen o destino no se puede ejecutar.	Compruebe si la configuración del punto de conexión y la instancia de replicación están en estado `Available` . Compruebe si el estado de la conexión del punto de conexión es `Successful` .

Problema	Solución
	Para obtener más información, consulte Cómo solucionar los errores de conectividad de los puntos de conexión de los puntos de conexión de AWS DMS en la AWS Support documentación.
La carga completa no se puede ejecutar.	Compruebe si las bases de datos de origen y destino tienen tipos y tamaños de datos coincidentes. Para obtener más información, consulte la sección Solución de problemas de las tareas de migración AWS DMS en la AWS DMS documentación.
Se producen errores en la ejecución de la validación.	Compruebe si la tabla tiene una clave principal , ya que las tablas de claves no principales no están validadas. Si la tabla tiene una clave principal y errores, compruebe que el atributo de conexión adicional del punto de conexión de origen tenga `numberDataTypeScale=-2` . Para obtener más información, consulte la configuración de los terminales cuando se utiliza Oracle como fuente y la solución de problemas en la AWS DMS documentación. AWS DMSOracleSettings

Recursos relacionados

- Instalación y configuración AWS SCT
- Introduction to AWS DMS (video)
- Ejemplos de comandos de operación de CloudFormation pila para AWS CLI y PowerShell

- Navegar por la interfaz de usuario del AWS SCT
- Uso de una base de datos Oracle como fuente para AWS DMS
- Conectarse a bases de datos de Oracle con AWS SCT
- Uso de una base de datos PostgreSQL como destino para AWS DMS
- Orígenes para la migración de datos
- Destinos para la migración de datos
- formación de nubes (documentación)AWS CLI
- create-stack (documentación)AWS CLI
- dms (documentación)AWS CLI

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migración de Amazon RDS para Oracle a Amazon RDS para PostgreSQL en modo SSL mediante AWS DMS

Pinesh Singal, Amazon Web Services

Resumen

Este patrón proporciona una guía para migrar una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para Oracle a una base de datos de Amazon RDS para PostgreSQL en la nube de Amazon Web Services (AWS). Para cifrar las conexiones entre las bases de datos, el patrón utiliza la autoridad de certificación (CA) y el modo SSL en Amazon RDS y AWS Database Migration Service (AWS DMS).

El patrón describe una estrategia de migración en línea con poco o ningún tiempo de inactividad para una base de datos de origen de Oracle de varios terabytes con un número elevado de transacciones. Para garantizar la seguridad de los datos, el patrón utiliza SSL al transferir los datos.

Este patrón utiliza la herramienta de conversión de esquemas de AWS (AWS SCT) para convertir el esquema de base de datos de Amazon RDS para Oracle en un esquema de Amazon RDS para PostgreSQL. A continuación, el patrón utiliza AWS DMS para migrar los datos de la base de datos de Amazon RDS para Oracle a la base de datos de Amazon RDS para PostgreSQL.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Autoridad de certificación (CA) de bases de datos de Amazon RDS configurada únicamente con rds-ca-rsa2048-g1
  - El certificado rds-ca-2019 venció en agosto de 2024.
  - El certificado rds-ca-2015 venció el 5 de marzo de 2020
- AWS SCT
- AWS DMS
- pgAdmin
- Herramientas de SQL (por ejemplo, SQL Developer o SQL*Plus)

Limitaciones

- Base de datos Amazon RDS para Oracle: el requisito mínimo es para las versiones 19c de Oracle, para las ediciones Enterprise y Standard Two.
- Base de datos Amazon RDS para PostgreSQL: el requisito mínimo es para PostgreSQL versión 12 y versiones posteriores (para las versiones 9.x y posteriores).

Versiones de producto

- Instancia de base de datos de Amazon RDS para Oracle versión 12.1.0.2
- Instancia de base de datos de Amazon RDS para PostgreSQL versión 11.5

Arquitectura

Pila de tecnología de origen

- Una instancia de base de datos de Amazon RDS para Oracle con la versión 12.1.0.2.v18.

Pila de tecnología de destino

- AWS DMS
- Instancia de base de datos de Amazon RDS para PostgreSQL con la versión 11.5.

Arquitectura de destino

El diagrama siguiente muestra la arquitectura de migración de datos entre las bases de datos de Oracle (origen) y de PostgreSQL (destino). La arquitectura incluye lo siguiente:

- Una nube privada virtual (VPC)
- Una zona de disponibilidad
- Una subred privada
- Una base de datos de Amazon RDS para Oracle
- Una instancia de replicación de AWS DMS
- Una base de datos RDS para PostgreSQL

Para cifrar las conexiones de las bases de datos de origen y destino, los modos CA y SSL deben estar habilitados en Amazon RDS y AWS DMS.

Tools (Herramientas)

Servicios de AWS

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Amazon Relational Database Service (Amazon RDS) para Oracle le ayuda a configurar, utilizar y escalar una base de datos relacional de Oracle en la nube de AWS.
- Amazon Relational Database Service (Amazon RDS) para PostgreSQL le ayuda a configurar, utilizar y escalar una base de datos relacional de PostgreSQL en la nube de AWS.
- La Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado, lo que incluye las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino.

Otros servicios

- pgAdmin es una herramienta de administración de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.

Prácticas recomendadas

Amazon RDS proporciona nuevos certificados de entidad de certificación como una práctica recomendada de seguridad de AWS. Para obtener información sobre los nuevos certificados y las regiones de AWS compatibles, consulte Uso SSL/TLS para cifrar una conexión a una instancia de base de datos o un clúster.

Si su instancia de RDS tiene actualmente el certificado CA `rds-ca-2019` y desea actualizar a `rds-ca-rsa2048-g1`, siga las instrucciones que se indican en Actualización del certificado de entidad de certificación modificando la instancia o el clúster de base de datos o Actualización del certificado de entidad de certificación mediante la aplicación de mantenimiento.

Epics

Configurar la instancia de Amazon RDS para Oracle

Tarea	Descripción	Habilidades requeridas
Cree la instancia de base de datos de Oracle.	Inicie sesión en la cuenta de AWS, abra la Consola de administración de AWS y navegue hasta la consola de Amazon RDS. En la consola, seleccione Create database (Crear base de datos) y, a continuación, Oracle.	AWS general, administrador de bases de datos
Configure grupos de seguridad.	Configure grupos de seguridad entrantes y salientes.	AWS general
Cree un grupo de opciones.	Cree un grupo de opciones en la misma VPC y grupo de seguridad que la base de datos Amazon RDS para Oracle. En Option, seleccione SSL. Para Port, seleccione 2484 (para conexiones SSL).	AWS general
Configure los ajustes de las opciones.	Utilice los siguientes valores: • `SQLNET.CIPHER_SUITE : SSL_RSA_WITH_AES_256_CBC_SHA` • `SQLNET.SSL_VERSION : 1.2 or 1.0`	AWS general
Modifique la instancia de base de datos de RDS para Oracle.	Establezca el certificado de CA como rds-ca-rsa2048-g1.	Administrador de base de datos, AWS general

Tarea	Descripción	Habilidades requeridas
	En Option group (Grupo de opciones), adjunte el grupo de opciones creado anteriormente.	

Tarea	Descripción	Habilidades requeridas

Confirme que la instancia de base de datos de RDS para Oracle esté disponible.	Compruebe que la instancia de base de datos Amazon RDS para Oracle esté activa y en ejecución y que se pueda acceder al esquema de la base de datos.
	
	Para conectarse a la base de datos de RDS for Oracle, utilice el comando `sqlplus` de la línea de comandos.
	
	`$ sqlplus orcl/**** @myoracledb.cokmvis0v46q.us-east-1.rds.amazonaws.com:1521/ORCL`
	`SQL*Plus: Release 12.1.0.2.0 Production on Tue Oct 15 18:11:07 2019`
	`Copyright (c) 1982, 2016, Oracle. All rights reserved.`
	`Last Successful login time: Mon Dec 16 2019 23:17:31 +05:30`
	`Connected to:`
	`Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production`
	`With the Partitioning, OLAP, Advanced Analytics and Real Application Testing options`
	`SQL>`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree objetos y datos en la base de datos de RDS para Oracle.	Cree objetos e inserte datos en el esquema.	Administrador de base de datos

Configurar la instancia de Amazon RDS para PostgreSQL

Tarea	Descripción	Habilidades requeridas
Cree la base de datos de RDS para PostgreSQL.	En la página Create database (Crear base de datos) de la consola de Amazon RDS, seleccione PostgreSQL para crear una instancia de base de datos de Amazon RDS para PostgreSQL.	Administrador de base de datos, AWS general
Configure grupos de seguridad.	Configure grupos de seguridad entrantes y salientes.	AWS general
Cree un grupo de parámetros.	Si utiliza la versión 11.x de PostgreSQL, cree un grupo de parámetros para configura r los parámetros de SSL. En la versión 12 de PostgreSQL, el grupo de parámetros SSL está habilitado de forma predeterm inada.	AWS general
Edite los parámetros.	Cambie el parámetro `rds.force_ssl` por `1` (activado). De forma predeterminada, el parámetro `ssl` está	AWS general

Tarea	Descripción	Habilidades requeridas
	definido como 1 (activado). Al establecer el `rds.force_ssl` parámetro en 1, se obliga a todas las conexiones a conectarse únicamente a través del modo SSL.	
Modifique la instancia de base de datos RDS para PostgreSQL.	Establezca el certificado de CA como 2048-g1. rds-ca-rsa Adjunte el grupo de parámetros predeterminado o el grupo de parámetros creado anteriormente, según la versión de PostgreSQL.	Administrador de base de datos, AWS general

Tarea	Descripción	Habilidades requeridas

Confirme que la instancia de base de datos de RDS para PostgreSQL esté disponible.	Compruebe que la base de datos de Amazon RDS para PostgreSQL esté activa y en funcionamiento.
	
	El comando `psql` establece una conexión SSL con el conjunto `sslmode` desde la línea de comandos.
	
	Una opción es configurar `sslmode=1` en el grupo de parámetros y usar una conexión `psql` sin incluir el parámetro `sslmode` en el comando.
	
	El resultado siguiente muestra que la conexión SSL está establecida.
	
	`$ psql -h mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com -p 5432 "dbname=pgdb user=pguser"`
	`Password for user pguser:`
	`psql (11.3, server 11.5)`
	`SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)`
	`Type "help" for help.`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	pgdb=>
	
	Una segunda opción es configurar `sslmode=1` en el grupo de parámetros e incluir el parámetro `sslmode` en el comando `psql`.
	
	El resultado siguiente muestra que la conexión SSL está establecida.
	
	`$ psql -h mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com -p 5432 "dbname=pgdb user=pguser sslmode=require"`
	`Password for user pguser:`
	`psql (11.3, server 11.5)`
	`SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)`
	`Type "help" for help.`
	`pgdb=>`	

Configuración y ejecución de AWS SCT

Tarea	Descripción	Habilidades requeridas
Instale AWS SCT.	Instale la versión más reciente de la aplicación AWS SCT.	AWS general

Tarea	Descripción	Habilidades requeridas
Configure AWS SCT con controladores JDBC.	Descargue los controladores de conectividad de bases de datos Java (JDBC) para Oracle (ojdbc8.jar) y PostgreSQL (postgresql-42.2.5.jar). Para configurar los controladores en AWS SCT, seleccione Settings (Configuración), Global settings (Configuración global) y Drivers (Controladores).	AWS general

Tarea	Descripción	Habilidades requeridas
Cree el proyecto AWS SCT.	Cree el proyecto y el informe de AWS SCT con Oracle como motor de base de datos de origen y Amazon RDS para PostgreSQL como motor de base de datos de destino: 1. Pruebe las conexiones a la base de datos de Oracle de origen y a la base de datos de destino de Amazon RDS para PostgreSQL proporcionando los detalles de la conexión. Para la base de datos de Oracle de origen, se requieren los permisos o privilegios siguientes: • `CONNECT` • `SELECT_CATALOG_ROLE` • `SELECT ANY DICTIONARY` • `SELECT on SYS.USER$ TO <sct_user>` Para obtener más información, consulte Using Oracle Database as a source for AWS SCT (Usar la base de datos de Oracle como origen para AWS SCT).	AWS general

Tarea	Descripción	Habilidades requeridas
	Tanto las conexiones de origen como las de destino deben realizarse correctamente antes de que AWS SCT pueda iniciar el informe de migración. 2. Tras el informe, especifiq ue el esquema que desee convertir y seleccione Finish (Finalizar).	

Tarea	Descripción	Habilidades requeridas
Valide los objetos de la base de datos.	1. Seleccione Load schema (Cargar esquema). AWS SCT muestra los objetos de origen y de destino convertidos, incluidos los objetos que tienen errores. Actualice los objetos incorrectos en la base de datos de destino. 2. Revise los errores y elimínelos mediante una intervención manual. 3. Una vez eliminados todos los errores, vuelva a seleccionar Load schema (Cargar esquema). 4. Seleccione Aplicar a la base de datos. 5. Conéctese a pgAdmin o a cualquier herramienta que admita una conexión a base de datos PostgreSQL y compruebe el esquema y los objetos.	Administrador de base de datos, AWS general

Configurar y ejecutar AWS SCT

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación.	1. Inicie sesión en la cuenta, abra la Consola de administración de AWS y	AWS general

Tarea	Descripción	Habilidades requeridas
	navegue hasta la consola de AWS DMS. 2. Cree una instancia de replicación con una configuración válida para la VPC, el grupo de seguridad , la zona de disponibilidad y los atributos de conexión adicionales.	
Importe el certificado.	Descargue la agrupación de certificados (PEM) para su región de AWS. El paquete contiene los certificados intermedio y raíz de `rds-ca-2019` . El paquete también contiene los certificados CA raíz `rds-ca-rsa2048-g1` , `rds-ca-rsa4096-g1` y `rds-ca-ecc384-g1` . El almacén de confianza de la aplicación necesita registrar únicamente el certificado CA raíz.	AWS general

Tarea	Descripción	Habilidades requeridas
Cree el punto de conexión de origen.	1. Cree un punto de conexión de origen para Amazon RDS para Oracle; para ello, seleccione Select RDS DB instance (Seleccionar instancia de base de datos RDS) y, a continuación, seleccione la instancia de base de datos RDS para Oracle que ha creado. Los detalles de configuración del punto de conexión se rellenarán automáticamente. 2. Seleccione Provide access information manually (Proporcionar información de acceso manualmente). En Port, asegúrese de especificar 2484. 3. En Modo de capa de conexión segura (SSL), elija `verify-ca` y, a continuación, seleccione el certificado CA que creó anteriormente. 4. En Endpoint settings (Configuración de punto de conexión), agregue el atributo de conexión adicional `NumberDataTypeScale=-2` para admitir el tipo de datos `NUMBER` sin tamaño.	AWS general

Tarea	Descripción	Habilidades requeridas
	Para obtener información, consulte Using an Oracle database as a source for AWS Database Migration Service (AWS DMS) (Usar una base de datos de Oracle como origen para AWS Database Migration Service (AWS DMS)).	

Tarea	Descripción	Habilidades requeridas
Cree el punto de conexión de destino.	1. Cree un punto de conexión de destino para Amazon RDS para PostgreSQL; para ello, seleccione Select RDS DB instance (Seleccionar instancia de base de datos de RDS) y, a continuación, seleccione su instancia de base de datos de RDS para PostgreSQL. Los detalles de configuración del punto de conexión se rellenarán automáticamente. 2. Seleccione Provide access information manually (Proporcionar información de acceso manualmente). En Port, asegúrese de especificar 2484. Para obtener más información, consulte Using a PostgreSQL database as a target for AWS Database Migration Service (AWS DMS) (Usar una base de datos de PostgreSQL como destino para AWS Database Migration Service (AWS DMS)).	AWS general

Tarea	Descripción	Habilidades requeridas
Pruebe los puntos de conexión.	1. Pruebe los puntos de conexión de origen y destino para confirmar que ambos funcionen correctamente y estén disponibles. 2. Si una prueba tiene errores, asegúrese de que las reglas de entrada del grupo de seguridad sean válidas.	AWS general

Tarea	Descripción	Habilidades requeridas
Cree tareas de migración.	Para crear una tarea de migración para la captura completa de datos y cambios (CDC) o para la validación de datos, siga los pasos siguientes: 1. Para crear una tarea de migración de base de datos, seleccione la instancia de replicación, el punto de conexión de la base de datos de origen y el punto de conexión de la base de datos de destino. Especifique el tipo de migración de una de las maneras siguientes: • Migración de datos existentes (carga completa) • Replicate data changes only (CDC) (Replicar solo los cambios en los datos [CDC]) • Migrate existing data and replicate ongoing changes (Migración de los datos existentes y réplica de los cambios en curso) (carga completa y CDC) 2. En Table mappings (Asignaciones de tabla),	AWS general

Tarea	Descripción	Habilidades requeridas

	puede configurar las reglas de selección y las reglas de transformación en los formatos GUI o JSON:
	• En Selection rules (Reglas de selección), seleccione el esquema, especifique el nombre de la tabla y seleccione la acción (incluir o excluir) que desee configurar; por ejemplo, Schema ORCL, Table name %, Action Include.
	• En Transformation rules (Reglas de transform ación), realice una de las acciones siguientes:
	  • Seleccione el esquema y elija la acción (mayúscula, prefijo, sufijo); por ejemplo, Target Schema ORCL, Action Make lowercase .
	  • Seleccione el esquema, especifiq ue el nombre de la tabla y elija la acción (mayúsculas, prefijo, sufijo); por ejemplo, Target Schema ORCL, Table %, Action Make lowercase.	

Tarea	Descripción	Habilidades requeridas
	3. Activa la supervisión de Amazon CloudWatch Logs. 4. Para las reglas de asignación, añada el código JSON siguiente. `{ "rules": [ { "rule-type": "transformation", "rule-id": "1", "rule-name": "1", "rule-target": "table", "object-locator": { "schema-name": "%", "table-name": "%" }, "rule-action": "convert-lowercase", "value": null, "old-value": null }, { "rule-type": "transformation", "rule-id": "2",`	

Tarea	Descripción	Habilidades requeridas
	"rule-name": "2", "rule-target": "schema", "object-locator": { "schema-name": "ORCL", "table-name": "%" }, "rule-action": "convert-lowercase", "value": null, "old-value": null }, { "rule-type": "selection", "rule-id": "3", "rule-name": "3", "object-locator": { "schema-name": "ORCL", "table-name": "DEPT" }, "rule-action": "include", "filters": [] }]	

Tarea	Descripción	Habilidades requeridas
	<pre>}</pre>	
Planifique el ciclo de producción.	Confirme el tiempo de inactividad con las partes interesadas, como los propietarios de las aplicaciones, para ejecutar AWS DMS en los sistemas de producción.	Líder de migración

Tarea	Descripción	Habilidades requeridas
Ejecute la tarea de migración.	1. Inicie la tarea de AWS DMS que tenga el estado Listo y supervise los registros de tareas de migración en Amazon CloudWatch para detectar cualquier error. Si eligió Migrate existing data and replicate ongoing changes (Migración de los datos existentes y réplica de los cambios en curso) como tipo de migración , y el estado es Load complete ongoing replicati on (Carga completa, réplica en curso), se ha completad o la migración completa con los datos de CDC y la validación está en curso. 2. Tras iniciar la migración, puede obtener información adicional sobre la conexión SSL en. CloudWatch En el caso de Oracle, CloudWatc h muestra la siguiente cadena de conexión. `2019-12-17T09:15:1 1 [SOURCE_U NLOAD ]I: Connectin g to Oracle: Beginning session (oracle_endpoint_c onn.c:834)`	AWS general

Tarea	Descripción	Habilidades requeridas
	La cadena de conexión de PostgreSQL será similar a la del siguiente ejemplo. `2019-12-17T09:15:11 [TARGET_LOAD ]I: Going to connect to ODBC connection string: PROTOCOL=7.4-0;DRIVER={PostgreSQL};SERVER=mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com;DATABASE=pgdb;PORT=5432;sslmode=require;UID=pguser; (odbc_endpoint_imp.c:2218)`	

Tarea	Descripción	Habilidades requeridas
Valide los datos.	Revise los resultados y los datos de las tareas de migración en las bases de datos de Oracle de origen y PostgreSQL de destino: 1. Conéctese a pgAdmin y compruebe los datos de su base de datos PostgreSQL con el esquema `ORCL`. 2. En el caso de los CDC, compruebe los cambios en curso; para ello, inserte o actualice los datos en la base de datos de Oracle de origen.	Administrador de base de datos
Detenga la tarea de migración.	Tras completarse correctam ente la validación de datos, detenga la tarea de migración.	AWS general

Limpie los recursos

Tarea	Descripción	Habilidades requeridas
Elimine las tareas de AWS DMS.	1. En la consola de AWS DMS, vaya a Database migration tasks (Tareas de migración de bases de datos) y detenga cualquier tarea de AWS DMS en curso o en ejecución. 2. Seleccione la tarea o las tareas, luego, Actions y,	AWS general

Tarea	Descripción	Habilidades requeridas
	a continuación, Delete (Borrar).	
Elimine los puntos de conexión de AWS DMS.	Seleccione los puntos de conexión de origen y destino que creó, elija Actions y, a continuación Delete (Eliminar).	AWS general
Elimine la instancia de replicación de AWS DMS.	Seleccione la instancia de replicación, elija Actions y, a continuación, Delete (Eliminar).	AWS general
Elimine la base de datos de PostgreSQL.	1. En la consola de Amazon RDS, seleccione Databases (Bases de datos). 2. Seleccione la instancia de base de datos PostgreSQ L que creó, elija Actions y, a continuación, Delete (Eliminar).	AWS general
Elimine la base de datos de Oracle.	En la consola de Amazon RDS, seleccione la instancia de la base de datos de Oracle, elija Actions y, a continuación, Delete (Eliminar).	AWS general

Resolución de problemas

Problema	Solución
Las conexiones de prueba de origen y destino de AWS SCT no funcionan.	Configure las versiones del controlador JDBC y las reglas de entrada del grupo de seguridad de VPC para que acepten el tráfico entrante.

Problema	Solución
La prueba del punto de conexión de origen de Oracle no se puede ejecutar.	Compruebe la configuración del punto de conexión y si la instancia de replicación está disponible.
Se produce un error en la ejecución a plena carga de la tarea de AWS DMS.	Compruebe si las bases de datos de origen y destino tienen tipos y tamaños de datos coincidentes.
La tarea de migración de validación de AWS DMS devuelve errores.	1. Compruebe si la tabla tiene una clave principal. Las tablas sin clave principal no se validan. 2. Si la tabla tiene una clave principal pero genera errores, compruebe el atributo de conexión adicional en el punto de conexión de origen. El atributo de conexión adicional debe tener `numberDataTypeScale=-2` para admitir el tipo de datos `NUMBER` sin tamaño de forma dinámica en función de los datos disponibles en la tabla.

Recursos relacionados

Bases de datos

- Amazon RDS para Oracle
- Amazon RDS para PostgreSQL

SSL DB connection (Conexión de bases de datos SSL)

- Se utiliza SSL/TLS para cifrar una conexión a una instancia de base de datos
  - Using SSL with an RDS for Oracle DB instance (Usar SSL con una instancia de base de datos de RDS para Oracle)
  - Securing connections to RDS for PostgreSQL with SSL/TLS (Proteger las conexiones a RDS para PostgreSQL con SSL/TLS)

  - Descarga de agrupaciones de certificados para regiones de AWS específicas
    - Descarga del certificado raíz CA-2019 (que venció en agosto de 2024)
- Working with option groups (Trabajar con grupos de opciones)
  - Adding options to Oracle DB instances (Cómo añadir opciones a instancias de base de datos de Oracle)
  - Oracle Secure Sockets Layer (Capa de conexión segura de Oracle)
- Working with parameter groups (Trabajar con grupos de parámetros)
- PostgreSQL sslmode connection parameter (Parámetro de conexión sslmode de PostgreSQL)
- Using SSL from JDBC (Usar SSL desde JDBC)
- Rotación del certificado SSL/TLS
  - Actualización del certificado de CA mediante la modificación de la instancia de base de datos o el clúster
  - Actualizar su certificado de CA mediante la aplicación del mantenimiento

AWS SCT

- Herramienta de conversión de esquemas de AWS
- Guía del usuario de la herramienta de conversión de esquemas de AWS
- Uso de la interfaz de usuario de AWS SCT
- Using Oracle Database as a source for AWS SCT (Utilizar la base de datos de Oracle como origen para AWS SCT)

AWS DMS

- AWS Database Migration Service (AWS DMS)
- AWS Database Migration Service User Guide (Guía del usuario de AWS Database Migration Service)
  - Uso de una base de datos de Oracle como origen de AWS DMS
  - Using a PostgreSQL database as a target for AWS DMS (Utilizar una base de datos de PostgreSQL como destino para AWS DMS)
- Using SSL with AWS Database Migration Service (AWS DMS) (Usar SSL con AWS Database Migration Service (AWS DMS))
- Migración de aplicaciones que ejecutan bases de datos relacionales a AWS

Información adicional

Los certificados `rds-ca-2019` de la entidad de certificación de Amazon RDS vencieron en agosto de 2024. Si utiliza o tiene pensado utilizar SSL o TLS con verificación de certificados para conectarse a las instancias de base de datos de RDS o clústeres de base de datos multi-AZ, considere la posibilidad de utilizar uno de los certificados CA nuevos: `rds-ca-rsa2048-g1`, `rds-ca-rsa4096-g1` o `rds-ca-ecc384-g1`.

Migración de los paquetes pragma SERIALLY_REUTILIZABLE de Oracle a PostgreSQL

Vinay Paladi, Amazon Web Services

Resumen

Este patrón proporciona un step-by-step enfoque para migrar paquetes de Oracle que se definen como pragma SERIALLY_REUTILIZABLE a PostgreSQL en Amazon Web Services (AWS). Este enfoque mantiene la funcionalidad del pragma SERIALLY_REUTILIZABLE.

PostgreSQL no admite el concepto de paquetes ni el pragma SERIALLY_REUTILIZABLE. Para obtener una funcionalidad similar en PostgreSQL, puede crear esquemas para paquetes e implementar todos los objetos relacionados (como funciones, procedimientos y tipos) dentro de los esquemas. Para lograr la funcionalidad del pragma SERIALLY_REUTILIZABLE, el script de función contenedora de ejemplo que se proporciona en este patrón utiliza un paquete de extensiones de Herramienta de conversión de esquemas de AWS (AWS SCT).

Para obtener más información, consulte SERIALLY_REUSABLE Pragma en la documentación de Oracle.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- La versión más reciente de AWS SCT y los controladores necesarios
- Una base de datos de Edición compatible con Amazon Aurora PostgreSQL o una Amazon Relational Database Service (Amazon RDS) para PostgreSQL

Versiones de producto

- Oracle Database versión 10g y posteriores

Arquitectura

Pila de tecnología de origen

- Oracle Database en las instalaciones

Pila de tecnología de destino

- Aurora compatible con PostgreSQL o Amazon RDS para PostgreSQL
- AWS SCT

Arquitectura de migración

Tools (Herramientas)

Servicios de AWS

- La Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado, lo que incluye las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino.
- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.
- Amazon Relational Database Service (Amazon RDS) para PostgreSQL le ayuda a configurar, utilizar y escalar una base de datos relacional de PostgreSQL en la nube de AWS.

Otras herramientas

- pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.

Epics

Migración del paquete de Oracle mediante AWS SCT

Tarea	Descripción	Habilidades requeridas
Configure AWS SCT.	Configure la conectividad de AWS SCT con la base de datos de origen. Para obtener más información, consulte	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	Uso de una base de datos de Oracle como origen para AWS SCT.	
Convierta el script.	Utilice AWS SCT para convertir el paquete de Oracle seleccionando la base de datos de destino como compatible con Aurora PostgreSQL.	Administrador de base de datos, desarrollador
Guarde los archivos.sql.	Antes de guardar el archivo.sql, modifique la opción Configuración del proyecto en AWS SCT a Archivo único por etapa. AWS SCT separará el archivo.sql en varios archivos.sql según el tipo de objeto.	Administrador de base de datos, desarrollador
Cambie el código.	Abra la función `init` generada por AWS SCT y cámbiela como se muestra en el ejemplo de la sección Información adicional. Añadirá una variable para lograr la funcionalidad de `pg_serialize = 0` .	Administrador de base de datos, desarrollador
Pruebe la conversión.	Implemente la función `init` en la base de datos compatible con Aurora PostgreSQL y pruebe los resultados.	Administrador de base de datos, desarrollador

Recursos relacionados

- Herramienta de conversión de esquemas de AWS

- Amazon RDS
- Características de Amazon Aurora
- SERIALLY_REUTILIZABLE Pragma

Información adicional

```
Source Oracle Code:

CREATE OR REPLACE PACKAGE test_pkg_var
IS
PRAGMA SERIALLY_REUSABLE;
PROCEDURE function_1
 (test_id number);
PROCEDURE function_2
 (test_id number
 );
END;

CREATE OR REPLACE PACKAGE BODY test_pkg_var
IS
PRAGMA SERIALLY_REUSABLE;
v_char VARCHAR2(20) := 'shared.airline';
v_num number := 123;

PROCEDURE function_1(test_id number)
IS
begin
dbms_output.put_line( 'v_char-'|| v_char);
dbms_output.put_line( 'v_num-'||v_num);
v_char:='test1';
function_2(0);
END;

PROCEDURE function_2(test_id number)
is
begin
dbms_output.put_line( 'v_char-'|| v_char);
dbms_output.put_line( 'v_num-'||v_num);
END;
END test_pkg_var;

Calling the above functions
```

```
set serveroutput on


EXEC test_pkg_var.function_1(1);


EXEC test_pkg_var.function_2(1);


Target Postgresql Code:


CREATE SCHEMA test_pkg_var;

CREATE OR REPLACE FUNCTION test_pkg_var.init(pg_serialize IN INTEGER DEFAULT 0)

RETURNS void
AS
$BODY$

DECLARE

BEGIN

if aws_oracle_ext.is_package_initialized( 'test_pkg_var' ) AND pg_serialize = 0

then

return;

end if;

PERFORM aws_oracle_ext.set_package_initialized( 'test_pkg_var' );

PERFORM aws_oracle_ext.set_package_variable( 'test_pkg_var', 'v_char',
 'shared.airline.basecurrency'::CHARACTER

VARYING(100));

PERFORM aws_oracle_ext.set_package_variable('test_pkg_var', 'v_num', 123::integer);

END;
```

```
$BODY$

LANGUAGE plpgsql;


CREATE OR REPLACE FUNCTION test_pkg_var.function_1(pg_serialize int default 1)

RETURNS void
AS

$BODY$
DECLARE

BEGIN

PERFORM test_pkg_var.init(pg_serialize);

raise notice 'v_char%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_char');

raise notice 'v_num%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_num');

PERFORM aws_oracle_ext.set_package_variable( 'test_pkg_var', 'v_char',
 'test1'::varchar);

PERFORM test_pkg_var.function_2(0);
END;

$BODY$
LANGUAGE plpgsql;


CREATE OR REPLACE FUNCTION test_pkg_var.function_2(IN pg_serialize integer default 1)

RETURNS void

AS

$BODY$

DECLARE

BEGIN

PERFORM test_pkg_var.init(pg_serialize);
```

```
raise notice 'v_char%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_char');

raise notice 'v_num%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_num');

END;
$BODY$
LANGUAGE plpgsql;


Calling the above functions

select test_pkg_var.function_1()

 select test_pkg_var.function_2()
```

Migración de tablas externas de Oracle a Amazon Aurora compatible con PostgreSQL

Anuradha Chintha y Rakesh Raghav, Amazon Web Services

Resumen

Las tablas externas permiten a Oracle consultar los datos almacenados fuera de la base de datos en archivos planos. Puede usar el controlador ORACLE_LOADER para acceder a cualquier dato almacenado en cualquier formato que pueda cargar la utilidad SQL*Loader. No puede usar el Lenguaje de Manipulación de Datos (DML) en tablas externas, pero puede usar las tablas externas para operaciones de consulta, unión y clasificación.

Amazon Aurora compatible con PostgreSQL no proporciona una funcionalidad similar a las tablas externas de Oracle. En su lugar, debe adoptar la modernización para desarrollar una solución escalable que cumpla con los requisitos funcionales y sea eficiente.

Este patrón proporciona los pasos para migrar diferentes tipos de tablas externas de Oracle a la edición de Aurora compatible con PostgreSQL en la nube de Amazon Web Services (AWS) mediante la extensión `aws_s3`.

Recomendamos probar exhaustivamente esta solución antes de implementarla en un entorno de producción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de AWS (AWS CLI)
- Una instancia disponible de base de datos Aurora compatible con PostgreSQL.
- Una base de datos de Oracle en las instalaciones con una tabla externa
- API de pg.Client
- Archivos de datos

Limitaciones

- Este patrón no proporciona la funcionalidad necesaria para sustituir a las tablas externas de Oracle. Sin embargo, los pasos y el código de muestra se pueden mejorar aún más para lograr sus objetivos de modernización de la base de datos.

- Los archivos no deben contener el carácter que se emplea como delimitador en las funciones de exportación e importación de `aws_s3`.

Versiones de producto

- Para realizar la importación de Amazon S3 en RDS para PostgreSQL, la base de datos debe ejecutar la versión PostgreSQL 10.7 o posterior.

Arquitectura

Pila de tecnología de origen

- Oracle

Arquitectura de origen

Pila de tecnología de destino

- Amazon Aurora compatible con PostgreSQL
- Amazon CloudWatch
- AWS Lambda
- AWS Secrets Manager
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)

Arquitectura de destino

En el siguiente diagrama se muestra una representación de alto nivel de la solución.

1. Los archivos se cargan en el bucket de S3.
2. Se inicia la función de Lambda.
3. La función de Lambda inicia la llamada a la función de base de datos.
4. Secrets Manager proporciona las credenciales para acceder a la base de datos.

5. Según la función de la base de datos, se crea una alarma de SNS.

Automatizar y escalar

Cualquier adición o cambio en las tablas externas se puede gestionar mediante el mantenimiento de los metadatos.

Tools (Herramientas)

- Amazon Aurora compatible con PostgreSQL: la edición de Amazon Aurora compatible con PostgreSQL es un motor de bases de datos relacionales, completamente administrado, compatible con PostgreSQL y conforme a ACID, que combina la velocidad y la fiabilidad de las bases de datos comerciales de tecnología avanzada con la rentabilidad de las bases de datos de código abierto.
- AWS CLI: la interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta unificada para administrar los servicios de AWS. Con una única herramienta para descargar y configurar, puede controlar varios servicios de AWS desde la línea de comando y automatizarlos mediante scripts.
- Amazon CloudWatch: Amazon CloudWatch supervisa los recursos y la utilización de Amazon S3.
- AWS Lambda: AWS Lambda es un servicio de computación sin servidor que permite ejecutar código sin aprovisionar ni administrar servidores, crear una lógica de escalado de clústeres adaptada a las cargas de trabajo, mantener las integraciones de eventos o gestionar los tiempos de ejecución. En este patrón, Lambda ejecuta la función de base de datos cada vez que se carga un archivo en Amazon S3.
- AWS Secrets Manager: AWS Secrets Manager es un servicio de almacenamiento y recuperación de credenciales. Con Secrets Manager puede reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) proporciona una capa de almacenamiento que permite recibir y almacenar archivos para su consumo y transmisión hacia y desde el clúster de Aurora compatible con PostgreSQL.
- aws_s3: la extensión `aws_s3` integra Amazon S3 y Aurora compatible con PostgreSQL.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y administra la entrega o el envío de mensajes entre publicadores y clientes. En este patrón, Amazon SNS se usa para enviar notificaciones.

Código

Siempre que se ubique un archivo en el bucket de S3, se debe crear una función de base de datos a la que llamar desde la aplicación de procesamiento o la función de Lambda. Para obtener más información, consulte el código (adjunto).

Epics

Cree un archivo externo

Tarea	Descripción	Habilidades requeridas
Añada un archivo externo a la base de datos de origen.	Cree un archivo externo y trasládelo al directorio `oracle`.	Administrador de base de datos

Configure el objetivo (Aurora compatible con PostgreSQL)

Tarea	Descripción	Habilidades requeridas
Cree una base de datos de Aurora PostgreSQL.	Cree una instancia de base de datos en su clúster de Amazon Aurora compatible con PostgreSQL.	Administrador de base de datos
Cree un esquema, una extensión aws_s3 y tablas.	Use el código que aparece en la sección `ext_tbl_scripts` de Información adicional. Las tablas incluyen tablas reales, tablas de ensayo, tablas de errores y registros y una metatabla.	Administrador de base de datos, desarrollador
Cree la función de base de datos.	Para crear la función de base de datos, use el código que aparece bajo la función `load_external_table_latest` en la sección de Información adicional.	Administrador de base de datos, desarrollador

Creación y configuración de la función de Lambda

Tarea	Descripción	Habilidades requeridas
Crear un rol.	Cree un rol con permisos para acceder a Amazon S3 y a Amazon Relational Database Service (Amazon RDS). Esta función se asignará a Lambda para ejecutar el patrón.	Administrador de base de datos
Crear la función de Lambda.	Cree una función de Lambda que lea el nombre del archivo de Amazon S3 (por ejemplo, `file_key = info.get('object', {}).get('key') )` y llame a la función de base de datos (por ejemplo, `curs.call proc("load_externa l_tables", [file_key ]) )` con el nombre del archivo como parámetro de entrada. Según el resultado de la llamada a la función, se iniciará una notificac ión de SNS (por ejemplo, `client.publish(Top icArn='arn:',Messa ge='fileloadsucces s',Subject='filelo adsuccess') )`. En función de las necesidad es de su empresa, puede crear una función de Lambda	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	con código adicional si es necesario. Para más informaci ón, consulte la documentación de Lambda.	
Configure un desencadenante de eventos en el bucket de S3.	Configure un mecanismo para llamar a la función de Lambda en todos los eventos de creación de objetos en el bucket de S3.	Administrador de base de datos
Cree un secreto.	Cree un nombre secreto para las credenciales de la base de datos mediante Secrets Manager. Pase el secreto a la función de Lambda.	Administrador de base de datos
Cargue los archivos de soporte de Lambda.	Cargue un archivo .zip que contenga los paquetes de soporte de Lambda y el script de Python adjunto para conectar a Aurora compatibl e con PostgreSQL. El código Python llamará a la función que creó en la base de datos.	Administrador de base de datos
Cree un tema de SNS.	Cree un tema de SNS para enviar un correo si la carga de datos se ha realizado correctamente o no.	Administrador de base de datos

Cómo añadir integración con Amazon S3

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	En la consola de Amazon S3, cree un bucket de S3 con un nombre único que no contenga barras diagonales en el inicio. Un nombre de bucket de S3 es globalmente único y todas las cuentas de AWS comparten el espacio de nombres.	Administrador de base de datos
Cree políticas de IAM .	Para crear las políticas de AWS Identity and Access Management (IAM), use el código que se describe en la sección `s3bucketpolicy_for_import` de Información adicional.	Administrador de base de datos
Cree roles.	Cree dos roles para Aurora compatible con PostgreSQL, uno para Importar y otro para Exportar. Asigne las políticas correspondientes a los roles.	Administrador de base de datos
Adjunte los roles al clúster de Aurora compatible con PostgreSQL.	En Administrar roles, adjunte los roles de Importar y Exportar al clúster de Aurora PostgreSQL.	Administrador de base de datos
Cree objetos de apoyo para Aurora compatible con PostgreSQL.	Para las tablas de scripts, utilice el código de `ext_tbl_scripts` en la sección Información adicional.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Para la función personalizada, utilice el código de `load_external_Table_latest` en la sección Información adicional.	

Procese un archivo de prueba

Tarea	Descripción	Habilidades requeridas
Cargar un archivo en el bucket de S3.	Para cargar un archivo de prueba en el bucket de S3, use la consola o ejecute el siguiente comando en la CLI de AWS. `aws s3 cp /Users/Desktop/ukpost/exttbl/"testing files"/aps s3://s3importtest/inputext/aps` En cuanto se carga el archivo, el evento de bucket inicia la función de Lambda, que ejecuta la función Aurora compatible con PostgreSQL.	Administrador de base de datos
Compruebe los datos y los archivos de registro y error.	La función de Aurora compatible con PostgreSQL carga los archivos en la tabla principal y crea los archivos `.log` y `.bad` en el bucket de S3.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Supervise la solución.	En la CloudWatch consola de Amazon, supervise la función Lambda.	Administrador de base de datos

Recursos relacionados

- Integración de Amazon S3
- Amazon S3
- Trabajar con la versión de Amazon Aurora compatible con PostgreSQL
- AWS Lambda
- Amazon CloudWatch
- AWS Secrets Manager
- Configuración de notificaciones de Amazon SNS

Información adicional

ext_table_scripts

```
CREATE EXTENSION aws_s3 CASCADE;
CREATE TABLE IF NOT EXISTS meta_EXTERNAL_TABLE
(
    table_name_stg character varying(100) ,
    table_name character varying(100)  ,
    col_list character varying(1000)  ,
    data_type character varying(100)  ,
    col_order numeric,
    start_pos numeric,
    end_pos numeric,
    no_position character varying(100)  ,
    date_mask character varying(100)  ,
    delimeter character(1)  ,
    directory character varying(100)  ,
    file_name character varying(100)  ,
    header_exist character varying(5)
);
CREATE TABLE IF NOT EXISTS ext_tbl_stg
```

```
(
    col1 text
);
CREATE TABLE IF NOT EXISTS error_table
(
    error_details text,
    file_name character varying(100),
    processed_time timestamp without time zone
);
CREATE TABLE IF NOT EXISTS log_table
(
    file_name character varying(50) COLLATE pg_catalog."default",
    processed_date timestamp without time zone,
    tot_rec_count numeric,
    proc_rec_count numeric,
    error_rec_count numeric
);
sample insert scripts of meta data:
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'source_filename', 'character varying', 2, 8, 27, NULL, NULL, NULL, 'databasedev',
 'externalinterface/loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'record_type_identifier', 'character varying', 3, 28, 30, NULL, NULL, NULL,
 'databasedev', 'externalinterface/loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'fad_code', 'numeric', 4, 31, 36, NULL, NULL, NULL, 'databasedev', 'externalinterface/
loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'session_sequence_number', 'numeric', 5, 37, 42, NULL, NULL, NULL, 'databasedev',
 'externalinterface/loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'transaction_sequence_number', 'numeric', 6, 43, 48, NULL, NULL, NULL, 'databasedev',
 'externalinterface/loaddir/APS', 'NO');
```

s3bucketpolicy_for import

```
---Import role policy
--Create an IAM policy to allow, Get,  and list actions on S3 bucket
 {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "s3import",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::s3importtest",
                "arn:aws:s3:::s3importtest/*"
            ]
        }
    ]
}
--Export Role policy
--Create an IAM policy to allow, put,  and list actions on S3 bucket
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "s3export",
            "Action": [
                "S3:PutObject",
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::s3importtest/*"
            ]
        }
    ]
}
```

Ejemplo de función de base de datos load_external_tables_latest

```
CREATE OR REPLACE FUNCTION public.load_external_tables(pi_filename text)
```

```
 RETURNS character varying
 LANGUAGE plpgsql
AS $function$
/* Loading data from S3 bucket into a APG table */
DECLARE
 v_final_sql TEXT;
 pi_ext_table TEXT;
 r refCURSOR;
 v_sqlerrm text;
 v_chunk numeric;
 i integer;
 v_col_list TEXT;
 v_postion_list CHARACTER VARYING(1000);
 v_len  integer;
 v_delim varchar;
 v_file_name CHARACTER VARYING(1000);
 v_directory CHARACTER VARYING(1000);
 v_table_name_stg CHARACTER VARYING(1000);
 v_sql_col TEXT;
 v_sql TEXT;
 v_sql1 TEXT;
 v_sql2 TEXT;
 v_sql3 TEXT;
 v_cnt integer;
 v_sql_dynamic TEXT;
 v_sql_ins TEXT;
 proc_rec_COUNT integer;
 error_rec_COUNT integer;
 tot_rec_COUNT integer;
 v_rec_val integer;
 rec record;
 v_col_cnt integer;
 kv record;
 v_val text;
 v_header text;
 j integer;
 ERCODE VARCHAR(5);
 v_region text;
 cr CURSOR FOR
 SELECT distinct DELIMETER,
   FILE_NAME,
   DIRECTORY
 FROM  meta_EXTERNAL_TABLE
 WHERE table_name = pi_ext_table
```

```
   AND DELIMETER IS NOT NULL;


 cr1 CURSOR FOR
   SELECT   col_list,
   data_type,
   start_pos,
   END_pos,
   concat_ws('',' ',TABLE_NAME_STG) as TABLE_NAME_STG,
   no_position,date_mask
 FROM  meta_EXTERNAL_TABLE
 WHERE table_name = pi_ext_table
 order by col_order asc;
cr2 cursor FOR
SELECT  distinct table_name,table_name_stg
   FROM  meta_EXTERNAL_TABLE
   WHERE upper(file_name) = upper(pi_filename);


BEGIN
 -- PERFORM utl_file_utility.init();
   v_region := 'us-east-1';
   /* find tab details from file name */


   --DELETE FROM  ERROR_TABLE WHERE file_name= pi_filename;
  -- DELETE FROM  log_table WHERE file_name= pi_filename;


 BEGIN


   SELECT distinct table_name,table_name_stg INTO strict pi_ext_table,v_table_name_stg
   FROM  meta_EXTERNAL_TABLE
   WHERE upper(file_name) = upper(pi_filename);
 EXCEPTION
   WHEN NO_DATA_FOUND THEN
    raise notice 'error 1,%',sqlerrm;
    pi_ext_table := null;
    v_table_name_stg := null;
      RAISE USING errcode = 'NTFIP' ;
    when others then
        raise notice 'error others,%',sqlerrm;
 END;
```

```
 j :=1 ;

for rec in  cr2
 LOOP




  pi_ext_table     := rec.table_name;
  v_table_name_stg := rec.table_name_stg;
  v_col_list := null;


 IF pi_ext_table IS NOT NULL
  THEN
    --EXECUTE concat_ws('','truncate table  ' ,pi_ext_table) ;
   EXECUTE concat_ws('','truncate table  ' ,v_table_name_stg) ;




      SELECT distinct DELIMETER INTO STRICT v_delim
      FROM  meta_EXTERNAL_TABLE
      WHERE table_name = pi_ext_table;


      IF v_delim IS NOT NULL THEN
    SELECT distinct DELIMETER,
      FILE_NAME,
      DIRECTORY ,
      concat_ws('',' ',table_name_stg),
      case  header_exist when 'YES' then 'CSV HEADER' else 'CSV' end as header_exist
    INTO STRICT v_delim,v_file_name,v_directory,v_table_name_stg,v_header
    FROM  meta_EXTERNAL_TABLE
    WHERE table_name = pi_ext_table
      AND DELIMETER IS NOT NULL;


    IF    upper(v_delim) = 'CSV'
    THEN
      v_sql := concat_ws('','SELECT aws_s3.table_import_FROM_s3 ( ''',
      v_table_name_stg,''','''',
      ''DELIMITER '''','''' CSV HEADER QUOTE '''''''''', aws_commons.create_s3_uri
( ''',
```

```
      v_directory,''',''',v_file_name,''', ''',v_region,'''))');
      ELSE
      v_sql := concat_ws('','SELECT aws_s3.table_import_FROM_s3(''',
          v_table_name_stg, ''','''', ''DELIMITER AS ''''^''''','''','
         aws_commons.create_s3_uri
          ( ''',v_directory, ''','''',
          v_file_name, ''',',
           '''',v_region,''')
         )');
         raise notice 'v_sql , %',v_sql;
      begin
       EXECUTE  v_sql;
      EXCEPTION
        WHEN OTHERS THEN
          raise notice 'error 1';
        RAISE USING errcode = 'S3IMP' ;
      END;


      select count(col_list) INTO v_col_cnt
      from  meta_EXTERNAL_TABLE where table_name = pi_ext_table;







       -- raise notice 'v_sql 2, %',concat_ws('','update ',v_table_name_stg, ' set
col1 = col1||''',v_delim,''''');


      execute concat_ws('','update ',v_table_name_stg, ' set col1 =
col1||''',v_delim,''''');




      i :=1;
      FOR rec in cr1
      loop
      v_sql1 := concat_ws('',v_sql1,'split_part(col1,''',v_delim,''',', i,')',' as
',rec.col_list,',');
      v_sql2 := concat_ws('',v_sql2,rec.col_list,',');
  --    v_sql3 := concat_ws('',v_sql3,'rec.',rec.col_list,'::',rec.data_type,',');
```

```
      case
        WHEN upper(rec.data_type) = 'NUMERIC'
        THEN v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                coalesce((trim(split_part(col1,''',v_delim,''',',
i,')))::NUMERIC,0)::',rec.data_type,' END as ',rec.col_list,',') ;
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'YYYYMMDD'
        THEN v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                to_date(coalesce((trim(split_part(col1,''',v_delim,''',',
i,'))),''99990101''),''YYYYMMDD'')::',rec.data_type,' END as ',rec.col_list,',');
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'MM/DD/YYYY hh24:mi:ss'
        THEN v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                to_date(coalesce((trim(split_part(col1,''',v_delim,''',',
i,'))),''01/01/9999 0024:00:00''),''MM/DD/YYYY hh24:mi:ss'')::',rec.data_type,' END as
',rec.col_list,',');
         ELSE
       v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                 coalesce((trim(split_part(col1,''',v_delim,''',',
i,'))),'''')::',rec.data_type,' END as ',rec.col_list,',') ;
      END case;


      i :=i+1;
      end loop;


        -- raise notice 'v_sql 3, %',v_sql3;
```

```
       SELECT trim(trailing ' ' FROM v_sql1) INTO v_sql1;
       SELECT trim(trailing ',' FROM v_sql1) INTO v_sql1;


       SELECT trim(trailing ' ' FROM v_sql2) INTO v_sql2;
       SELECT trim(trailing ',' FROM v_sql2) INTO v_sql2;


       SELECT trim(trailing ' ' FROM v_sql3) INTO v_sql3;
       SELECT trim(trailing ',' FROM v_sql3) INTO v_sql3;


       END IF;
      raise notice 'v_delim , %',v_delim;


     EXECUTE concat_ws('','SELECT COUNT(*) FROM ',v_table_name_stg)  INTO v_cnt;


    raise notice 'stg cnt , %',v_cnt;


    /* if upper(v_delim) = 'CSV' then
       v_sql_ins := concat_ws('', ' SELECT * from ' ,v_table_name_stg );
     else
      -- v_sql_ins := concat_ws('',' SELECT ',v_sql1,'  from (select col1 from
 ' ,v_table_name_stg , ')sub ');
       v_sql_ins := concat_ws('',' SELECT ',v_sql3,'  from (select col1 from
 ' ,v_table_name_stg , ')sub ');
       END IF;*/


v_chunk := v_cnt/100;




for i in 1..101
loop
     BEGIN
    -- raise notice 'v_sql , %',v_sql;
       -- raise notice 'Chunk number , %',i;
       v_sql_ins := concat_ws('',' SELECT ',v_sql3,'  from (select col1 from
 ' ,v_table_name_stg , ' offset ',v_chunk*(i-1), ' limit ',v_chunk,') sub ');
```

```
    v_sql := concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins);
    -- raise notice 'select statement , %',v_sql_ins;
         -- v_sql := null;
    -- EXECUTE concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins, 'offset
',v_chunk*(i-1), ' limit ',v_chunk );
    --v_sql := concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins );


    -- raise notice 'insert statement , %',v_sql;


   raise NOTICE 'CHUNK START %',v_chunk*(i-1);
  raise NOTICE 'CHUNK END %',v_chunk;


    EXECUTE v_sql;


 EXCEPTION
      WHEN OTHERS THEN
      -- v_sql_ins := concat_ws('',' SELECT ',v_sql1, '  from (select col1 from
' ,v_table_name_stg , ' )sub ');
        -- raise notice 'Chunk number for cursor , %',i;


   raise NOTICE 'Cursor - CHUNK START %',v_chunk*(i-1);
  raise NOTICE 'Cursor -  CHUNK END %',v_chunk;
        v_sql_ins := concat_ws('',' SELECT ',v_sql3, '  from (select col1 from
' ,v_table_name_stg , ' )sub ');


        v_final_sql := REPLACE (v_sql_ins, ''''::text, ''''''::text);
       -- raise notice 'v_final_sql %',v_final_sql;
        v_sql :=concat_ws('','do $a$ declare  r refcursor;v_sql text; i
numeric;v_conname text;  v_typ  ',pi_ext_table,'[]; v_rec  ','record',';
          begin
```

```
          open r for execute ''select col1 from ',v_table_name_stg ,'  offset
 ',v_chunk*(i-1), ' limit ',v_chunk,''';
          loop
          begin
          fetch r into v_rec;
          EXIT WHEN NOT FOUND;




          v_sql := concat_ws('''','insert into  ',pi_ext_table,' SELECT ',REPLACE
 (v_sql3, ''''::text, ''''''::text) , '  from ( select ''''''',v_rec.col1,''''''' as
 col1) v'');
           execute v_sql;


          exception
           when others then
         v_sql := ''INSERT INTO  ERROR_TABLE VALUES (concat_ws(''''''''','''''Error
 Name: ''''',$$''||SQLERRM||''$$,''''Error State: ''''',''''''||
SQLSTATE||''''''',''''record : ''''',$$''||v_rec.col1||''$$),'''''||
pi_filename||''''',now())'';


             execute v_sql;
            continue;
          end ;
          end loop;
          close r;
          exception
          when others then
        raise;
          end ; $a$');
     -- raise notice ' inside excp v_sql %',v_sql;
         execute v_sql;
     --  raise notice 'v_sql %',v_sql;
      END;
  END LOOP;
     ELSE


     SELECT distinct DELIMETER,FILE_NAME,DIRECTORY ,concat_ws('',' ',table_name_stg),
       case  header_exist when 'YES' then 'CSV HEADER' else 'CSV' end as header_exist
       INTO STRICT v_delim,v_file_name,v_directory,v_table_name_stg,v_header
```

```
    FROM  meta_EXTERNAL_TABLE
    WHERE table_name = pi_ext_table                  ;
    v_sql := concat_ws('','SELECT aws_s3.table_import_FROM_s3(''',
      v_table_name_stg, ''','''', ''DELIMITER AS ''''#'''' ',v_header,' '','','
     aws_commons.create_s3_uri
      ( ''',v_directory, ''','''',
      v_file_name, ''',',
       '''',v_region,''')
     )');
        EXECUTE  v_sql;


    FOR rec in cr1
    LOOP


     IF rec.start_pos IS NULL AND rec.END_pos IS NULL AND rec.no_position = 'recnum'
     THEN
       v_rec_val := 1;
     ELSE


      case
        WHEN upper(rec.data_type) = 'NUMERIC'
        THEN v_sql1 := concat_ws('',' case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
               THEN null
                ELSE
                coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1)))::NUMERIC,0)::',rec.data_type,' END as
',rec.col_list,',') ;
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'YYYYMMDD'
        THEN v_sql1 := concat_ws('','case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
               THEN null
                ELSE
                to_date(coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1))),''99990101''),''YYYYMMDD''):',rec.data_type,'
END as ',rec.col_list,',');
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'YYYYMMDDHH24MISS'
        THEN v_sql1 := concat_ws('','case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
```

```
               THEN null
                ELSE
                to_date(coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1))),''9999010100240000''),''YYYYMMDDHH24MISS''):',rec.data_
END as ',rec.col_list,',');
         ELSE
       v_sql1 := concat_ws('',' case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
               THEN null
                ELSE
                 coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1))),''''):',rec.data_type,' END as
',rec.col_list,',') ;
      END case;


     END IF;
     v_col_list := concat_ws('',v_col_list ,v_sql1);
    END LOOP;




          SELECT trim(trailing ' ' FROM v_col_list) INTO v_col_list;
          SELECT trim(trailing ',' FROM v_col_list) INTO v_col_list;


          v_sql_col   :=  concat_ws('',trim(trailing ',' FROM v_col_list) , ' FROM
',v_table_name_stg,' WHERE col1 IS NOT NULL AND length(col1)>0 ');




          v_sql_dynamic := v_sql_col;


          EXECUTE  concat_ws('','SELECT COUNT(*) FROM ',v_table_name_stg) INTO v_cnt;




        IF v_rec_val = 1 THEN
            v_sql_ins := concat_ws('',' select row_number() over(order by ctid) as
line_number ,' ,v_sql_dynamic) ;
```

```
        ELSE
              v_sql_ins := concat_ws('',' SELECT' ,v_sql_dynamic) ;
          END IF;


    BEGIN
      EXECUTE concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins);
          EXCEPTION
             WHEN OTHERS THEN
         IF v_rec_val = 1 THEN
                v_final_sql := ' select row_number() over(order by ctid) as
line_number ,col1 from ';
               ELSE
                v_final_sql := ' SELECT col1 from';
              END IF;
      v_sql :=concat_ws('','do $a$ declare  r refcursor;v_rec_val numeric :=
',coalesce(v_rec_val,0),';line_number numeric; col1 text; v_typ  ',pi_ext_table,'[];
v_rec  ',pi_ext_table,';
            begin
            open r for execute ''',v_final_sql, ' ',v_table_name_stg,' WHERE col1 IS
NOT NULL AND length(col1)>0 '' ;
            loop
            begin
            if   v_rec_val = 1 then
            fetch r into line_number,col1;
            else
            fetch r into col1;
            end if;


            EXIT WHEN NOT FOUND;
             if v_rec_val = 1 then
             select line_number,',trim(trailing ',' FROM v_col_list) ,' into v_rec;
             else
               select ',trim(trailing ',' FROM v_col_list) ,' into v_rec;
             end if;


            insert into  ',pi_ext_table,' select v_rec.*;
             exception
             when others then
```

```
              INSERT INTO  ERROR_TABLE VALUES (concat_ws(''''',''Error Name:
'',SQLERRM,''Error State: '',SQLSTATE,''record : '',v_rec),''',pi_filename,''',now());
              continue;
             end ;
              end loop;
            close r;
             exception
             when others then
             raise;
             end ; $a$');
        execute v_sql;


    END;


        END IF;


  EXECUTE concat_ws('','SELECT COUNT(*) FROM  ' ,pi_ext_table)   INTO proc_rec_COUNT;


  EXECUTE concat_ws('','SELECT COUNT(*) FROM  error_table WHERE file_name
='''',pi_filename,''' and processed_time::date = clock_timestamp()::date')  INTO
error_rec_COUNT;


  EXECUTE concat_ws('','SELECT COUNT(*) FROM ',v_table_name_stg)   INTO tot_rec_COUNT;


  INSERT INTO  log_table values(pi_filename,now(),tot_rec_COUNT,proc_rec_COUNT,
error_rec_COUNT);


  raise notice 'v_directory, %',v_directory;


  raise notice 'pi_filename, %',pi_filename;


  raise notice 'v_region, %',v_region;
```

```
  perform aws_s3.query_export_to_s3('SELECT
 replace(trim(substring(error_details,position(''('' in
 error_details)+1),'')''),'','','';''),file_name,processed_time FROM  error_table WHERE
 file_name = '''||pi_filename||'''',
   aws_commons.create_s3_uri(v_directory, pi_filename||'.bad', v_region),
   options :='FORmat csv, header, delimiter $$,$$'
   );


raise notice 'v_directory, %',v_directory;


   raise notice 'pi_filename, %',pi_filename;


   raise notice 'v_region, %',v_region;


  perform aws_s3.query_export_to_s3('SELECT * FROM  log_table WHERE file_name = '''||
pi_filename||'''',
   aws_commons.create_s3_uri(v_directory, pi_filename||'.log', v_region),
   options :='FORmat csv, header, delimiter $$,$$'
   );




   END IF;
 j := j+1;
 END LOOP;


       RETURN 'OK';
EXCEPTION
    WHEN  OTHERS THEN
  raise notice 'error %',sqlerrm;
   ERCODE=SQLSTATE;
   IF ERCODE = 'NTFIP' THEN
     v_sqlerrm := concat_Ws('',sqlerrm,'No data for the filename');
   ELSIF ERCODE = 'S3IMP' THEN
    v_sqlerrm := concat_Ws('',sqlerrm,'Error While exporting the file from S3');
   ELSE
      v_sqlerrm := sqlerrm;
   END IF;
```

```
 select distinct directory into v_directory from  meta_EXTERNAL_TABLE;



 raise notice 'exc v_directory, %',v_directory;


   raise notice 'exc pi_filename, %',pi_filename;


   raise notice 'exc v_region, %',v_region;


  perform aws_s3.query_export_to_s3('SELECT * FROM  error_table WHERE file_name = '''||
pi_filename||'''',
   aws_commons.create_s3_uri(v_directory, pi_filename||'.bad', v_region),
   options :='FORmat csv, header, delimiter $$,$$'
   );
    RETURN null;
END;
$function$
```

Migración de índices basados en funciones de Oracle a PostgreSQL

Veeranjaneyulu Grandhi y Navakanth Talluri, Amazon Web Services

Resumen

Los índices son una forma común de mejorar el rendimiento de las bases de datos. Un índice permite al servidor de bases de datos encontrar y recuperar filas específicas mucho más rápido de lo que lo haría sin un índice. Sin embargo, los índices también añaden una sobrecarga al sistema de bases de datos en su conjunto, por lo que deben utilizarse con sensatez. Los índices basados en funciones, que se basan en una función o expresión, pueden incluir varias columnas y expresiones matemáticas. Un índice basado en funciones mejora el rendimiento de las consultas que utilizan la expresión de índice.

De forma nativa, PostgreSQL no admite la creación de índices basados en funciones mediante funciones cuya volatilidad se define como estable. Sin embargo, puede crear funciones similares con volatilidad `IMMUTABLE` y utilizarlas en la creación de índices.

Una función `IMMUTABLE` no puede modificar la base de datos y se garantiza que devolverá los mismos resultados con los mismos argumentos para siempre. Esta categoría permite al optimizador evaluar previamente la función cuando una consulta la llama con argumentos constantes.

Este patrón ayuda a migrar los índices basados en funciones de Oracle cuando se utilizan con funciones como `to_char`, `to_date` y `to_number` al equivalente de PostgreSQL.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa
- Una instancia de base de datos de Oracle de origen con el servicio de escucha configurado y en ejecución
- Familiaridad con bases de datos PostgreSQL

Limitaciones

- El límite de tamaño de la base de datos es de 64 TB
- Las funciones utilizadas en la creación de índices deben ser INMUTABLES.

Versiones de producto

- Todas las ediciones de bases de datos de Oracle para las versiones 11g (versiones 11.2.0.3.v1 y posteriores) y hasta 12.2, y 18c
- Versiones 9.6 y posteriores de PostgreSQL

Arquitectura

Pila de tecnología de origen

- Una base de datos Oracle local o en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o una instancia de base de datos Amazon RDS for Oracle

Pila de tecnología de destino

- Cualquier motor de PostgreSQL

Tools (Herramientas)

- pgAdmin 4 es una herramienta de administración de código abierto para Postgres. La herramienta pgAdmin 4 proporciona una interfaz gráfica para crear, mantener y utilizar objetos de base de datos.
- Oracle SQL Developer es un entorno de desarrollo integrado (IDE) para desarrollar y gestionar bases de datos de Oracle tanto en implementaciones tradicionales como en la nube.

Epics

Cree un índice basado en funciones mediante una función predeterminada

Tarea	Descripción	Habilidades requeridas
Cree un índice basado en funciones en una columna mediante la función to_char.	Utilice el siguiente código para crear el índice basado en funciones. `postgres=# create table funcindex( col1`	Administrador de base de datos, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

```
 timestamp without time
 zone);
CREATE TABLE
postgres=# insert
 into funcindex values
 (now());
INSERT 0 1
postgres=# select *
 from funcindex;
            col1
----------------------
------
 2022-08-09 16:00:57.
77414
(1 rows)

postgres=# create
 index funcindex_idx
 on funcindex(to_char(
col1,'DD-MM-YYYY
 HH24:MI:SS'));
ERROR:  functions in
 index expression must
 be marked IMMUTABLE
```

> **Note**
>
> PostgreSQL no permite crear un índice basado en funciones sin la cláusula `IMMUTABLE` .

Tarea	Descripción	Habilidades requeridas
Compruebe la volatilidad de la función.	Para comprobar la volatilidad de la función, utilice el código de la sección Información adicional.	Administrador de base de datos

Crear índices basados en funciones utilizando una función envolvente

Tarea	Descripción	Habilidades requeridas
Cree una función de encapsulación.	Para crear una función de encapsulación, utilice el código de la sección de información adicional.	Desarrollador de PostgreSQL
Cree un índice mediante la función de encapsulación.	Utilice el código de la sección Información adicional para crear una función definida por el usuario con la palabra clave `IMMUTABLE` en el mismo esquema que la aplicación y consúltela en el script de creación de índices. Si se crea una función definida por el usuario en un esquema común (del ejemplo anterior), actualice `search_path` tal como se muestra. `ALTER ROLE <ROLENAME> set search_path=$user, COMMON;`	Administrador de base de datos, desarrollador de PostgreSQL

Validar creación del índice

Tarea	Descripción	Habilidades requeridas
Valide la creación del índice.	Valide que es necesario crear el índice en función de los patrones de acceso a las consultas.	Administrador de base de datos
Valide que se pueda utilizar el índice.	Para comprobar si el optimizador de PostgreSQL recoge el índice basado en funciones, ejecute una instrucción SQL mediante explain o explain analyze. Utilice el código de la sección Información adicional. Si es posible, recopile también las estadísticas de la tabla. **Note** Si observa el plan de explicación, el optimizador de PostgreSQL ha elegido un índice basado en funciones debido a la condición de predicado.	Administrador de base de datos

Recursos relacionados

- Índices basados en funciones (documentación de Oracle)
- Índices de expresiones (documentación de PostgreSQL)
- Volatilidad de PostgreSQL (documentación de PostgreSQL)

- PostgreSQL search_path (documentación de PostgreSQL)
- Manual de migración de Oracle Database 19c a Amazon Aurora PostgreSQL

Información adicional

Crear una función de encapsulación

```
CREATE OR REPLACE FUNCTION myschema.to_char(var1 timestamp without time zone, var2
 varchar) RETURNS varchar AS $BODY$ select to_char(var1, 'YYYYMMDD'); $BODY$ LANGUAGE
 sql IMMUTABLE;
```

Crear un índice mediante la función de encapsulación

```
postgres=# create function common.to_char(var1 timestamp without time zone, var2
 varchar) RETURNS varchar AS $BODY$ select to_char(var1, 'YYYYMMDD'); $BODY$ LANGUAGE
 sql IMMUTABLE;
CREATE FUNCTION
postgres=# create index funcindex_idx on funcindex(common.to_char(col1,'DD-MM-YYYY
 HH24:MI:SS'));
CREATE INDEX
```

Comprobar la volatilidad de la función

```
SELECT DISTINCT p.proname as "Name",p.provolatile as "volatility" FROM
 pg_catalog.pg_proc p
 LEFT JOIN pg_catalog.pg_namespace n ON n.oid = p.pronamespace
 LEFT JOIN pg_catalog.pg_language l ON l.oid = p.prolang
 WHERE n.nspname OPERATOR(pg_catalog.~) '^(pg_catalog)$' COLLATE pg_catalog.default AND
 p.proname='to_char'GROUP BY p.proname,p.provolatile
ORDER BY 1;
```

Validar que se pueda utilizar el índice

```
explain analyze <SQL>


postgres=# explain select col1 from funcindex where common.to_char(col1,'DD-MM-YYYY
 HH24:MI:SS') = '09-08-2022 16:00:57';
                                                    QUERY PLAN
-----------------------------------------------------------------------------------------------
```

```
 Index Scan using funcindex_idx on funcindex  (cost=0.42..8.44 rows=1 width=8)
   Index Cond: ((common.to_char(col1, 'DD-MM-YYYY HH24:MI:SS'::character
 varying))::text = '09-08-2022 16:00:57'::text)
(2 rows)
```

Migración de las funciones nativas de Oracle a PostgreSQL mediante extensiones

Pinesh Singal, Amazon Web Services

Resumen

Este patrón de migración proporciona step-by-step orientación para migrar una base de datos de Amazon Relational Database Service (Amazon RDS) para Oracle a una base de datos de Amazon RDS for PostgreSQL o Amazon Aurora PostgreSQL Edition compatible con PostgreSQL mediante la modificación y las extensiones del código integrado nativo de PostgreSQL (). `aws_oracle_ext` `orafce` `psql` Esto ahorrará tiempo de procesamiento.

El patrón describe una estrategia de migración manual fuera de línea sin tiempo de inactividad para una base de datos de origen de Oracle de varios terabytes con un elevado número de transacciones.

El proceso de migración utiliza la herramienta de conversión de esquemas de AWS (AWS SCT) con las extensiones `aws_oracle_ext` y `orafce` para convertir un esquema de base de datos de Amazon RDS para Oracle en un esquema de base de datos compatible con Amazon RDS para PostgreSQL o Aurora PostgreSQL. Luego, el código se cambia manualmente al código integrado de `psql` nativo compatible con PostgreSQL. Esto se debe a que las llamadas a la extensión afectan al procesamiento del código en el servidor de bases de datos PostgreSQL y no todo el código de la extensión es totalmente compatible o compatible con el código PostgreSQL.

Este patrón se centra principalmente en la migración manual de códigos SQL mediante AWS SCT y las extensiones `aws_oracle_ext` y. `orafce` Las extensiones que ya se utilizan se convierten en elementos integrados (`psql`) nativos de PostgreSQL. A continuación, se eliminan todas las referencias a las extensiones y se convierten los códigos en consecuencia.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Sistema operativo (Windows o Mac) o EC2 instancia de Amazon (en funcionamiento)
- Orafce

Limitaciones

No todas las funciones de Oracle que utilizan extensiones `aws_oracle_ext` o `orafce` se pueden convertir en funciones nativas de PostgreSQL. Es posible que necesite una revisión manual para poder compilarlo con las bibliotecas de PostgreSQL.

Un inconveniente del uso de extensiones SCT de AWS es su lento rendimiento a la hora de ejecutar y obtener los resultados. Su costo se puede entender a partir del simple plan EXPLAIN de PostgreSQL (plan de ejecución de una declaración) sobre la migración de la función `SYSDATE` de Oracle a la función `NOW()` de PostgreSQL entre los tres códigos (`aws_oracle_ext`, `orafce` y `psql` predeterminados), como se explica en la sección Performance comparison check del documento adjunto.

Versiones de producto

- Origen: base de datos 10.2 y versiones posteriores de Amazon RDS para Oracle (para 10.x), 11g (11.2.0.3.v1 y versiones posteriores) y hasta 12.2, 18c y 19c (y versiones posteriores) para Enterprise Edition, Standard Edition, Standard Edition 1 y Standard Edition 2
- Destino: base de datos compatible con Amazon RDS para PostgreSQL o Aurora PostgreSQL 9.4 y versiones posteriores (para 9.x), 10.x, 11.x, 12.x, 13.x y 14.x (y versiones posteriores)
- AWS SCT: última versión (este patrón se probó con 1.0.632)
- Oracle: última versión (este patrón se probó con la versión 3.9.0)

Arquitectura

Pila de tecnología de origen

- Instancia de base de datos de Amazon RDS para Oracle con versión 12.1.0.2.v18

Pila de tecnología de destino

- Una instancia de base de datos compatible con Amazon RDS para PostgreSQL o Aurora PostgreSQL con la versión 11.5

Arquitectura de migración de bases de datos

El siguiente diagrama representa la arquitectura de migración de bases de datos entre las bases de datos de Oracle de origen y PostgreSQL de destino. La arquitectura incluye la nube de AWS, una nube privada virtual (VPC), zonas de disponibilidad, una subred privada, una base de datos Amazon RDS para Oracle, AWS SCT, una base de datos Amazon RDS para PostgreSQL o Aurora

compatible con PostgreSQL, extensiones para Oracle (`aws_oracle_ext` y `orafce`) y archivos de lenguaje de consulta estructurado (SQL).

1. Inicie la instancia de base de datos de Amazon RDS para Oracle (base de datos de origen).
2. Utilice AWS SCT con los `aws_oracle_ext` paquetes de `orafce` extensión para convertir el código fuente de Oracle a PostresQL.
3. La conversión produce archivos.sql migrados compatibles con PostgreSQL.
4. Convierta manualmente los códigos de extensión de Oracle no convertidos en códigos PostgreSQL (`psql`).
5. La conversión manual produce archivos.sql convertidos compatibles con PostgreSQL.
6. Ejecute estos archivos.sql en su instancia de base de datos de Amazon RDS para PostgreSQL (base de datos de destino).

Tools (Herramientas)

Herramientas

Servicios de AWS

- AWS SCT: la herramienta de conversión de esquemas de AWS (AWS SCT) convierte el esquema de base de datos existente de un motor de base de datos a otro. Puede convertir un esquema de procesamiento de transacciones en línea (OLTP) relacional o un esquema de almacenamiento de datos. Su esquema convertido es adecuado para una instancia de base de datos de Amazon RDS para MySQL, un clúster de base de datos de Amazon Aurora, una instancia de base de datos de Amazon RDS para PostgreSQL o un clúster de Amazon Redshift. El esquema convertido también se puede usar con una base de datos en una EC2 instancia de Amazon o se puede almacenar como datos en un bucket de Amazon S3.

  AWS SCT proporciona una interfaz de usuario basada en proyectos para convertir automáticamente el esquema de la base de datos de origen a un formato compatible con su instancia de Amazon RDS de destino.

  Puede usar AWS SCT para realizar la migración desde una base de datos de origen de Oracle a cualquiera de los destinos enumerados anteriormente. Con AWS SCT, puede exportar las definiciones de los objetos de la base de datos de origen, como el esquema, las vistas, los procedimientos almacenados y las funciones.

Puede utilizar AWS SCT para convertir datos de Oracle a Amazon RDS para PostgreSQL o Amazon Aurora PostgreSQL-Compatible Edition.

Este patrón utiliza AWS SCT para convertir y migrar el código de Oracle a PostgreSQL mediante las extensiones `aws_oracle_ext` y `orafce` migrar manualmente los códigos `psql` de extensión a código integrado nativo o predeterminado.

- El paquete de extensión de AWS SCT es un módulo complementario que simula funciones presentes en la base de datos de origen que son necesarias a la hora de convertir objetos a la base de datos de destino. Antes de poder instalar el paquete de extensión AWS SCT, debe convertir el esquema de su base de datos.

  Cuando convierte su base de datos o esquema de almacén de datos, AWS SCT agrega un esquema adicional a su base de datos de destino. Este esquema implementa las funciones del sistema SQL de la base de datos de origen que son necesarias al escribir su esquema convertido en la base de datos de destino. El esquema adicional se denomina esquema del paquete de extensión.

  El esquema del paquete de extensión para bases de datos OLTP se nombra según la base de datos de origen. Para las bases de datos de Oracle, el esquema del paquete de extensiones es `AWS_ORACLE_EXT`.

Otras herramientas

- Oracle: Orafce es un módulo que implementa funciones, tipos de datos y paquetes compatibles con Oracle. Es una herramienta de código abierto con una licencia de Berkeley Source Distribution (BSD) para que cualquiera pueda usarla. El módulo `orafce` es útil para migrar de Oracle a PostgreSQL porque tiene muchas funciones de Oracle implementadas en PostgreSQL.

Código

Para obtener una lista de todos los códigos más utilizados y migrados de Oracle a PostgreSQL para evitar el uso del código de extensión SCT de AWS, consulte el documento adjunto.

Epics

Configuración de la base de datos de origen de Amazon RDS para Oracle

Tarea	Descripción	Habilidades requeridas
Cree la instancia de base de datos de Oracle.	Cree una instancia de base de datos compatible con Amazon RDS para Oracle o Aurora PostgreSQL desde la consola de Amazon RDS.	AWS general, administrador de bases de datos
Configuración de los grupos de seguridad.	Configure grupos de seguridad entrantes y salientes.	AWS general
Cree la base de datos.	Crear la base de datos de Oracle con los usuarios y esquemas necesarios.	AWS general, administrador de bases de datos
Cree los objetos.	Crear objetos e introducir datos en el esquema.	Administrador de base de datos

Configuración de la base de datos de destino de Amazon RDS para PostgreSQL

Tarea	Descripción	Habilidades requeridas
Cree la instancia de base de datos PostgreSQL.	Cree una instancia de base de datos de Amazon RDS para PostgreSQL o de Amazon Aurora mediante la consola de Amazon RDS.	AWS general, administrador de bases de datos
Configuración de los grupos de seguridad.	Configure grupos de seguridad entrantes y salientes.	AWS general

Tarea	Descripción	Habilidades requeridas
Cree la base de datos.	Cree la base de datos PostgreSQL con los usuarios y esquemas necesarios.	AWS general, administrador de bases de datos
Valide las extensiones.	Asegúrese de que `aws_oracle_ext` y `orafce` están instalados y configura dos correctamente en la base de datos PostgreSQL.	Administrador de base de datos
Compruebe que la base de datos PostgreSQL esté disponible.	Asegúrese de que la base de datos PostgreSQL esté activa y en funcionamiento.	Administrador de base de datos

Migración del esquema de Oracle a PostgreSQL con AWS SCT y las extensiones

Tarea	Descripción	Habilidades requeridas
Instale AWS SCT.	Instale la versión más reciente de AWS SCT.	Administrador de base de datos
Configure AWS SCT.	Configure AWS SCT con los controladores de conectividad de bases de datos Java (JDBC) para Oracle (`ojdbc8.jar`) y PostgreSQL (`postgresql-42.2.5.jar`).	Administrador de base de datos
Habilite el paquete o la plantilla de extensiones SCT de AWS.	En AWS SCT Configuración de proyecto, habilite la implementación de funciones integradas con las extensiones `aws_oracle_ext` y	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`orafce` para el esquema de base de datos de Oracle.	
Convierta el esquema.	En AWS SCT, seleccione Convertir esquema para convertir el esquema de Oracle a PostgreSQL y generar los archivos.sql.	Administrador de base de datos

Convierta el código de extensión SCT de AWS en código psql

Tarea	Descripción	Habilidades requeridas
Convertir el código manualmente.	Convierta manualmente cada línea de código compatible con la extensión en código integrado predeterminado `psql`, como se detalla en el documento adjunto. Por ejemplo, cambie `AWS_ORACLE_EXT.SYSDATE()` a `ORACLE.SYSDATE()` o `NOW()`.	Administrador de base de datos
Valida el código	(Opcional) Valide cada línea de código ejecutándola temporalmente en la base de datos PostgreSQL.	Administrador de base de datos
Cree objetos en la base de datos PostgreSQL.	Para crear objetos en la base de datos de PostgreSQL, ejecute los archivos.sql generados por AWS SCT y modificados en los dos pasos anteriores.	Administrador de base de datos

Recursos relacionados

- Base de datos
  - Oracle en Amazon RDS
  - PostgreSQL en Amazon RDS
  - Uso de Amazon Aurora PostgreSQL
  - Plan EXPLAIN de PostgreSQL
- AWS SCT
  - Descripción general de la herramienta de conversión de esquemas de AWS
  - Guía del usuario de AWS SCT
  - Uso de la interfaz de usuario de AWS SCT
  - Utilizar la base de datos de Oracle como origen para AWS SCT
- Extensiones para AWS SCT
  - Uso del paquete de extensión de AWS SCT
  - Funcionalidad de Oracle (en)
  - PGXN oracle
  - GitHub orafce

Información adicional

Para obtener más información, siga los comandos detallados, con sintaxis y ejemplos, para convertir el código manualmente en el documento adjunto.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migre una base de datos Db2 de Amazon EC2 a Aurora compatible con MySQL mediante AWS DMS

Pinesh Singal, Amazon Web Services

Resumen

Tras migrar la base de datos de IBM Db2 for LUW a Amazon Elastic Compute Cloud EC2 (Amazon), considere la posibilidad de rediseñar la base de datos pasando a una base de datos nativa de la nube de Amazon Web Services (AWS). Este patrón cubre la migración de una base de datos IBM Db2 for LUW que se ejecuta en una EC2 instancia de Amazon a una base de datos Amazon Aurora MySQL Edition compatible con AWS.

El patrón describe una estrategia de migración en línea con un tiempo de inactividad mínimo para una base de datos fuente de Db2 de varios terabytes con un número elevado de transacciones.

Este patrón utiliza la Herramienta de conversión de esquemas de AWS (AWS SCT) para convertir el esquema de la base de datos de Db2 en un esquema de Aurora compatible con MySQL. A continuación, el patrón utiliza AWS Database Migration Service (AWS DMS) para migrar datos desde la base de datos Db2 a la base de datos de Aurora compatible con MySQL. Se requerirán conversiones manuales para el código que AWS SCT no convierta.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa con una nube privada virtual (VPC)
- AWS SCT
- AWS DMS

Versiones de producto

- Versión más reciente de AWS SCT
- Db2 para Linux, versión 11.1.4.4 y posteriores

Arquitectura

Pila de tecnología de origen

- DB2/Linux x86-64 bits montado en una instancia EC2

Pila de tecnología de destino

- Una instancia de base de datos de la edición de Amazon Aurora compatible con MySQL

Arquitectura de origen y destino

El siguiente diagrama muestra la arquitectura de migración de datos entre las bases de datos compatibles con MySQL de Aurora de origen y de destino. La arquitectura de la nube de AWS incluye una nube privada virtual (VPC), una zona de disponibilidad, una subred pública para la instancia de Db2 y la instancia de replicación de AWS DMS, y una subred privada para la base de datos Aurora compatible con MySQL.

Tools (Herramientas)

Servicios de AWS

- Amazon Aurora es un motor de base de datos relacional completamente administrado diseñado para la nube y compatible con MySQL y PostgreSQL.
- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- La Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado, lo que incluye las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino. AWS SCT admite como origen las versiones 9.1, 9.5, 9.7, 10.1, 10.1, 10.5, 11.1 y 11.5 de IBM Db2 para LUW.

Prácticas recomendadas

Para prácticas recomendadas, consulte Prácticas recomendadas para AWS Database Migration Service (AWS DMS).

Epics

Configurar la base de datos IBM Db2 de origen

Tarea	Descripción	Habilidades requeridas
Cree la base de datos IBM Db2 en Amazon EC2.	Puede crear una base de datos IBM Db2 en una EC2 instancia mediante una Amazon Machine Image (AMI) de AWS Marketplace o instalando el software Db2 en una EC2 instancia. Para lanzar una EC2 instancia , seleccione una AMI para IBM Db2 (por ejemplo, IBM Db2 v11.5.7 RHEL 7.9), que es similar a una base de datos local.	Administrador de base de datos, AWS general
Configuración de grupos de seguridad.	Configure las reglas de entrada del grupo de seguridad de VPC para SSH (Secure Shell) y TCP con los puertos 22 y 50000, respectiv amente.	AWS general
Crear la instancia de base de datos.	Cree una instancia (usuario) y una base de datos (esquema) nuevas, o utilice la instancia y la base de datos `db2inst1` de muestra predeterminadas. 1. Conéctese a la EC2 instancia mediante el terminal para conectarse a la base de datos de Db2.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Como alternativa, puede instalar cualquier software cliente de base de datos que se conecte a la base de datos de Db2. 2. Para establecer la contraseña del usuario db2inst1, ejecute el comando `sudo passwd db2inst1`. 3. Para conectarse a la instancia db2inst1, ejecute el comando `sudo su - db2inst1`. 4. Para conectarse a la base de datos de Db2, ejecute el comando `db2`. 5. Para conectarse a la base de datos de muestra, utilice el comando `connect to sample`. Como alternativa, conéctese a la base de datos que creó. 6. Tras conectarse a la instancia de base de datos, cree objetos e inserte datos en estos objetos mediante declaraciones de SQL de Db2.	

Tarea	Descripción	Habilidades requeridas
Confirme que la instancia de la base de datos Db2 está disponible.	Para confirmar que la instancia de la base de datos de Db2 está activa y en ejecución, utilice el comando `Db2pd -`.	Administrador de base de datos

Configurar la base de datos de destino de Aurora compatible con MySQL

Tarea	Descripción	Habilidades requeridas
Cree la base de datos de Aurora compatible con MySQL.	Crear una base de datos de Amazon Aurora con compatibilidad con MySQL desde el servicio de AWS RDS • Crear una base de datos en Amazon Aurora con compatibilidad con MySQL y la versión que prefiera, por ejemplo Aurora (MySQL)-5.6.10a • Instalar la aplicación MySQL Workbench o su software cliente de base de datos preferido, que le permite conectarse a la base de datos MySQL	Administrador de base de datos, AWS general
Configuración de grupos de seguridad.	Configure las reglas de entrada del grupo de seguridad de la VPC para las conexiones SSH y TCP.	AWS general
Confirme que la base de datos de Aurora esté disponible.	Para asegurarse de que la base de datos de Aurora	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	compatible con MySQL esté en funcionamiento, haga lo siguiente: 1. Conéctate a la EC2 instancia a través de SSH. 2. Configure y conéctese a la instancia de Aurora compatible con MySQL desde MySQL Workbench. Utilice el punto de conexión como nombre de host, tal y como se muestra en el siguiente ejemplo. `mysql-cluster-instance-1.cokmvis0v46q.us-east-1.rds.amazonaws.com` 3. Cree el nuevo esquema y conéctese al nuevo esquema (por ejemplo, `mysql-sample-db2`). 4. Ejecute las declaraciones de MySQL para comprobar los esquemas y objetos de la base de datos.	

Configuración y ejecución de AWS SCT

Tarea	Descripción	Habilidades requeridas
Instale AWS SCT.	Descargue e instale la versión más reciente de AWS SCT (la	AWS general

Tarea	Descripción	Habilidades requeridas
	versión actual más reciente es 1.0.628).	
Configure AWS SCT.	1. Descargue los controladores de conectividad de bases de datos Java (JDBC) para IBM Db2 (versión 4.22.X) y MySQL (8.x). 2. Para configurar los controladores en AWS SCT, seleccione Settings (Configuración), Global settings (Configuración global) y Drivers (Controladores).	AWS general
Cree un proyecto de AWS SCT.	Cree un proyecto y un informe de AWS SCT que utilice Db2 para LUW como motor de base de datos de origen y Aurora compatible con MySQL para el motor de base de datos de destino. Para identificar los privilegios necesarios para conectarse a una base de datos de Db2 para LUW, consulte Uso de Db2 LUW como fuente de AWS SCT.	AWS general

Tarea	Descripción	Habilidades requeridas
Valide los objetos.	Seleccione Cargar esquema, validar los objetos. Actualice cualquier objeto incorrecto en la base de datos de destino: 1. Conéctese al servidor de Amazon Aurora compatibl e con MySQL proporcio nando los detalles de la conexión y seleccione Probar conexión. Tanto las conexiones de origen como las de destino deben realizarse correctamente antes de que AWS SCT pueda iniciar el informe de migración. 2. Una vez completado el informe, introduzca el esquema que desee convertir y seleccione Finalizar. AWS SCT muestra todos los objetos de origen y destino que se han convertido y tienen errores. 3. Revise los errores y elimínelos manualmente. 4. Una vez que se hayan borrado todos los errores, abra el menú contextua l (haga clic con el botón derecho) del esquema	Administrador de base de datos, AWS general

Tarea	Descripción	Habilidades requeridas
	y seleccione Cargar esquema. 5. Seleccione Aplicar a la base de datos. 6. En MySQL Workbench , conéctese a la base de datos de Aurora compatible con MySQL y compruebe el esquema y los objetos.	

Configurar y ejecutar AWS SCT

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación.	Inicie sesión en la consola de administración de AWS, navegue hasta el servicio AWS DMS y cree una instancia de replicación con una configuración válida para el grupo de seguridad de VPC que configuró para las bases de datos de origen y destino.	AWS general
Cree puntos de conexión.	Cree el punto de conexión de origen para la base de datos Db2 y cree el punto de conexión de destino para la base de datos Aurora compatible con MySQL: 1. Cree un punto de conexión para IBM Db2 como origen seleccionando Seleccion	AWS general

Tarea	Descripción	Habilidades requeridas
	ar la instancia de base de datos RDS y, a continuación, seleccionando la instancia de Db2 que ha creado. Los detalles de configuración del punto de conexión se rellenarán automáticamente. 2. En la configuración específica del punto de conexión, añada los siguientes atributos de conexión adicionales. `CurrentLSN=<scan>; MaxKBytesPerRead=64; SetDataCaptureChanges=true` Si no menciona estos atributos, la conexión de prueba del punto de conexión de origen no se realizará correctamente. Para obtener más información, consulte Uso de IBM Db2 LUW como fuente de AWS DMS. 3. Para crear un punto de conexión de Aurora compatible con MySQL como destino, seleccione Seleccionar instancia de base de datos RDS y, a continuación, seleccion	

Tarea	Descripción	Habilidades requeridas
	e la instancia de Aurora compatible con MySQL que creó. Los detalles de configuración del punto de conexión se rellenará n automáticamente. Para obtener más información, consulte Usar una base de datos compatible con MySQL como destino para AWS Database Migration Service (AWS DMS). 4. Pruebe los puntos de conexión de origen y destino. Confirme que ambos son correctos y están disponibles. 5. Si la prueba falla, asegúrese de que las reglas de entrada del grupo de seguridad sean válidas.	

Tarea	Descripción	Habilidades requeridas
Cree tareas de migración.	Cree una o varias tareas de migración para completar la carga y validar los CDC o los datos: 1. Para crear una tarea de migración de base de datos, seleccione la instancia de replicación, el punto de conexión de la base de datos de origen y el punto de conexión de la base de datos de destino. Especifique el tipo de migración como Migración de los datos existentes (carga completa), Replicar solo los cambios de datos (CDC) o Migración de los datos existentes y réplica de los cambios en curso (carga completa y CDC). 2. En las Asignaciones de tablas, puede configurar las reglas de selección y las reglas de transformación en formatos GUI o JSON. 3. En Reglas de selección , seleccione el esquema, introduzca el nombre de la tabla y seleccione la Acción (Incluir/Excluir) que desee configurar (por ejemplo, Esquema:	AWS general

Tarea	Descripción	Habilidades requeridas
	MUESTRA; Nombre de tabla: %, Acción: Incluir). 4. En Reglas de transformación, seleccione el objetivo (esquema, tabla o columna). Seleccione el nombre del esquema y seleccione la acción (mayúscula, prefijo, sufijo); por ejemplo, Objetivo: Esquema; `mysql-sample-db` ; Acción: Convertir a minúsculas. 5. Activa la supervisión de Amazon CloudWatch Logs.	
Planifique el ciclo de producción.	Confirme el tiempo de inactividad con las partes interesadas, como los propietarios de las aplicaciones, para ejecutar AWS DMS en los sistemas de producción.	Líder de migración
Ejecute las tareas de migración.	1. Inicie la tarea de AWS DMS que tenga el estado Listo. 2. Supervisa los registros de tareas de migración en Amazon CloudWatch Logs para detectar cualquier error.	AWS general

Tarea	Descripción	Habilidades requeridas
Valide los datos.	Revise los resultados y los datos de las tareas de migración en las bases de datos Db2 de origen y MySQL de destino: 1. Si el estado es Cargar la replicación en curso completa, significa que la carga completa con la migración de datos de los CDC se ha completado y la validación está en curso. 2. Conéctese a la base de datos de Aurora compatibl e con MySQL y compruebe los datos. 3. Compruebe los cambios en curso insertando o actualiza ndo los datos en la base de datos Db2.	Administrador de base de datos
Detenga las tareas de migración.	Una vez que la validación de datos se haya completad o correctamente, detenga las tareas de migración de la validación.	AWS general

Resolución de problemas

Problema	Solución
Las conexiones de prueba de origen y destino de AWS SCT no funcionan.	Configure las versiones del controlador JDBC y las reglas de entrada del grupo de seguridad de VPC para que acepten el tráfico entrante.
Se produce un error en la ejecución de la prueba del punto de conexión de origen de Db2.	Configure la configuración `CurrentLSN=<scan>;` de conexión adicional.

La AWSDMS tarea no se puede conectar a la fuente de Db2 y aparece el siguiente error.
`database is recoverable if either or both of the database configuration parameters LOGARCHMETH1 and LOGARCHMETH2 are set to ON`
	Para evitar el error, ejecute los siguientes comandos:
	1. `$ db2 update db cfg for sample using LOGARCHMETH1 DISK:/home/db2inst1/logs`
	2. `$ db2stop`
	3. `$ db2start`
	4. `$ db2 connect to sample`
	`SQL1116N A connection to or activation of database "SAMPLE" cannot be made because of BACKUP PENDING. SQLSTATE=57019`
	5. `$ db2 backup database sample to ../logs`
	`SQL2036N The path for the file or device "../logs" is not valid`
	6. `$ cd`
	7. `$ pwd`
	`/home/db2inst1`
	8. `$ mkdir /tmp/backup`

Problema	Solución

	9. `$ db2 backup database sample to /tmp/backup`
	`Backup successful. The timestamp for this backup image is : 20190530084921`
	10. `$ db2 connect to sample`
	`Database Connection Information`
	`Database server = DB2/LINUX 9.7.1`
	`SQL authorization ID = DB2INST1`
	`Local database alias = SAMPLE`

Recursos relacionados

Amazon EC2

- Amazon EC2
- Guías EC2 de usuario de Amazon

Bases de datos

- Base de datos IBM Db2
- Amazon Aurora
- Uso de Amazon Aurora MySQL

AWS SCT

- Conversión de esquemas AWS DMS
- Guía del usuario de la herramienta de conversión de esquemas de AWS
- Uso de la interfaz de usuario de AWS SCT
- Uso de IBM Db2 LUW como origen para AWS SCT

AWS DMS

- AWS Database Migration Service (AWS DMS)
- Guía del usuario de AWS Database Migration Service (AWS DMS)
- Orígenes para la migración de datos
- Destinos para la migración de datos
- AWS Database Migration Service (AWS DMS) y la herramienta de conversión de esquemas de AWS ahora admiten IBM Db2 LUW como fuente (entrada del blog)
- Migración de aplicaciones que ejecutan bases de datos relacionales a AWS

Migre una base de datos de Microsoft SQL Server de Amazon EC2 a Amazon DocumentDB mediante AWS DMS

Umamaheswara Nooka, Amazon Web Services

Resumen

Este patrón describe cómo usar AWS Database Migration Service (AWS DMS) para migrar una base de datos de Microsoft SQL Server alojada en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) a una base de datos de Amazon DocumentDB (compatible con MongoDB).

La tarea de replicación de AWS DMS lee la estructura de tablas de la base de datos de SQL Server, crea la colección correspondiente en Amazon DocumentDB y lleva a cabo una migración de carga completa.

También se puede usar este patrón para migrar una instancia de base de datos de SQL Server en las instalaciones o Amazon Relational Database Service (Amazon RDS) para SQL Server a Amazon DocumentDB. Para obtener más información, consulte la guía Migrating Microsoft SQL Server databases to the AWS Cloud (Migrar bases de datos de Microsoft SQL Server a la nube de AWS) en el sitio web de Recomendaciones de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una base de datos de SQL Server existente en una instancia. EC2
- Función de base de datos fija (db_owner) asignada a AWS DMS en la base de datos de SQL Server. Para obtener más información, consulte Database-level roles (Roles en el nivel de base de datos) de la documentación de SQL Server.
- Familiaridad con el uso de los programas de utilidades `mongodump`, `mongorestore`,`mongoexport` y `mongoimport` para mover datos dentro y fuera de un clúster de Amazon DocumentDB.
- Microsoft SQL Server Management Studio, instalado y configurado.

Limitaciones

- El límite de tamaño del clúster en Amazon DocumentDB es de 64 TB. Para obtener más información, consulte Cluster limits (Límites de los clústeres) en la documentación de Amazon DocumentDB.
- AWS DMS no permite combinar varias tablas de origen en una sola colección de Amazon DocumentDB.
- Si AWS DMS procesa los cambios de una tabla de origen sin una clave principal, omitirá las columnas de objetos grandes (LOB) de la tabla de origen.

Arquitectura

Pila de tecnología de origen

- Amazon EC2

Pila de tecnología de destino

- Amazon DocumentDB

Arquitectura de destino

Tools (Herramientas)

- WS DMS: AWS Database Migration Service (AWS DMS) ayuda a migrar los datos de forma rápida y segura.
- Amazon DocumentDB: Amazon DocumentDB (con compatibilidad con MongoDB) es un servicio de bases de datos rápido, fiable y totalmente gestionado.
- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS.
- Microsoft SQL Server: SQL Server es un sistema de administración de bases de datos relacionales.
- SQL Server Management Studio (SSMS): SSMS es una herramienta para administrar SQL Server, que incluye el acceso, la configuración y la administración de los componentes de SQL Server.

Epics

Crear y configurar una VPC

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	Inicie sesión en la consola de administración de AWS y abra la consola de Amazon VPC. Cree una nube privada virtual (VPC) con un rango de bloques IPv4 CIDR.	Administrador de sistemas
Cree redes y grupos de seguridad. ACLs	En la consola de Amazon VPC, cree grupos de seguridad y listas de control de acceso a la red (red ACLs) para su VPC, según sus necesidades. También puede utilizar la configuración predeterminada para estas configuraciones. Para obtener más información sobre esta y otras historias, consulte la sección “Recursos relaciona dos”.	Administrador de sistemas

Crear y configurar el clúster de Amazon DocumentDB

Tarea	Descripción	Habilidades requeridas
Cree un clúster de Amazon DocumentDB.	Abra la consola de Amazon DocumentDB y elija “Clústere s”. Elija “Crear” y cree un clúster de Amazon DocumentDB con una instancia. Importante:	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	Asegúrese de configurar este clúster con los grupos de seguridad de su VPC.	
Instale el intérprete de comandos de mongo.	El intérprete de comandos de mongo es un programa de utilidad de línea de comandos que se utiliza para conectars e al clúster de Amazon DocumentDB y consultarlo. Para instalarla, ejecute el comando «/etc/yum.repos.d/ mongodb-org-3.6.repo» para crear el archivo de repositor io. Ejecute el comando «sudo yum install -y mongodb-org-shell" para instalar el shell mongo. Para cifrar los datos en tránsito, descargue la clave pública de Amazon DocumentDB y, a continuac ión, conéctese a su instancia de Amazon DocumentDB. Para obtener más información sobre estos pasos, consulte la sección “Recursos relaciona dos”.	Administrador de sistemas
Cree una base de datos en el clúster de Amazon DocumentDB.	Ejecute el comando «use» con el nombre de la base de datos para crear una base de datos en el clúster de Amazon DocumentDB.	Administrador de sistemas

Cree y configure una instancia de replicación de AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación de AWS DMS.	Abra la consola de AWS DMS y elija “Crear una instancia de replicación”. Especifique un nombre y una descripción para la tarea de replicación. Seleccione la clase de instancia, la versión del motor, el almacenamiento, la VPC y las zonas de disponibilidad múltiples (Multi-AZ) y póngalas a disposición del público. Elija la pestaña “Avanzado” para establecer la configuración de red y de cifrado. Especifique la configuración de mantenimiento y, a continuación, elija “Crear una instancia de replicación”.	Administrador de sistemas
Configure la base de datos de SQL Server.	Inicie sesión en Microsoft SQL Server y agregue una regla de entrada para la comunicación entre el punto de conexión de origen y la instancia de replicación de AWS DMS. Utilice la dirección IP privada de la instancia de replicación como origen. Importante: La instancia de replicación y el punto de conexión de destino deben estar en la misma VPC. Utilice una fuente alternati	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	va en el grupo de seguridad si VPCs son diferentes para las instancias de origen y de replicación.	

Cree y pruebe los puntos de conexión de origen y destino en AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree puntos de conexión de base de datos de origen y destino.	Abra la consola de AWS DMS y elija “Conectar puntos de conexión de la base de datos de origen y de destino”. Especifique la información de conexión para las bases de datos de origen y destino. Si es necesario, elija la pestaña “Avanzado” para establece r los valores de “Atributos de conexión adicionales”. Descargue y utilice el grupo de certificados de la configura ción del punto de conexión.	Administrador de sistemas
Pruebe la conexión del punto de conexión.	Elija “Ejecutar prueba” para probar la conexión. Para solucionar cualquier mensaje de error, compruebe la configuración del grupo de seguridad y las conexiones a la instancia de replicación de AWS DMS desde las instancia s de base de datos de origen y destino.	Administrador de sistemas

Migración de datos

Tarea	Descripción	Habilidades requeridas
Cree la tarea de migración de AWS DMS.	En la consola de AWS DMS, elija “Tareas” y “Crear una tarea”. Especifique las opciones de la tarea, incluidos los nombres de los puntos de conexión de origen y destino y los nombres de las instancia s de replicación. En “Tipo de migración”, elija “Migrar los datos existentes” y “Replicar solo los cambios en los datos”. Elija “Iniciar tarea”.	Administrador de sistemas
Ejecute la tarea de migración de AWS DMS.	En “Configuración de la tarea”, especifique los ajustes del modo de preparación de tablas, como “No hacer nada”, “Borrar tablas en el destino”, “Truncar” e “Incluir las columnas LOB en la replicación”. Establezca un tamaño de LOB máximo que AWS DMS acepte y elija “Habilitar registro”. Deje “Configuración avanzada” en sus valores predeterminados y elija “Crear una tarea”.	Administrador de sistemas
Supervise la migración.	En la consola de AWS DMS, elija “Tareas” y, a continuac ión, su tarea de migración. Elija “Supervisión de tareas” para supervisar su tarea. La	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	tarea se detiene cuando la migración de carga completa finaliza y se aplican los cambios guardados en la memoria caché.	

Probar y verificar la aplicación

Tarea	Descripción	Habilidades requeridas
Conéctese al clúster de Amazon DocumentDB mediante el intérprete de comandos de mongo.	Abra la consola de Amazon DocumentDB y seleccione su clúster en “Clústeres”. En la pestaña “Conectividad y seguridad”, elija “Conectar a este clúster con el shell mongo”.	Administrador de sistemas
Verifique los resultados de la migración.	Ejecute el comando “use” con el nombre de su base de datos y, a continuac ión, ejecute el comando “show collections”. Ejecute el comando “db. .count ();” con el nombre de su base de datos. Si los resultado s coinciden con la base de datos de origen, la migración se ha realizado correctam ente.	Administrador de sistemas

Recursos relacionados

Create and configure a VPC (Crear y configurar una VPC)

- Create a security group for your VPC (Crear un grupo de seguridad para la VPC)
- Create a network ACL (Crear una ACL de red)

Create and configure the Amazon DocumentDB cluster (Crear y configurar el clúster de Amazon DocumentDB)

- Create an Amazon DocumentDB cluster (Crear un clúster de Amazon DocumentDB)
- Install the mongo shell for Amazon DocumentDB (Instalar el intérprete de comandos de mongo para Amazon DocumentDB)
- Connect to your Amazon DocumentDB cluster (Conectarse al clúster de Amazon DocumentDB)

Create and configure the AWS DMS replication instance (Crear y configurar una instancia de replicación de AWS DMS)

- Use public and private replication instances (Usar instancias de replicación pública y privada)

Create and test the source and target endpoints in AWS DMS (Crear y probar los puntos de conexión de origen y destino en AWS DMS)

- Use Amazon DocumentDB as a target for AWS DMS (Utilizar Amazon DocumentDB como destino para AWS DMS)
- Use a SQL Server database as a source for AWS DMS (Utilizar una base de datos de SQL Server como origen para AWS DMS)
- Use AWS DMS endpoints (Utilizar puntos de conexión de AWS DMS)

Migración de datos

- Migrate to Amazon DocumentDB (Migrar a Amazon DocumentDB)

Otros recursos

- Limitations on using SQL Server as a source for AWS DMS (Restricciones en el uso de SQL Server como origen para AWS DMS)
- How to use Amazon DocumentDB to build and manage applications at scale (Cómo utilizar Amazon DocumentDB para crear y gestionar aplicaciones a gran escala)

Migre una base de datos ThoughtSpot Falcon local a Amazon Redshift

Battulga Purevragchaa y Antony Prasad Thevaraj, Amazon Web Services

Resumen

El almacenamiento de datos en las instalaciones requiere una cantidad considerable de tiempo y recursos de administración, especialmente en el caso de conjuntos de datos de gran tamaño. El costo financiero de compilar, mantener y hacer crecer estos almacenes también es muy alto. Para ayudar a administrar los costos, mantener baja la complejidad de extracción, transformación y carga (ETL) y ofrecer rendimiento a medida que sus datos crecen, debe elegir constantemente qué datos cargar y qué datos archivar.

Al migrar sus bases de datos ThoughtSpot Falcon locales a la nube de Amazon Web Services (AWS), puede acceder a lagos de datos y almacenes de datos basados en la nube que aumentan la agilidad, la seguridad y la confiabilidad de las aplicaciones de su empresa, además de reducir los costos generales de infraestructura. Amazon Redshift ayuda a reducir considerablemente los costos y los gastos operativos de un almacenamiento de datos. También puede usar Amazon Redshift Spectrum para analizar grandes cantidades de datos en su formato nativo sin necesidad de cargar los datos.

Este patrón describe los pasos y el proceso para migrar una base de datos ThoughtSpot Falcon de un centro de datos local a una base de datos de Amazon Redshift en la nube de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos ThoughtSpot Falcon alojada en un centro de datos local

Versiones de producto

- ThoughtSpot versión 7.0.1

Arquitectura

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Los datos se alojan en una base de datos relacional en las instalaciones.
2. La herramienta de conversión de esquemas de AWS (AWS SCT) convierte el lenguaje de definición de datos (DDL) que es compatible con Amazon Redshift.
3. Una vez creadas las tablas, puede migrar los datos mediante AWS Database Migration Service (AWS DMS).
4. Los datos se cargan en Amazon Redshift.
5. Los datos se almacenan en Amazon Simple Storage Service (Amazon S3) si utiliza Redshift Spectrum o si ya aloja los datos en Amazon S3.

Tools (Herramientas)

- AWS DMS: AWS Data Migration Service (AWS DMS) le ayuda a migrar bases de datos a AWS de forma rápida y segura.
- Amazon Redshift: Amazon RedShift es un servicio de almacenamiento de datos de escala de petabyte rápido, totalmente administrado, que hace que sea simple y rentable analizar de manera eficiente todos sus datos utilizando sus herramientas de inteligencia empresariales existentes.
- AWS SCT: la herramienta de conversión de esquemas de AWS (AWS SCT) convierte el esquema de base de datos existente de un motor de base de datos a otro.

Epics

Preparación para la migración

Tarea	Descripción	Habilidades requeridas
Identifique la configuración de Amazon Redshift adecuada.	Identifique la configuración de clúster de Amazon Redshift adecuada en función de sus requisitos y volumen de datos. Para obtener más información, consulte Clústeres de Amazon Redshift en la documentación de Amazon Redshift.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Investigue Amazon Redshift para evaluar si cumple con sus requisitos.	Utilice Amazon Redshift FAQs para comprender y evaluar si Amazon Redshift cumple sus requisitos.	Administrador de base de datos

Preparación del clúster de Amazon Redshift de destino

Tarea	Descripción	Habilidades requeridas
Crear un clúster de Amazon Redshift.	Inicie sesión en la consola de administración de AWS, abra la consola de Amazon Redshift y, a continuación, cree un clúster de Amazon Redshift en una nube privada virtual (VPC). Para obtener más informaci ón, consulte Creación de un clúster en una VPC en la documentación de Amazon Redshift.	Administrador de base de datos
Lleve a cabo una PoC para el diseño de su base de datos de Amazon Redshift.	Siga las prácticas recomenda das de Amazon Redshift realizando una prueba de concepto (PoC) para el diseño de su base de datos. Para obtener más informaci ón, consulte Realización de una prueba de concepto para Amazon Redshift en la documentación de Amazon Redshift.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree usuarios de bases de datos.	Cree los usuarios en la base de datos de Amazon Redshift y asigne los roles adecuados para acceder al esquema y a las tablas. Para obtener más informaci ón, consulte Conceder privilegi os de acceso a un usuario o grupo de usuarios en la documentación de Amazon Redshift.	Administrador de base de datos
Aplique los parámetros de configuración a la base de datos de destino.	Aplique los parámetros de configuración a la base de datos de Amazon Redshift según sus requisitos. Para obtener más informaci ón sobre cómo habilitar los parámetros de base de datos, sesión y servidor, consulte la Referencia de configura ción en la documentación de Amazon Redshift.	Administrador de base de datos

Crear objetos en el clúster de Amazon Redshift

Tarea	Descripción	Habilidades requeridas
Cree tablas manualmente con DDL en Amazon Redshift.	(Opcional) Si utiliza AWS SCT, las tablas se crean automáticamente. Sin embargo, si se producen errores al replicar DDLs,	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	tendrá que crear las tablas manualmente	
Crear tablas externas para Redshift Spectrum.	Cree una tabla externa con un esquema externo para Amazon Redshift Spectrum. Para crear tablas externas, debe ser el propietario del esquema externo o un superusuario de base de datos. Para obtener más informaci ón, consulte Creación de tablas externas para Amazon Redshift Spectrum en la documentación de Amazon Redshift.	Administrador de base de datos

Migración de datos utilizando AWS DMS

Tarea	Descripción	Habilidades requeridas
Utilice AWS DMS para migrar los datos.	Tras crear el DDL de las tablas en la base de datos de Amazon Redshift, migre sus datos a Amazon Redshift mediante AWS DMS. Para obtener instrucciones y pasos detallados, consulte Uso de una base de datos de Amazon Redshift como destino de AWS DMS en la documentación de AWS DMS.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Uso del comando COPY para cargar datos.	Utilice el comando `COPY` de Amazon Redshift para cargar los datos desde Amazon S3 a Amazon Redshift. Para obtener más informaci ón, consulte Uso del comando COPIAR para cargar desde Amazon S3 en la documenta ción de Amazon Redshift.	Administrador de base de datos

Validar el clúster de Amazon Redshift

Tarea	Descripción	Habilidades requeridas
Valide los registros de origen y destino.	Valide el recuento de tablas de los registros de origen y destino que se cargaron desde el sistema de origen.	Administrador de base de datos
Implemente las prácticas recomendadas de Amazon Redshift para el ajuste del rendimiento.	Implemente las prácticas recomendadas de Amazon Redshift para el diseño de tablas y bases de datos. Para obtener más informaci ón, consulte la siguiente entrada del blog: Las 10 técnicas principales de ajuste del rendimiento de Amazon Redshift.	Administrador de base de datos
Optimizar el rendimiento de la consulta.	Amazon RedShift utiliza consultas basadas en SQL para interactuar con datos y	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	objetos en el sistema. El Data Manipulation Language (DML, Lenguaje de manipulación de datos) es el subconjunto de SQL que el usuario utiliza para ver, añadir, cambiar y eliminar datos. DDL es el subconjun to de SQL que el usuario utiliza para añadir, cambiar y eliminar objetos de la base de datos como tablas y vistas. Para obtener más información, consulte Ajuste del rendimien to de las consultas en la documentación de Amazon Redshift.	
Implemente WLM.	Puede utilizar workload management (WLM) para definir varias colas de consultas y dirigir las consultas a las colas adecuadas en tiempo de ejecución. Para obtener más información, consulte Implementación de la administración de la carga de trabajo en la documentación de Amazon Redshift.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Trabajar con escalado de concurrencia.	Al usar la característica de escalado de concurrencia, puede admitir usuarios concurrentes prácticamente ilimitados y consultas concurrentes, con un rendimiento de consulta consistentemente rápido. Para obtener más información, consulte Uso del escalado de simultaneidad en la documentación de Amazon Redshift.	Administrador de base de datos
Use las prácticas recomendadas de Amazon RedShift para el diseño de tablas.	Cuando planifica su base de datos, ciertas decisiones importantes de diseño de tabla pueden influir considerablemente en el rendimiento general de la consulta. Para obtener más información sobre seleccionar la opción de diseño de tablas más adecuada, consulte Prácticas recomendadas de Amazon Redshift para el diseño de tablas en la documentación de Amazon Redshift.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Crear vistas materializadas en Amazon Redshift.	Una vista materializada contiene un conjunto de resultados computados previamente, basados en una consulta de SQL sobre una o más tablas base. Puede emitir instrucciones SELECT para consultar una vista materiali zada, de la misma manera que puede consultar otras tablas o vistas en la base de datos. Para obtener más información, consulte Creación de vistas materializadas en Amazon Redshift en la documentación de Amazon Redshift.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Defina las uniones entre las tablas.	Para buscar en más de una tabla al mismo tiempo ThoughtSpot, debe definir las uniones entre las tablas especificando columnas que contengan datos coincidentes en dos tablas. Estas columnas representan la `primary key` y `foreign key` de la unión. Puede definirlos mediante el `ALTER TABLE` comando de Amazon Redshift o. ThoughtSpot Para obtener más información, consulte ALTER TABLE en la documentación de Amazon RedShift.	Administrador de base de datos

Configurar la ThoughtSpot conexión a Amazon Redshift

Tarea	Descripción	Habilidades requeridas
Añada una conexión de Amazon Redshift.	Añada una conexión Amazon Redshift a su base de datos Falcon local. ThoughtSpot Para obtener más informaci ón, consulte Añadir una conexión Amazon Redshift en la ThoughtSpot documenta ción.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Edite la conexión de Amazon Redshift.	Puede editar la conexión de Amazon Redshift para añadir tablas y columnas. Para obtener más información, consulte Edición de una conexión de Amazon Redshift en la ThoughtSpot documentación.	Administrador de base de datos
Reasigne la conexión de Amazon Redshift.	Modifique los parámetros de conexión editando el archivo .yaml de asignación de origen que se creó al añadir la conexión de Amazon Redshift. Por ejemplo, puede reasignar la tabla o columna existente a una tabla o columna diferente en una conexión de base de datos existente. ThoughtSpot recomienda comprobar las dependencias antes y después de volver a mapear una tabla o columna de una conexión para asegurarse de que se muestran según sea necesario. Para obtener más información, consulte Remapear una conexión de Amazon Redshift en ThoughtSpot la documentación.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Elimine una tabla de la conexión de Amazon Redshift.	(Opcional) Si intenta eliminar una tabla de una conexión de Amazon Redshift, ThoughtSpot comprueba las dependencias y muestra una lista de objetos dependientes. Puede elegir los objetos de la lista para eliminarlos o eliminar la dependencia. A continuación puede eliminar la tabla. Para obtener más información, consulte Eliminar una tabla de una conexión de Amazon Redshift en la ThoughtSpot documentación.	Administrador de base de datos
Elimine una tabla con objetos dependientes de una conexión de Amazon Redshift.	(Opcional) Si intenta eliminar una tabla con objetos dependientes, la operación se bloquea. Se muestra una ventana `Cannot delete` con una lista de enlaces a objetos dependientes. Cuando se eliminen todas las dependencias, podrá eliminar la tabla Para obtener más información, consulte Eliminar una tabla con objetos dependientes de una conexión de Amazon Redshift en la ThoughtSpot documentación.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Elimine una conexión de Amazon Redshift.	(Opcional) Como una conexión se puede utilizar en varios orígenes de datos o visualizaciones, debe eliminar todas las fuentes y tareas que utilizan esa conexión antes de poder eliminar la conexión de Amazon Redshift. Para obtener más informaci ón, consulte Eliminar una conexión de Amazon Redshift en la ThoughtSpot documenta ción.	Administrador de base de datos
Compruebe la referencia de conexión de Amazon Redshift.	Asegúrese de proporcionar la información requerida para su conexión a Amazon Redshift utilizando la referencia de conexión de la documenta ción. ThoughtSpot	Administrador de base de datos

Información adicional

- Análisis basados en IA a cualquier escala con Amazon ThoughtSpot Redshift
- Precios de Amazon Redshift
- Introducción a AWS SCT
- Introducción a Amazon Redshift
- Uso de agentes de extracción de datos
- Chick-fil-A mejora la velocidad de obtención de información con ThoughtSpot AWS

Migre de Oracle Database a Amazon RDS for PostgreSQL mediante Oracle GoldenGate

Dhairya Jindani, Sindhusha Paturu y Rajeshkumar Sabankar, Amazon Web Services

Resumen

Este patrón muestra cómo migrar una base de datos Oracle a Amazon Relational Database Service (Amazon RDS) para PostgreSQL mediante Oracle Cloud Infrastructure (OCI). GoldenGate

Con Oracle GoldenGate, puede replicar datos entre la base de datos de origen y una o más bases de datos de destino con un tiempo de inactividad mínimo.

> **Note**
>
> La base de datos Oracle de origen puede estar en las instalaciones o en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Puede utilizar un procedimiento similar cuando utilice herramientas de replicación en las instalaciones.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una licencia de Oracle GoldenGate
- Controlador de Java Database Connectivity (JDBC) para conectarse a la base de datos PostgreSQL
- Esquema y tablas creados con la herramienta de conversión de esquemas de AWS (AWS SCT) en la base de datos Amazon RDS para PostgreSQL de destino

Limitaciones

- Oracle solo GoldenGate puede replicar los datos de las tablas existentes (carga inicial) y los cambios en curso (captura de datos de cambios)

Versiones de producto

- Oracle Database 10g Enterprise Edition o versiones más recientes
- Oracle GoldenGate 12.2.0.1.1 para Oracle o versiones más recientes
- Oracle GoldenGate 12.2.0.1.1 para PostgreSQL o versiones más recientes

Arquitectura

El siguiente diagrama muestra un ejemplo de flujo de trabajo para migrar una base de datos de Oracle a Amazon RDS for PostgreSQL mediante Oracle: GoldenGate

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El proceso de GoldenGate extracción de Oracle se ejecuta en la base de datos de origen para extraer los datos.
2. El proceso de Oracle GoldenGate Replicat entrega los datos extraídos a la base de datos Amazon RDS for PostgreSQL de destino.

Tools (Herramientas)

- Oracle le GoldenGate ayuda a diseñar, ejecutar, organizar y monitorear sus soluciones de procesamiento de datos y de replicación de datos en streaming en Oracle Cloud Infrastructure.
- Amazon Relational Database Service (Amazon RDS) para PostgreSQL le ayuda a configurar, utilizar y escalar una base de datos relacional de PostgreSQL en la nube de AWS.

Epics

Descargue e instale Oracle GoldenGate

Tarea	Descripción	Habilidades requeridas
Descargue Oracle GoldenGate.	Descargue las siguientes versiones de Oracle GoldenGate: • Oracle GoldenGate 12.2.0.1.1 para Oracle o una versión más reciente	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	• Oracle GoldenGate 12.2.0.1.1 para PostgreSQL o una versión más reciente Para descargar el software, consulte GoldenGate Descargas de Oracle en el sitio web de Oracle.	
Instale Oracle GoldenGate for Oracle en el servidor de Oracle Database de origen.	Para obtener instrucciones, consulte la GoldenGate documentación de Oracle.	Administrador de base de datos
Instale la base de datos Oracle GoldenGate for PostgreSQL en la instancia de Amazon. EC2	Para obtener instrucciones, consulte la documentación de Oracle GoldenGate .	Administrador de base de datos

Configure Oracle GoldenGate en las bases de datos de origen y destino

Tarea	Descripción	Habilidades requeridas
Configure Oracle GoldenGate for Oracle Database en la base de datos de origen.	Para obtener instrucciones, consulte la GoldenGate documentación de Oracle. Asegúrese de configurar lo siguiente: • Registro suplementario • GoldenGate Usuarios de Oracle • Cualquier concesión y permiso necesarios • Archivos de parámetros	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	• Proceso de gestión • Directorio • Archivos GLOBALS • Monedero de Oracle	
Configure Oracle GoldenGat e para PostgreSQL en la base de datos de destino.	Para obtener instrucciones, consulte la Parte VI Uso de Oracle GoldenGate para PostgreSQL en el sitio web de Oracle. Asegúrese de configurar lo siguiente: • Proceso de gestión • Archivos GLOBALS • Monedero de Oracle	Administrador de base de datos

Configuración de la captura de datos

Tarea	Descripción	Habilidades requeridas
Configure el proceso de extracción en la base de datos de origen.	En la base de datos de Oracle de origen, cree un archivo de extracción para extraer los datos. Para obtener instrucciones, consulte ADD EXTRACT en la documentación de Oracle. **Note** El archivo de extracció n incluye la creación	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	del archivo de parámetros de extracción y el directorio de archivos de seguimiento.	
Configure una bomba de datos para transferir el archivo de seguimiento de la base de datos de origen a la de destino.	Cree un archivo de parámetros EXTRACT y un directorio de archivos de seguimiento siguiendo las instrucciones que aparecen en PARFILE en Utilidades de bases de datos, en el sitio web de Oracle. Para obtener más información, consulte ¿Qué es una ruta? en Fusion Middleware Understanding Oracle GoldenGate en el sitio web de Oracle.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Configure la replicación en la EC2 instancia de Amazon.	Cree un archivo de parámetros de replicación y un directorio de archivos de seguimiento. Para obtener más información sobre la creación de archivos de parámetros de replicación, consulte la sección 3.5 Validación de un archivo de parámetros en la documentación de la base de datos de Oracle. Para obtener más información, consulte Creación de un registro de seguimiento en la documentación de CloudTrail. ⚠ Important Asegúrese de agregar una entrada en la tabla de puntos de control en el archivo GLOBALS del destino. Para obtener más información, consulte ¿Qué es un replicante? en Fusion Middleware Understanding Oracle GoldenGate en el sitio web de Oracle.	Administrador de base de datos

Configure la replicación de datos

Tarea	Descripción	Habilidades requeridas
En la base de datos de origen, cree un archivo de parámetros para extraer los datos de la carga inicial.	Siga las instrucciones de la sección Creación de un archivo de parámetros en GGSCI en la documentación de Oracle Cloud. **Important** Asegúrese de que el administrador se ejecute en el destino.	Administrador de base de datos
En la base de datos de destino, cree un archivo de parámetros para replicar los datos de la carga inicial.	Siga las instrucciones de la sección Creación de un archivo de parámetros en GGSCI en la documentación de Oracle Cloud. **Important** Asegúrese de agregar e iniciar el proceso de replicación.	Administrador de base de datos

Cambie a la base de datos de Amazon RDS para PostgreSQL

Tarea	Descripción	Habilidades requeridas
Detenga el proceso de replicación y asegúrese de que las bases de datos	Compare los recuentos de filas entre las bases de datos de origen y destino para asegurarse de que la replicaci	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
de origen y destino estén sincronizadas.	ón de los datos se realizó correctamente.	
Compatibilidad con el lenguaje de definición de datos (DDL) de configuración.	Ejecute el script DDL para crear activadores, secuencias, sinónimos y claves referenciales en PostgreSQL. **Note** Puede usar cualquier aplicación cliente de SQL estándar para conectarse al clúster de base de datos. Por ejemplo, puede usar pgAdmin para conectarse a su instancia de base de datos.	Administrador de base de datos

Recursos relacionados

- Amazon RDS para PostgreSQL en la Guía del usuario de Amazon RDS
- EC2 Documentación de Amazon
- Métodos de procesamiento y bases de datos GoldenGate compatibles con Oracle (documentación de Oracle)

Migración de una tabla particionada de Oracle a PostgreSQL mediante AWS DMS

Saurav Mishra y Eduardo Valentim, Amazon Web Services

Resumen

Este patrón describe cómo acelerar la carga de una tabla particionada de Oracle a PostgreSQL mediante AWS Database Migration Service (AWS DMS), que no admite el particionamiento nativo. La base de datos PostgreSQL de destino se puede instalar en Amazon Elastic Compute Cloud (EC2Amazon) o puede ser una instancia de base de datos Edition compatible con PostgreSQL o Amazon Aurora PostgreSQL compatible con PostgreSQL.

La carga de una tabla particionada incluye los pasos siguientes:

1. Cree una tabla principal similar a la tabla de particiones de Oracle, pero no incluya ninguna partición.
2. Cree tablas secundarias que hereden de la tabla principal que se creó en el paso 1.
3. Cree una función de procedimiento y un disparador para gestionar las inserciones en la tabla principal.

Sin embargo, dado que el disparador se activa para cada inserción, la carga inicial con AWS DMS puede ser muy lenta.

Para acelerar las cargas iniciales de Oracle a PostgreSQL 9.0, este patrón crea una tarea de AWS DMS independiente para cada partición y carga las tablas secundarias correspondientes. A continuación, se crea un disparador durante la transición.

La versión 10 de PostgreSQL admite particiones nativas. Sin embargo, en algunos casos puede decidir utilizar la partición heredada. Para obtener más información, consulte la sección Additional information (Información adicional).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de Oracle de origen con una tabla particionada
- Una base de datos PostgreSQL en AWS

Versiones de producto

- PostgreSQL 9.0

Arquitectura

Pila de tecnología de origen

- Una tabla particionada en Oracle

Pila de tecnología de destino

- Una tabla particionada en PostgreSQL (en EC2 Amazon, Amazon RDS for PostgreSQL o Aurora PostgreSQL)

Arquitectura de destino

Tools (Herramientas)

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.

Epics

Configure AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree las tablas en PostgreSQL.	Cree las tablas principales y secundarias correspondientes en PostgreSQL con las condiciones de comprobación necesarias para las particiones.	Administrador de base de datos
Cree la tarea AWS DMS para cada partición.	Incluya el estado del filtro de la partición en la tarea	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de AWS DMS. Asigne las particiones a las tablas secundarias de PostgreSQL correspondientes.	
Ejecute las tareas de AWS DMS con captura de datos de cambio y carga completa (CDC).	Además, compruebe que el parámetro `StopTaskCachedChangesApplied` está establecido en `true` y que el parámetro `StopTaskCachedChangesNotApplied` está establecido en `false`.	Administrador de base de datos

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Detiene la tarea de replicación.	Antes de detener las tareas, confirme que el origen y el destino están sincronizados.	Administrador de base de datos
Cree un disparador en la tabla principal.	Como la tabla principal recibirá todos los comandos de inserción y actualización, cree un activador que dirija estos comandos a las tablas secundarias respectivas en función de la condición de partición.	Administrador de base de datos

Recursos relacionados

- AWS DMS

- Particionamiento de tablas (documentación de PostgreSQL)

Información adicional

Aunque la versión 10 de PostgreSQL admite la partición nativa, puede decidir usar la partición heredada para los siguientes casos de uso:

- La partición impone una regla según la cual todas las particiones deben tener el mismo conjunto de columnas que la principal, pero la herencia de tablas permite que las particiones secundarias tengan columnas adicionales.
- La herencia de tablas admite herencias múltiples.
- La partición declarativa solo admite la partición de listas y rangos. Con la herencia de tablas, puede dividir los datos como desee. Sin embargo, si la exclusión de la restricción no puede reducir las particiones de forma eficaz, el rendimiento de las consultas se verá afectado.
- Algunas operaciones necesitan un bloqueo más fuerte cuando se usa la partición declarativa que cuando se usa la herencia de tablas. Por ejemplo, añadir o quitar una partición de una tabla particionada requiere un bloqueo `ACCESS EXCLUSIVE` en la tabla principal, mientras que un bloqueo `SHARE UPDATE EXCLUSIVE` es suficiente para una herencia normal.

Si utiliza particiones de trabajo independientes, también puede volver a cargar las particiones si hay algún problema de validación de AWS DMS. Para mejorar el rendimiento y el control de la replicación, ejecute las tareas en instancias de replicación independientes.

Migración de de Amazon RDS para Oracle a Amazon RDS para MySQL

Jitender Kumar, Srini Ramaswamy y Neha Sharma, Amazon Web Services

Resumen

Este patrón proporciona una guía para migrar una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para Oracle a una base de datos de Amazon RDS para MySQL en la nube de Amazon Web Services (AWS). Este patrón utiliza AWS Database Migration Service (AWS DMS) y la Herramienta de conversión de esquemas de AWS (AWS SCT).

El patrón proporciona las prácticas recomendadas para gestionar la migración de los procedimientos almacenados. También trata y cambia el código para admitir la capa de aplicación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una base de datos de origen de Amazon RDS para Oracle.
- Una base de datos de destino de Amazon RDS para MySQL. Las bases de datos de origen y de destino deben estar en la misma nube privada virtual (VPC). Si utilizas varios VPCs o debes tener los permisos de acceso necesarios.
- Grupos de seguridad que permiten la conectividad entre las bases de datos de origen y destino, AWS SCT, el servidor de la aplicación y AWS DMS.
- Una cuenta de usuario con los privilegios necesarios para ejecutar AWS SCT en la base de datos de origen.
- Registro suplementario activado para ejecutar AWS DMS en la base de datos de origen.

Limitaciones

- El límite de tamaño de la base de datos de Amazon RDS de origen y destino es de 64 TB. Para obtener información sobre el tamaño de Amazon RDS, consulte la documentación de AWS.
- Oracle distingue mayúsculas de minúsculas para los objetos de base de datos, pero MySQL no. AWS SCT puede gestionar este problema al crear un objeto. Sin embargo, es necesario llevar a cabo algunos trabajos manuales para no distinguir entre mayúsculas y minúsculas.

- Esta migración no utiliza extensiones de MySQL para habilitar las funciones nativas de Oracle. AWS SCT gestiona la mayor parte de la conversión, pero es necesario trabajar un poco para cambiar el código manualmente.
- Se requieren cambios en el controlador de Java Database Connectivity (JDBC) en la aplicación.

Versiones de producto

- Amazon RDS para Oracle 12.2.0.1 y versiones posteriores. Para ver las versiones de RDS para Oracle compatibles actualmente, consulte la documentación de AWS.
- Amazon RDS para MySQL 8.0.15 y versiones posteriores Para ver las versiones de RDS para MySQL compatibles actualmente, consulte la documentación de AWS.
- AWS DMS, versión 3.3.0 y posteriores. Consulte la documentación de AWS para obtener más información sobre los puntos de conexión de origen y de destino compatibles con AWS DMS.
- AWS SCT, versión 1.0.628 y posteriores. Consulte AWS SCT source and target endpoint support matrix en la documentación de AWS.

Arquitectura

Pila de tecnología de origen

- Amazon RDS para Oracle. Para obtener más información, consulte Using an Oracle database as a source for AWS DMS.

Pila de tecnología de destino

- Amazon RDS para MySQL. Para obtener más información, consulte Using a MySQL-Compatible database as a target for AWS DMS.

Arquitectura de migración

En el siguiente diagrama, AWS SCT copia y convierte los objetos de esquema de la base de datos de origen de Amazon RDS para Oracle y envía los objetos a la base de datos de destino de Amazon RDS para MySQL. AWS DMS replica los datos de la base de datos de origen y los envía a la instancia de Amazon RDS para MySQL.

Tools (Herramientas)

- AWS Database Migration Service lo ayuda a migrar almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS. Este patrón utiliza Amazon RDS para Oracle and Amazon RDS para MySQL.
- La Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado, lo que incluye las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino.

Epics

Preparación para la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.		Administrador de base de datos
Identifique los requisitos de hardware de la instancia del servidor de destino.		DBA, SysAdmin
Identifique los requisitos de almacenamiento (como el tipo y la capacidad de almacenam iento).		DBA, SysAdmin
Elija el tipo de instancia apropiado (capacidad, características de almacenam iento y características de red).		DBA, SysAdmin
Identifique los requisitos de seguridad de acceso a la		DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
red de las bases de datos de origen y destino.		
Elija una estrategia de migración de aplicaciones.	Considere si desea un tiempo de inactividad total o parcial para las actividades en transición.	DBA, propietario de la SysAdmin aplicación

Configurar la infraestructura

Tarea	Descripción	Habilidades requeridas
Creación de una VPC y de subredes.		SysAdmin
Cree grupos de seguridad y listas de control de acceso a la red (ACLs).		SysAdmin
Configure e inicie la instancia de Amazon RDS para Oracle.		DBA, SysAdmin
Configure e inicie la instancia de Amazon RDS para MySQL.		DBA, SysAdmin
Prepare un caso de prueba para la validación de la conversión de código.	Esto ayudará a realizar pruebas unitarias para el código convertido.	Administrador de base de datos, desarrollador
Configure la instancia de AWS DMS.		
Configure los puntos de conexión de origen y destino en AWS DMS.		

Migración de datos

Tarea	Descripción	Habilidades requeridas
Generar el script de la base de datos de destino mediante AWS SCT.	Compruebe la precisión del código convertido por AWS SCT. Será necesario realizar algunos trabajos manuales.	Administrador de base de datos, desarrollador
En AWS SCT, elija la configuración “Sin distinción entre mayúsculas y minúsculas”.	En AWS SCT, elija Configuración del proyecto, Distinción entre mayúsculas y minúsculas del destino, Sin distinción entre mayúsculas y minúsculas.	Administrador de base de datos, desarrollador
En AWS SCT, opte por no utilizar la función nativa de Oracle.	En la configuración del proyecto, compruebe las funciones TO_ _DATECHAR/ TO_NUMBER/TO.	Administrador de base de datos, desarrollador
Realice cambios en el código “sql%notfound”.	Puede que tenga que convertir el código manualmente.	
Realice consultas sobre tablas y objetos en procedimientos almacenados (utilice consultas en minúsculas).		Administrador de base de datos, desarrollador
Cree el script principal después de realizar todos los cambios y, a continuación, impleméntelo en la base de datos de destino.		Administrador de base de datos, desarrollador
Realice pruebas unitarias de procedimientos almacenad		

Tarea	Descripción	Habilidades requeridas
os y llamadas a aplicaciones utilizando datos de muestra.		
Limpie los datos que se crearon durante las pruebas unitarias.		Administrador de base de datos, desarrollador
Elimine las restricciones de clave externa en la base de datos de destino.	Este paso es obligatorio para cargar los datos iniciales. Si no desea eliminar las restricciones de clave externa, debe crear una tarea de migración para los datos específicos de las tablas principal y secundaria.	Administrador de base de datos, desarrollador
Coloque las claves principales y las claves únicas en la base de datos de destino.	Este paso da como resultado un mejor rendimiento para la carga inicial.	Administrador de base de datos, desarrollador
Habilitar el registro suplementario en la base de datos de origen.		Administrador de base de datos
Cree una tarea de migración para la carga inicial en AWS DMS y ejecútela.	Seleccione la opción de migrar datos existentes.	Administrador de base de datos
Añada las claves principales y las claves externas a la base de datos de destino.	Las restricciones deben añadirse después de la carga inicial.	Administrador de base de datos, desarrollador
Cree una tarea de migración para la replicación continua.	La replicación continua mantiene la base de datos de destino sincronizada con la base de datos de origen.	Administrador de base de datos

Migración de aplicaciones

Tarea	Descripción	Habilidades requeridas
Sustituya las funciones nativas de Oracle por funciones nativas de MySQL.		Propietario de la aplicación
Asegúrese de que solo se usen nombres en minúscula para los objetos de base de datos en las consultas SQL.		DBA, SysAdmin propietario de la aplicación

Realizar la transición a la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Apague el servidor de la aplicación.		Propietario de la aplicación
Valide que las bases de datos de origen y destino estén sincronizadas.		Administrador de base de datos, propietario de la aplicación
Detenga la instancia de base de datos de Amazon RDS para Oracle.		Administrador de base de datos
Detenga la tarea de migración.	Se detendrá automáticamente después de completar el paso anterior.	Administrador de base de datos
Cambie la conexión JDBC de Oracle a MySQL.		Administrador de base de datos, propietario de la aplicación
Inicie la aplicación.		DBA, propietario de la SysAdmin aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Revise y valide los documentos del proyecto.		DBA, SysAdmin
Recopile métricas sobre el tiempo de migración, el porcentaje de tareas manuales en comparación con las tareas automatizadas, el ahorro de costos, etc.		DBA, SysAdmin
Detenga y elimine las instancias de AWS DMS.		Administrador de base de datos
Elimine los puntos de conexión de la base de datos de origen y de destino.		Administrador de base de datos
Elimine las tareas de migración.		Administrador de base de datos
Realice una instantánea de la instancia de base de datos de Amazon RDS para Oracle.		Administrador de base de datos
Elimine la instancia de base de datos de Amazon RDS para Oracle.		Administrador de base de datos
Cierre y elimine cualquier otro recurso temporal de AWS que haya utilizado.		DBA, SysAdmin
Cierre el proyecto y envíe sus comentarios.		Administrador de base de datos

Recursos relacionados

- AWS DMS
- AWS SCT
- Precios de Amazon RDS
- Introducción a AWS DMS
- Introducción a Amazon RDS

Migre de IBM Db2 en Amazon EC2 a Aurora compatible con PostgreSQL mediante AWS DMS y AWS SCT

Sirsendu Halder y Abhimanyu Chhabra, Amazon Web Services

Resumen

Este patrón proporciona orientación para migrar una base de datos IBM Db2 en una instancia de Amazon Elastic Compute Cloud EC2 (Amazon) a una instancia de base de datos Edition compatible con Amazon Aurora PostgreSQL. Este patrón utiliza AWS Database Migration Service (AWS DMS) y Herramienta de conversión de esquemas de AWS (AWS SCT) para la migración de datos y la conversión de esquemas.

El patrón describe una estrategia de migración en línea con poco o ningún tiempo de inactividad para una base de datos IBM Db2 de varios terabytes que tiene un número elevado de transacciones. Le recomendamos que convierta las columnas de claves principales (PKs) y claves externas (FKs) con el tipo de datos `NUMERIC` a PostgreSQL `INT` o `BIGINT` en PostgreSQL para obtener un mejor rendimiento.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos IBM Db2 de origen en una instancia EC2

Versiones de producto

- DB2/LINUXX8664 versión 11.1.4.4 y versiones posteriores

Arquitectura

Pila de tecnología de origen

- Una base de datos Db2 en una instancia EC2

Pila de tecnología de destino

- Una instancia de base de datos compatible con Aurora PostgreSQ versión 10.18 o instancia de base de datos posterior

Arquitectura de migración de base de datos

Tools (Herramientas)

- AWS Database Migration Service (AWS DMS) ayuda a migrar los bases de datos a la nube de AWS o entre combinaciones de configuraciones en las instalaciones y en la nube. La base de datos de origen permanece totalmente operativa durante la migración, minimizando así el tiempo de inactividad de las aplicaciones que dependen de ella. Puede utilizar AWS DMS puede migrar sus datos desde y hasta las bases de datos comerciales y de código abierto más usadas. AWS DMS admite migraciones heterogéneas entre diferentes plataformas de bases de datos, como IBM Db2 a una versión 10.18 o posterior compatible con Aurora PostgreSQL. Para obtener más información, consulte Fuentes de migración de datos y Objetivos de migración de datos en la documentación de AWS DMS.
- Herramienta de conversión de esquemas de AWS (AWS SCT) ademite las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte de los objetos de código de base de datos, incluidas las vistas, los procedimientos almacenados y las funciones, a un formato que sea compatible con la base de datos de destino. Los objetos que no se conviertan automáticamente se marcan claramente para que puedan convertirse manualmente con el objetivo de completar la migración. AWS SCT también puede analizar el código fuente de su aplicación en busca de instrucciones de SQL incrustadas y convertirlas.

Epics

Configuración del entorno

Tarea	Descripción	Habilidades requeridas
Crear una instancia de base de datos compatible con Aurora PostgreSQL.	Para crear una instancia de base de datos, siga las instrucciones de la documentación de AWS. Para engine type (Tipo de motor), elija Amazon Aurora. En edition (edición), seleccione Edición	Amazon RDS

Tarea	Descripción	Habilidades requeridas
	compatible con Amazon Aurora PostgreSQL. La instancia de base de datos de la versión 10.18 o posterior compatible con Aurora PostgreSQL debe estar en la misma nube privada virtual (VPC) que la base de datos de origen de IBM Db2.	

Convertir su esquema de base de dato

Tarea	Descripción	Habilidades requeridas
Instalar y verificar AWS SCT.	1. Instale AWS SCT siguiendo los pasos de la documentación de AWS SCT. 2. Verifique la instalación siguiendo los procedimientos de la documentación de AWS SCT.	Administrador de AWS, administrador de base de datos, ingeniero de migraciones
Inicie AWS SCT y cree un proyecto.	Para iniciar la herramienta AWS SCT y crear un nuevo proyecto para ejecutar un informe de evaluación de la migración de bases de datos, siga las instrucciones de la documentación de AWS SCT.	Ingeniero de migraciones
Añada servidores de bases de datos y cree una regla de asignación.	1. Añada servidores de bases de datos de origen y destino siguiendo las instrucciones de la	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	documentación de AWS SCT. 2. Cree una regla de asignación para definir la plataforma de base de datos de destino para su base de datos de origen. Para obtener instrucciones, consulte la documentación de AWS SCT.	
Crear un informe de evaluación de la migración de la base de datos.	Cree el informe de evaluación de la migración de la base de datos siguiendo los pasos de la documentación de AWS SCT.	Ingeniero de migraciones
Consultar del informe de evaluación.	Utilice la pestaña Resumen del informe de evaluación de la migración de la base de datos para ver el informe y analizar los datos. Este análisis le ayudará a determinar la complejidad de la migración. Para obtener más información, consulte la documentación de AWS SCT.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Convierta el esquema.	Para convertir su esquemas de base de datos de origen: 1. En la consola AWS SCT, elija Ver y, a continuación, Vista principal. 2. Seleccione el objeto o el nodo principal del esquema de origen, abra el menú contextual (haga clic con el botón derecho) y, a continuación, elija Convertir esquema. Para obtener más información, consulte la documentación de AWS SCT.	Ingeniero de migraciones
Aplicar el esquema de base de datos convertido a su instancia de base de datos de destino.	1. Seleccione el elemento del esquema del panel derecho del proyecto que indique el esquema previsto para su instancia de base de datos de destino. 2. Abra el menú contextual (clic con el botón secundario) del elemento del esquema y seleccione Aplicar a base de datos. Para obtener más información, consulte la documentación de AWS SCT.	Ingeniero de migraciones

Migración de datos

Tarea	Descripción	Habilidades requeridas
Configurar grupos de parámetros de base de datos y una VPC.	Configure grupos de parámetors de base de datos y una VPC, y configure las reglas y parámetros de entrada necesarios para la migración. Para obtener instrucciones, consulte la Documentación de AWS DMS. Para el grupo de seguridad de VPC, seleccione la EC2 instancia para Db2 y la instancia de base de datos compatible con Aurora PostgreSQL. Esta instancia de replicación debe estar en la misma región que las instancias de base de datos de origen y de destino.	Ingeniero de migraciones
Prepare las instancias de base de datos de origen y destino.	Prepare las instancias de base de datos de origen y destino para la migración. En un entorno de producción, la base de datos de origen ya existirá. Para la base de datos de origen, el nombre del servidor debe ser el sistema de nombres de dominio (DNS) público de la instancia en la EC2 que se ejecuta Db2. Para el nombre de usuario, puede	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	usar `db2inst1` seguido del puerto, que será 5000 para IBM Db2.	
Crea un EC2 cliente y puntos de conexión de Amazon.	1. Crea un EC2 cliente de Amazon. Puede utilizar este cliente para rellenar la base de datos de origen con datos para replicar. También utiliza este cliente para verificar la replicación mediante la ejecución de consultas en la base de datos de destino. 2. Cree puntos de conexión para la base de datos de origen y la instancia de base de datos de destino para utilizarlos en los siguientes pasos. Para obtener instrucciones, consulte la Documentación de AWS DMS. Debe crear puntos de conexión independientes para las bases de datos de origen y de destino. Para la versión 10.18 o posterior compatible con Aurora PostgreSQL, el puerto será 5432 y podrá obtener el nombre del servidor desde el punto de conexión de la instancia de base de datos.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación.	Cree una instancia de replicación mediante la consola de AWS DMS y especifique los puntos de conexión de origen y destino. La instancia de replicación realiza la migración de datos entre los puntos de conexión. Para obtener más información, consulte la documentación de AWS DMS.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Crear una tarea de AWS DMS para migrar los datos.	Cree una tarea para cargar las tablas de IBM Db2 de origen en la instancia de base de datos PostgreSQL de destino siguiendo los pasos de la documentación de AWS DMS. • Para el origen y el destino, utilice los nombres de los puntos de conexión de origen y destino. • El tipo de migración puede ser de carga completa. • Para la regla de esquema, puede usar el esquema `inst1` de la base de datos Db2. • Para el nombre de la tabla, especifique `%` si desea migrar todas las tablas. Cuando se complete la carga, verá que las tablas de Db2 del esquema `inst1` aparecen en la base de datos compatible con Aurora PostgreSQL.	Ingeniero de migraciones

Recursos relacionados

Referencias

- Documentación de Amazon Aurora
- Documentación del contenedor de datos externos (FDW) de PostgreSQL
- Documentación IMPORT FOREIGN SCHEMA de PostgreSQL

- Documentación de AWS DMS
- Documentación de AWS SCT

Tutoriales y videos

- Introducción a AWS DMS (guía)
- Introducción a Amazon EC2 : Elastic Cloud Server & Hosting con AWS (vídeo)

Migre de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante AWS DMS SharePlex

Kumar Babu P G, Amazon Web Services

Resumen

Este patrón describe cómo migrar una base de datos de Oracle 8i o 9i en las instalaciones a una base de datos de Amazon Relational Database Service (Amazon RDS) para PostgreSQL o Amazon Aurora PostgreSQL. AWS Database Migration Service (AWS DMS) no admite Oracle 8i o 9i como fuente, por lo que Quest SharePlex replica los datos de una base de datos 8i o 9i local en una base de datos Oracle intermedia (Oracle 10g u 11g), que es compatible con AWS DMS.

Desde la instancia intermedia de Oracle, el esquema y los datos se migran a la base de datos PostgreSQL en AWS mediante la herramienta de conversión de esquemas de AWS (AWS SCT) y AWS DMS. Este método ayuda a lograr una transmisión continua de datos desde la base de datos de Oracle de origen a la instancia de base de datos PostgreSQL de destino con un retraso de replicación mínimo. En esta implementación, el tiempo de inactividad se limita al tiempo que se tarda en crear o validar todas las claves, activadores y secuencias externas en la base de datos PostgreSQL de destino.

La migración utiliza una instancia de Amazon Elastic Compute Cloud (Amazon EC2) con Oracle 10g u 11g instalado para alojar los cambios de la base de datos Oracle de origen. AWS DMS utiliza esta instancia intermedia de Oracle como fuente para transmitir los datos a Amazon RDS para PostgreSQL o Aurora PostgreSQL. La replicación de datos se puede pausar y reanudar desde la base de datos de Oracle en las instalaciones a la instancia intermedia de Oracle. También se puede pausar y reanudar desde la instancia intermedia de Oracle hasta la base de datos PostgreSQL de destino para que pueda validar los datos mediante la validación de datos de AWS DMS o una herramienta de validación de datos personalizada.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de Oracle 8i o 9i de origen en un centro de datos en las instalaciones
- AWS Direct Connect, configurado entre el centro de datos en las instalaciones y AWS
- Controladores de conectividad de bases de datos Java (JDBC) para conectores SCT de AWS instalados en una máquina local o en la instancia en la EC2 que está instalado AWS SCT

- Uso de una base de datos de Oracle como origen para AWS DMS
- Uso de una base de datos de PostgreSQL como destino para AWS DMS
- Familiaridad con la replicación de datos de Quest SharePlex

Limitaciones

- El límite de tamaño de la base de datos es de 64 TB
- La base de datos de Oracle en las instalaciones debe ser Enterprise Edition

Versiones de producto

- Oracle 8i o 9i para la base de datos de origen
- Oracle 10g o 11g para la base de datos intermedia
- PostgreSQL 9.6 o posterior

Arquitectura

Pila de tecnología de origen

- Base de datos de Oracle 8i o 9i
- Quest SharePlex

Pila de tecnología de destino

- Amazon RDS para PostgreSQL o Amazon Aurora PostgreSQL.

Arquitectura de origen y destino

Tools (Herramientas)

- AWS DMS – AWS Database Migration Service (AWS DMS) ayuda a migrar los datos de forma rápida y segura a AWS. La base de datos de origen permanece totalmente operativa durante la

migración, minimizando así el tiempo de inactividad de las aplicaciones que dependen de ella. AWS DMS puede migrar sus datos desde y hasta las bases de datos comerciales y de código abierto más usadas.

- AWS SCT – La herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado, incluidas las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino. Los objetos que no se conviertan automáticamente se marcan claramente para que puedan convertirse manualmente con el objetivo de completar la migración. AWS SCT también puede analizar el código fuente de su aplicación en busca de instrucciones de SQL incrustadas y convertirlas como parte de un proyecto de conversión de esquemas de bases de datos. Durante este proceso, AWS SCT optimiza el código nativo en la nube al convertir las funciones heredadas de Oracle y SQL Server en sus equivalentes de AWS, para ayudarlo a modernizar sus aplicaciones mientras migra sus bases de datos. Una vez finalizada la conversión del esquema, AWS SCT puede ayudar a migrar datos de una variedad de almacenamiento de datos a Amazon Redshift mediante el uso de agentes de migración de datos integrados.
- Quest SharePlex: Quest SharePlex es una herramienta de replicación de Oracle-to-Oracle datos para mover datos con un tiempo de inactividad mínimo y sin pérdida de datos.

Epics

Cree la EC2 instancia e instale Oracle

Tarea	Descripción	Habilidades requeridas
Configura la red para Amazon EC2.	Creación de la nube privada virtual (VPC), subredes, puerta de enlace de Internet, tablas de enrutamiento y grupos de seguridad.	AWS SysAdmin
Crea la nueva EC2 instancia.	Selecciona Amazon Machine Image (AMI) para la EC2 instancia. Elija el tamaño de la instancia y configura los detalles de la instancia : la cantidad de instancias	AWS SysAdmin

Tarea	Descripción	Habilidades requeridas
	(1), la VPC y la subred del paso anterior, la asignación automática de la IP pública y otras opciones. Agregue almacenamiento, configure grupos de seguridad y lance la instancia. Cuando se le pida, cree y guarde un par de claves para el siguiente paso.	
Instale Oracle en la EC2 instancia.	Adquiera las licencias y los binarios de Oracle necesarios e instale Oracle 10g u 11g en la instancia. EC2	Administrador de base de datos

Configure SharePlex en una EC2 instancia y configure la replicación de datos

Tarea	Descripción	Habilidades requeridas
Configurar SharePlex.	Cree una EC2 instancia de Amazon e instale los SharePlex binarios compatibl es con Oracle 8i o 9i.	AWS SysAdmin, administrador de bases de datos
Configure la replicación de datos.	Siga las prácticas SharePlex recomendadas para configura r la replicación de datos desde una base de datos Oracle 8i/9i local a una instancia Oracle 10g/11g.	Administrador de base de datos

Convertir el esquema de base de datos de Oracle a PostgreSQL

Tarea	Descripción	Habilidades requeridas
Configure AWS SCT.	Cree un informe nuevo y, a continuación, conéctese a Oracle como origen y a PostgreSQL como destino. En la configuración del proyecto, abra la pestaña SQL Scripting y cambie el script SQL de destino a Varios archivos.	Administrador de base de datos
Convertir el esquema de base de datos de Oracle.	En la pestaña Acción, elija Generar informe, Convertir esquema y, a continuación, Guardar como SQL.	Administrador de base de datos
Modifique los scripts SQL generados por AWS SCT.		Administrador de base de datos

Creación y configuración de la instancia de base de datos de Amazon RDS

Tarea	Descripción	Habilidades requeridas
Creación de una instancia de base de datos de Amazon RDS	En la consola de Amazon RDS, cree una nueva instancia de base de datos PostgreSQL.	AWS SysAdmin, administrador de bases de datos
Configure la instancia de base de datos.	Especifique la versión del motor de base de datos, la clase de instancia de base de datos, la implement ación Multi-AZ, el tipo de almacenamiento y el almacenamiento asignado.	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	Introduzca el identificador de la instancia de base de datos, un nombre de usuario maestro y una contraseña maestra.	
Configurar la red y la seguridad.	Especifique la VPC, el grupo de subredes, la accesibilidad pública, la preferencia de zona de disponibilidad y los grupos de seguridad.	AWS SysAdmin, administrador de bases de datos
Configurar las opciones de la base de datos.	Especifique el nombre, el puerto, el grupo de parámetros, el cifrado y la clave maestra de la base de datos.	AWS SysAdmin, administrador de bases de datos
Configure copias de seguridad.	Especifique el período de retención de la copia de seguridad, la ventana de copia de seguridad, la hora de inicio, la duración y si desea copiar las etiquetas a las instantáneas.	AWS SysAdmin, administrador de bases de datos
Configure las opciones de monitoreo.	Habilite y desactive la monitorización mejorada de información sobre rendimiento.	AWS SysAdmin, administrador de bases de datos
Configurar las opciones de mantenimiento.	Especifique la actualización automática de la versión secundaria, el período de mantenimiento y el día, la hora y la duración de inicio.	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Ejecute los scripts previos a la migración desde AWS SCT.	En la instancia de Amazon RDS, ejecute los siguientes scripts: reate_database.sql , create_sequence.sql, create_table.sql, create_vi ew.sql y create_function.sql.	AWS SysAdmin, administrador de bases de datos

Migración de datos mediante AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicaci ón en AWS DMS.	Complete los campos para el nombre, la clase de instancia , la VPC (igual que para la EC2 instancia), la zona de disponibilidad múltiple y la accesibilidad pública. En la sección de configuración avanzada, especifique el almacenamiento asignado, el grupo de subredes, la zona de disponibilidad, los grupos de seguridad de VPC y la clave raíz de AWS Key Managemen t Service (AWS KMS).	AWS SysAdmin, administrador de bases de datos
Cree el punto de conexión de origen de la base de datos.	Especifique el nombre, el tipo, el motor de origen (Oracle), el nombre del servidor (nombre DNS EC2 privado de Amazon), el puerto, el modo SSL, el nombre de usuario, la contraseña, el SID, la VPC (especifique la VPC que tiene	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	la instancia de replicación) y la instancia de replicación. Para probar la conexión, seleccione Ejecutar prueba y, a continuación, cree el punto de conexión. También puede configurar los siguientes ajustes avanzados: maxFileSize y numberDataType Scale.	
Cree una tarea de replicación de AWS DMS.	Especifique el nombre de la tarea, la instancia de replicación, los puntos de conexión de origen y destino y la instancia de replicación. Para tipo de migración, seleccione la opción «Migrate existing data and replication ongoing changes» (Migración de los datos existentes y réplica de los cambios en curso). Desactive la casilla de verificación «Start task on create» (Iniciar la tarea al crearla).	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Configure la configuración de la tarea de replicación de AWS DMS.	Para el modo de preparación de la tabla de destino, elija «Do nothing» (No hacer nada). Detenga la tarea cuando se complete la carga completa para crear las claves principales. Especifique el modo LOB limitado o completo y habilite las tablas de control. Si lo desea, puede configurar la configuración CommitRate avanzada.	Administrador de base de datos
Configure las asignaciones de tablas.	En la sección Mapeos de tablas, cree una regla de Inclusión para todas las tablas de todos los esquemas incluidos en la migración y, a continuación, cree una regla de Exclusión. Agregue tres reglas de transformación para convertir los nombres del esquema, la tabla y las columnas a minúsculas y añada cualquier otra regla necesaria para esta migración específica.	Administrador de base de datos
Iniciar la tarea.	Iniciar la tarea de replicación. Asegúrese de que la carga completa está ejecutando. Ejecute ALTER SYSTEM SWITCH LOGFILE en la base de datos principal de Oracle para iniciar la tarea.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Ejecute los scripts de la migración intermedia desde AWS SCT.	En Amazon RDS para PostgreSQL, ejecute los siguientes scripts: create_index.sql y create_constraint.sql.	Administrador de base de datos
Reinicie la tarea para continuar con la captura de datos de cambio (CDC).	Ejecute VACUUM en la instancia de base de datos Amazon RDS para PostgreSQL y reinicie la tarea de AWS DMS para aplicar los cambios de CDC en caché.	Administrador de base de datos

Realizar la transición a la base de datos de PostgreSQL

Tarea	Descripción	Habilidades requeridas
Consulte los registros y las tablas de metadatos de AWS DMS.	Valide cualquier error y corríjalo si es necesario.	Administrador de base de datos
Detenga todas las dependencias de Oracle.	Cierre los oyentes de la base de datos de Oracle y ejecute ALTER SYSTEM SWITCH LOGFILE. Detenga la tarea de AWS DMS cuando no muestre actividad.	Administrador de base de datos
Ejecute los scripts posteriores a la migración desde AWS SCT.	En Amazon RDS para PostgreSQL, ejecute los siguientes scripts: create_foreign_key_constraint.sql y create_triggers.sql.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Complete los pasos adicionales de Amazon RDS para PostgreSQL.	Aumente las secuencias para que coincidan con las de Oracle si es necesario, ejecute VACUUM y ANALYZE y tome una instantánea para comprobar la conformidad.	Administrador de base de datos
Abra las conexiones hacia Amazon RDS para PostgreSQL.	Elimine los grupos de seguridad de AWS DMS de Amazon RDS para PostgreSQL, añada grupos de seguridad de producción y dirija sus aplicaciones a la nueva base de datos.	Administrador de base de datos
Limpie los recursos de AWS DMS.	Elimine los puntos finales, las tareas de replicación, las instancias de replicación y la EC2 instancia.	SysAdmin, DBA

Recursos relacionados

- Documentación de AWS DMS
- Documentación de AWS SCT
- Precio de Amazon RDS para PostgreSQL
- Uso de una base de datos de Oracle como origen para AWS DMS
- Uso de una base de datos de PostgreSQL como destino para AWS DMS
- Documentación de Quest SharePlex

Migración de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante la vista materializada y AWS DMS

Kumar Babu P G y Pragnesh Patel, Amazon Web Services

Resumen

Este patrón describe cómo migrar una base de datos de Oracle 8i o 9i en las instalaciones a una base de datos de Amazon Relational Database Service (Amazon RDS) para PostgreSQL o para una edición compatible de Amazon Aurora PostgreSQL.

AWS Database Migration Service (AWS DMS) no admite Oracle 8i o 9i como fuente, por lo que este patrón utiliza una instancia de base de datos de Oracle intermedia que es compatible con AWS DMS, como Oracle 10g u 11g. También utiliza la característica de vistas materializadas para migrar los datos de la instancia 8i/9i de origen de Oracle a la instancia intermedia 10g/11g de Oracle.

La Herramienta de conversión de esquemas de AWS (AWS SCT) convierte el esquema de la base de datos y AWS DMS migra los datos a la base de datos PostgreSQL de destino.

Este patrón ayuda a los usuarios que desean migrar desde bases de datos de Oracle heredadas con un tiempo de inactividad mínimo. En esta implementación, el tiempo de inactividad se limita al tiempo que se tarda en crear o validar todas las claves externas, activadores y secuencias en la base de datos de destino.

El patrón utiliza instancias de Amazon Elastic Compute Cloud (Amazon EC2) con una base de datos Oracle 10g/11g instalada para ayudar a AWS DMS a transmitir los datos. Puede pausar temporalmente la replicación del streaming desde la base de datos de Oracle en las instalaciones a una instancia de Oracle para activar AWS DMS y ponerse al día con la validación de datos o para utilizar otra herramienta de validación de datos. La instancia de base de datos PostgreSQL y la base de datos intermedia de Oracle tendrán los mismos datos cuando AWS DMS haya terminado de migrar los cambios actuales.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de Oracle 8i o 9i de origen en un centro de datos en las instalaciones
- AWS Direct Connect, configurado entre el centro de datos en las instalaciones y AWS

- Controladores de conectividad de bases de datos Java (JDBC) para conectores SCT de AWS instalados en una máquina local o en la instancia en la EC2 que está instalado AWS SCT
- Uso de una base de datos de Oracle como origen para AWS DMS
- Uso de una base de datos de PostgreSQL como destino para AWS DMS

Limitaciones

- El límite de tamaño de la base de datos es de 64 TB

Versiones de producto

- Oracle 8i o 9i para la base de datos de origen
- Oracle 10g o 11g para la base de datos intermedia
- PostgreSQL 10.17 o posterior

Arquitectura

Pila de tecnología de origen

- Base de datos de Oracle 8i o 9i

Pila de tecnología de destino

- Amazon RDS para PostgreSQL o Aurora PostgreSQL compatibles

Arquitectura de destino

Tools (Herramientas)

- AWS DMS ayuda a migrar las bases de datos de forma rápida y segura. La base de datos de origen permanece totalmente operativa durante la migración, minimizando así el tiempo de inactividad de las aplicaciones que dependen de ella. AWS DMS puede migrar sus datos desde y hasta las bases de datos comerciales y de código abierto más usadas.
- AWS SCT ayuda a convertir automáticamente el esquema de la base de datos de origen y la mayor parte de los objetos de código de la base de datos, incluidas las vistas, los procedimientos

almacenados y las funciones, a un formato compatible con la base de datos de destino. Los objetos que no se conviertan automáticamente se marcan claramente para que puedan convertirse manualmente con el objetivo de completar la migración. AWS SCT también puede analizar el código fuente de su aplicación en busca de instrucciones de SQL incrustadas y convertirlas como parte de un proyecto de conversión de esquemas de bases de datos. Durante este proceso, AWS SCT optimiza el código nativo en la nube al convertir las funciones heredadas de Oracle y SQL Server en sus equivalentes de AWS, para ayudarlo a modernizar sus aplicaciones mientras migra sus bases de datos. Una vez finalizada la conversión del esquema, AWS SCT puede ayudar a migrar datos de una variedad de almacenamiento de datos a Amazon Redshift mediante el uso de agentes de migración de datos integrados.

Prácticas recomendadas

Para conocer las prácticas recomendadas para actualizar las vistas materializadas, consulte la siguiente documentación de Oracle:

- Actualización de vistas materializadas
- Actualización rápida para vistas materializadas

Epics

Instale Oracle en una EC2 instancia y cree vistas materializadas

Tarea	Descripción	Habilidades requeridas
Configure la red para la EC2 instancia.	Creación de la nube privada virtual (VPC), subredes, puerta de enlace de Internet, tablas de enrutamiento y grupos de seguridad.	AWS SysAdmin
Crea la EC2 instancia.	Selecciona Amazon Machine Image (AMI) para la EC2 instancia. Elija el tamaño de la instancia y configura los detalles de la instancia : la cantidad de instancias	AWS SysAdmin

Tarea	Descripción	Habilidades requeridas
	(1), la VPC y la subred del paso anterior, la asignación automática de la IP pública y otras opciones. Agregue almacenamiento, configure grupos de seguridad y lance la instancia. Cuando se le pida, cree y guarde un par de claves para el siguiente paso.	
Instale Oracle en la EC2 instancia.	Adquiera las licencias y los binarios de Oracle necesarios e instale Oracle 10g u 11g en la instancia. EC2	Administrador de base de datos
Configure las redes de Oracle.	Modifique o añada entradas en `listener.ora` para conectarse a la base de datos de Oracle 8i/9i de origen en las instalaciones y, a continuación, cree los enlaces de la base de datos.	Administrador de base de datos
Cree vistas materializadas.	Identifique los objetos de la base de datos que desee replicar en la base de datos de Oracle 8i/9i de origen y, a continuación, cree vistas materializadas de todos los objetos mediante el enlace a la base de datos.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Implemente scripts para actualizar las vistas materiali zadas a los intervalos necesarios.	Desarrolle e implemente scripts para actualizar las vistas materializadas a los intervalos requeridos en la instancia Amazon EC2 Oracle 10g/11g. Utilice la opción de actualización incremental para refrescar las vistas materiali zadas.	Administrador de base de datos

Convertir el esquema de base de datos de Oracle a PostgreSQL

Tarea	Descripción	Habilidades requeridas
Configure AWS SCT.	Cree un informe nuevo y, a continuación, conéctese a Oracle como origen y a PostgreSQL como destino. En la Configuración del proyecto, vaya a la pestaña SQL Scripting. Cambie el Script SQL de destino a Varios archivos. (AWS SCT no es compatible con las bases de datos de Oracle 8i/9i, por lo que debe restaurar el volcado exclusivo del esquema en la instancia intermedia de Oracle 10g/11g y usarlo como fuente para AWS SCT).	Administrador de base de datos
Convertir el esquema de base de datos de Oracle.	En la pestaña Action (Acción), elija Generate Report (Generar informe), Convert	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Schema (Convertir esquema) y, a continuación, Save as SQL (Guardar como SQL).	
Modifique los scripts SQL.	Realice las modificaciones en función de las prácticas recomendadas. Por ejemplo, cambie a los tipos de datos adecuados y desarrolle equivalentes de PostgreSQL para funciones específicas de Oracle.	Administrador de base de datos, DevDBA

Creación y configuración de la instancia de base de datos de Amazon RDS para alojar la base de datos convertida

Tarea	Descripción	Habilidades requeridas
Creación de una instancia de base de datos de Amazon RDS	En la consola de Amazon RDS, cree una nueva instancia de base de datos PostgreSQL.	AWS SysAdmin, DBA
Configure la instancia de base de datos.	Especifique la versión del motor de base de datos, la clase de instancia de base de datos, la implement ación Multi-AZ, el tipo de almacenamiento y el almacenamiento asignado. Introduzca el identificador de la instancia de base de datos, un nombre de usuario maestro y una contraseña maestra.	AWS SysAdmin, DBA

Tarea	Descripción	Habilidades requeridas
Configurar la red y la seguridad.	Especifique la VPC, el grupo de subredes, la accesibilidad pública, la preferencia de zona de disponibilidad y los grupos de seguridad.	DBA, SysAdmin
Configurar las opciones de la base de datos.	Especifique el nombre, el puerto, el grupo de parámetros, el cifrado y la clave maestra de la base de datos.	ADMINISTRADOR DE BASES DE DATOS, AWS SysAdmin
Configure copias de seguridad.	Especifique el período de retención de la copia de seguridad, la ventana de copia de seguridad, la hora de inicio, la duración y si desea copiar las etiquetas a las instantáneas.	AWS SysAdmin, DBA
Configure las opciones de monitoreo.	Habilite y desactive la monitorización mejorada de información sobre rendimiento.	AWS SysAdmin, DBA
Configurar las opciones de mantenimiento.	Especifique la actualización automática de la versión secundaria, el período de mantenimiento y el día, la hora y la duración de inicio.	AWS SysAdmin, DBA

Tarea	Descripción	Habilidades requeridas
Ejecute los scripts previos a la migración desde AWS SCT.	En la instancia de Amazon RDS para PostgreSQL de destino, cree el esquema de base de datos mediante los scripts SQL de AWS SCT con otras modificaciones. Estas pueden incluir la ejecución de varios scripts e incluir la creación de usuarios, la creación de bases de datos, la creación de esquemas, tablas, vistas, funciones y otros objetos de código.	AWS SysAdmin, DBA

Migración de datos mediante AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación en AWS DMS.	Complete los campos para el nombre, la clase de instancia, la VPC (igual que para la EC2 instancia), la zona de disponibilidad múltiple y la accesibilidad pública. En la configuración avanzada, especifique el almacenamiento asignado, el grupo de subredes, la zona de disponibilidad, los grupos de seguridad de VPC y la clave de AWS Key Management Service (AWS KMS).	AWS SysAdmin, DBA
Cree el punto de conexión de origen de la base de datos.	Especifique el nombre, el tipo, el motor de origen (Oracle),	AWS SysAdmin, DBA

Tarea	Descripción	Habilidades requeridas
	el nombre del servidor (el nombre DNS privado de la EC2 instancia), el puerto, el modo SSL, el nombre de usuario, la contraseña, el SID, la VPC (especifique la VPC que tiene la instancia de replicación) y la instancia de replicación. Para probar la conexión, seleccione Ejecutar prueba y, a continuación, cree el punto de conexión. También puede configurar los siguientes ajustes avanzados : maxFileSizey numberDat aType Scale.	
Conecte AWS DMS a Amazon RDS para PostgreSQL.	Cree un grupo de seguridad de migración para las conexiones entre sí VPCs, si su base de datos PostgreSQL está en otra VPC.	AWS SysAdmin, DBA

Tarea	Descripción	Habilidades requeridas
Cree puntos de conexión de base de datos de destino.	Especifique el nombre del punto de conexión, el tipo, el motor de origen (PostgreSQL), el nombre del servidor (punto de conexión de Amazon RDS), el puerto, el modo SSL, el nombre de usuario, la contraseña, el nombre de la base de datos, la VPC (especifique la VPC que tiene la instancia de replicación) y la instancia de replicación. Para probar la conexión, seleccione Ejecutar prueba y, a continuación, cree el punto de conexión. También puede configurar los siguientes ajustes avanzados: maxFileSizey numberDataTypeScale.	AWS SysAdmin, DBA
Cree una tarea de replicación de AWS DMS.	Especifique el nombre de la tarea, la instancia de replicación, los puntos de conexión de origen y destino y la instancia de replicación. Para tipo de migración, seleccione la opción Migrate existing data and replication ongoing changes (Migración de los datos existentes y réplica de los cambios en curso). Desactive la casilla Start task on create (Iniciar la tarea al crearla).	AWS SysAdmin, DBA

Tarea	Descripción	Habilidades requeridas
Configure la configuración de la tarea de replicación de AWS DMS.	Para el modo de preparación de la tabla de destino, elija No hacer nada. Detenga la tarea cuando se complete la carga completa para crear las claves principales. Especifique el modo LOB limitado o completo y habilite las tablas de control. Si lo desea, puede configura r la configuración CommitRat eavanzada.	Administrador de base de datos
Configure las asignaciones de tablas.	En la sección Table mappings (Mapeos de tabla), cree una regla de inclusión para todas las tablas de todos los esquemas incluidos en la migración y, a continuación, cree una regla de exclusión . Agregue tres reglas de transformación para convertir los nombres del esquema, la tabla y las columnas a minúsculas y añada cualquier otra regla necesaria para esta migración específica.	Administrador de base de datos
Iniciar la tarea.	Iniciar la tarea de replicación. Asegúrese de que la carga completa está ejecutand o. Ejecute `ALTER SYSTEM SWITCH LOGFILE` en la base de datos principal de Oracle para iniciar la tarea.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Ejecute los scripts de la migración intermedia desde AWS SCT.	En Amazon RDS para PostgreSQL, ejecute los siguientes scripts: `create_index.sql` y `create_constraint.sql` (si el esquema completo no se creó inicialmente).	Administrador de base de datos
Reanude la tarea para continuar con la captura de datos de cambio (CDC).	Ejecute `VACUUM` en la instancia de base de datos Amazon RDS para PostgreSQL y reinicie la tarea de AWS DMS para aplicar los cambios de CDC en caché.	Administrador de base de datos

Realizar la transición a la base de datos de PostgreSQL

Tarea	Descripción	Habilidades requeridas
Consulte los registros y las tablas de validación de AWS DMS.	Compruebe y corrija cualquier error de replicación o validación.	Administrador de base de datos
Deje de utilizar la base de datos de Oracle en las instalaciones y sus dependencias.	Detenga todas las dependencias de Oracle, cierre los oyentes de la base de datos de Oracle y ejecute `ALTER SYSTEM SWITCH LOGFILE`. Detenga la tarea de AWS DMS cuando no muestre actividad.	Administrador de base de datos
Ejecute los scripts posteriores a la migración desde AWS SCT.	En Amazon RDS para PostgreSQL, ejecute estos scripts: `create_fo`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`reign_key_constrai nt.sql and create_tr iggers.sql` . Asegúrese de que las secuencias estén actualizadas.	
Complete los pasos adicional es de Amazon RDS para PostgreSQL.	Aumente las secuencias para que coincidan con las de Oracle si es necesario, ejecute `VACUUM` y ANALYZE y `ANALYZE`, y tome una instantánea para comprobar la conformidad.	Administrador de base de datos
Abra las conexiones hacia Amazon RDS para PostgreSQ L.	Elimine los grupos de seguridad de AWS DMS de Amazon RDS para PostgreSQ L, añada grupos de seguridad de producción y dirija sus aplicaciones a la nueva base de datos.	Administrador de base de datos
Limpie los objetos de AWS DMS.	Elimine los puntos finales, las tareas de replicación, las instancias de replicación y la EC2 instancia.	SysAdmin, DBA

Recursos relacionados

- Documentación de AWS DMS
- Documentación de AWS SCT
- Precio de Amazon RDS para PostgreSQL
- Uso de una base de datos de Oracle como origen para AWS DMS
- Uso de una base de datos de PostgreSQL como destino para AWS DMS

Migración de Oracle en Amazon EC2 a Amazon RDS para MySQL con AWS DMS y AWS SCT

Anil Kunapareddy, Amazon Web Services

Harshad Gohil, ninguno

Resumen

La administración de bases de datos de Oracle en instancias de Amazon Elastic Compute Cloud (Amazon EC2) requiere recursos y puede resultar costosa. Mover estas bases de datos a una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para MySQL le facilitará el trabajo al optimizar el presupuesto global de TI. Amazon RDS para MySQL también ofrece funciones como Multi-AZ, escalabilidad y copias de seguridad automáticas.

Este patrón le guía a través de la migración de una base de datos de Oracle de origen en Amazon EC2 a una instancia de base de datos Amazon RDS para MySQL de destino. Utiliza AWS Database Migration Service (AWS DMS) para migrar los datos y la Herramienta de conversión de esquemas de AWS (AWS SCT) para convertir el esquema y los objetos de la base de datos de origen a un formato compatible con Amazon RDS para MySQL.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos fuente con servicios de instancia y escucha en ejecución, en modo ARCHIVELOG
- Una base de datos Amazon RDS para MySQL de destino, con suficiente almacenamiento para la migración de datos

Limitaciones

- AWS DMS no crea un esquema en la base de datos de destino; debe hacerlo usted. El nombre de esquema ya tiene que existir para el destino. Las tablas del esquema de origen se importan al usuario o esquema que AWS DMS utiliza para conectarse a la instancia de destino. Debe crear varias tareas de replicación si tiene que migrar varios esquemas.

Versiones de producto

- Todas las ediciones de las bases de datos de Oracle para las versiones 10.2 y posteriores, 11g y versiones posteriores a la 12.2 y 18c. Para ver la lista actualizada de versiones compatibles, consulte Uso de una base de datos de Oracle como fuente para AWS DMS y Uso de una base de datos compatible con MySQL como destino para AWS DMS. Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características. Para obtener información sobre las versiones de bases de datos de Oracle compatibles con AWS SCT, consulte la documentación de AWS SCT.
- AWS DMS es compatible con las versiones 5.5, 5.6 y 5.7 de MySQL.

Arquitectura

Pila de tecnología de origen

- Una base de datos de Oracle en una instancia EC2

Pila de tecnología de destino

- Instancia de base de datos de Amazon RDS para MySQL

Arquitectura de migración de datos

Arquitectura de origen y destino

Tools (Herramientas)

- AWS DMS: AWS Database Migration Service (AWS DMS) es un servicio web que puede utilizar para migrar datos de una base de datos en las instalaciones, de una instancia de base de datos de Amazon RDS o de una base de datos de una instancia EC2 a una base de datos de un servicio de AWS, como Amazon RDS para MySQL o una instancia EC2. Puede también migrar desde una base de datos de un servicio de AWS a otra base de datos local. Puede migrar datos entre motores de bases de datos heterogéneos u homogéneos.
- AWS SCT: la herramienta de conversión de esquemas de AWS (AWS SCT) hace más predecible las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado, incluidas las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de

destino. Tras convertir el esquema de la base de datos y los objetos de código mediante AWS SCT, puede utilizar AWS DMS para migrar los datos de la base de datos de origen a la base de datos de destino para completar sus proyectos de migración.

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Identifique las versiones y motores de la base de datos de origen y destino.		Administrador de base de datos/desarrollador
Identifique la instancia de replicación de DMS.		Administrador de base de datos/desarrollador
Identifique los requisitos de almacenamiento, como el tipo y la capacidad de almacenamiento.		Administrador de base de datos/desarrollador
Identifique los requisitos de la red, como la latencia y el ancho de banda.		Administrador de base de datos/desarrollador
Identifique los requisitos de hardware para las instancias del servidor de origen y destino (según la lista de compatibilidad de Oracle y los requisitos de capacidad).		Administrador de base de datos/desarrollador
Identifique requisitos de seguridad para acceder a la red de las bases de datos de origen y destino.		Administrador de base de datos/desarrollador

Tarea	Descripción	Habilidades requeridas
Instale los controladores AWS SCT y Oracle.		Administrador de base de datos/desarrollador
Determine una estrategia de copia de seguridad.		Administrador de base de datos/desarrollador
Determine los requisitos de disponibilidad.		Administrador de base de datos/desarrollador
Identifique la estrategia de migración y cambio de aplicaciones.		Administrador de base de datos/desarrollador
Seleccione el tipo de instancia de base de datos adecuado en función de la capacidad , el almacenamiento y las características de la red.		Administrador de base de datos/desarrollador

Configure el entorno

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC). El origen, el destino y la instancia de replicación deben estar en la misma VPC. También es bueno tenerlos en la misma zona de disponibi lidad.		Desarrollador
Cree los grupos de seguridad necesarios para el acceso a la base de datos.		Desarrollador

Tarea	Descripción	Habilidades requeridas
Genere y configure un par de claves.		Desarrollador
Configure las subredes, las zonas de disponibilidad y los bloques CIDR.		Desarrollador

Configure la fuente: base de datos de Oracle en una instancia EC2

Tarea	Descripción	Habilidades requeridas
Instale Oracle Database en Amazon EC2 con los usuarios y roles necesarios.		Administrador de base de datos
Realice los tres pasos de la siguiente columna para acceder a Oracle desde fuera de la instancia EC2.	1. Cambie el host local en `tnsnames` al DNS público de Amazon EC2. 2. Cambie el host local en `listener` al DNS público de Amazon EC2. 3. Detenga y vuelva a iniciar el oyente.	Administrador de base de datos
Cuando se reinicia Amazon EC2, el DNS público cambia. Asegúrese de actualizar el DNS público de Amazon EC2 en “tnsnames” y “listener ” o utilice una dirección IP elástica.		Administrador de base de datos/desarrollador
Configure el grupo de seguridad de la instancia de EC2 para que la instancia		Administrador de base de datos/desarrollador

Tarea	Descripción	Habilidades requeridas
de replicación y los clientes necesarios puedan acceder a la base de datos de origen.		

Configure el destino: Amazon RDS para MySQL

Tarea	Descripción	Habilidades requeridas
Configure e inicie la instancia de base de datos de Amazon RDS para MySQL.		Desarrollador
Cree el espacio de tablas necesario en la instancia de base de datos de Amazon RDS para MySQL.		Administrador de base de datos
Configure el grupo de seguridad para que la instancia de replicación y los clientes necesarios puedan acceder a la base de datos de destino.		Desarrollador

Configure AWS SCT y cree un esquema en la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Instale los controladores AWS SCT y Oracle.		Desarrollador
Introduzca los parámetros adecuados y conéctese a la fuente y al destino.		Desarrollador

Tarea	Descripción	Habilidades requeridas
Genere un informe de conversión de esquemas.		Desarrollador
Corrija el código y el esquema según sea necesario, especialmente los espacios de tabla y las comillas, y ejecútelos en la base de datos de destino.		Desarrollador
Valide el esquema en el origen y en el destino antes de migrar los datos.		Desarrollador

Migración de datos utilizando AWS DMS

Tarea	Descripción	Habilidades requeridas
Para carga completa y la captura de datos de cambios (CDC) o simplemente para CDC, debe configurar un atributo de conexión adicional.		Desarrollador
Al usuario especificado en las definiciones de la base de datos de Oracle de origen de AWS DMS se le deben conceder todos los privilegi os necesarios. Para obtener una lista completa, consulte https://docs.aws.amazon.com /dms/ latest/userguide/C HAP _Source.Oracle.html		Administrador de base de datos/desarrollador

Tarea	Descripción	Habilidades requeridas
#CHAP_Source .Oracle.Self-Managed.		
Habilitar el registro suplementario en la base de datos de origen.		Administrador de base de datos/desarrollador
Para la captura completa de datos y cambios (CDC) o simplemente CDC, habilite el modo ARCHIVELOG en la base de datos de origen.		Administrador de base de datos
Cree puntos de conexión de origen y destino y pruebe las conexiones.		Desarrollador
Cuando los puntos de conexión estén conectados correctamente, cree una tarea de replicación.		Desarrollador
Seleccione solo CDC (o) carga completa más CDC en la tarea para capturar los cambios para la replicación continua únicamente (o) carga completa más los cambios en curso, respectivamente.		Desarrollador
Ejecute la tarea de replicación y supervise CloudWatch los registros de Amazon.		Desarrollador
Valide los datos en las bases de datos de origen y destino.		Desarrollador

Migración de su aplicación y cómo realizar la transición

Tarea	Descripción	Habilidades requeridas
Siga los pasos de su estrategia de migración de aplicaciones.		Administrador de base de datos, desarrollador, propietario de la aplicación
Siga los pasos de su estrategia de transición o cambio de aplicaciones.		Administrador de base de datos, desarrollador, propietario de la aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Valide el esquema y los datos en las bases de datos de origen y de destino.		Administrador de base de datos/desarrollador
Recopile métricas en función del tiempo de migración, el porcentaje de trabajo manual en comparación con el trabajo con herramientas, el ahorro de costos, etc.		DBA/Developer/AppOwner
Revise los documentos y artefactos del proyecto.		DBA/Developer/AppOwner
Cerrar los recursos temporales de AWS.		Administrador de base de datos/desarrollador
Cerrar el proyecto y enviar comentarios.		DBA/Developer/AppOwner

Recursos relacionados

- Documentación de AWS DMS
- Sitio web de AWS DMS
- Publicaciones del blog de AWS DMS
- Strategies for Migrating Oracle Database to AWS
- Amazon RDS para Oracle FAQs
- Preguntas frecuentes sobre Oracle
- Amazon EC2
- Amazon EC2 FAQs
- Concesión de licencias de software de Oracle en el entorno de computación en la nube

Migre una base de datos Oracle de Amazon EC2 a Amazon RDS para MariaDB con AWS DMS y AWS SCT

Veeranjaneyulu Grandhi y Vinod Kumar, Amazon Web Services

Resumen

Este patrón le guía por los pasos para migrar una base de datos Oracle en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) a una instancia de base de datos Amazon Relational Database Service (Amazon RDS) para MariaDB. Este patrón utiliza AWS Data Migration Service (AWS DMS) y Herramienta de conversión de esquemas de AWS (AWS SCT) para la conversión de esquemas.

La administración de bases de datos Oracle en EC2 instancias requiere más recursos y es más costosa que usar una base de datos en Amazon RDS. Amazon RDS facilita la configuración, el funcionamiento y el escalado de una base de datos relacional en la nube. Amazon RDS proporciona una capacidad rentable y redimensionable a la vez que automatiza las tareas de administración que tanto tiempo consumen, como el aprovisionamiento de hardware, la configuración de la base de datos, la aplicación de parches y las copias de seguridad.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una base de datos de Oracle de origen con servicios de instancia y escucha en funcionamiento. Esta base de datos debe estar en modo ARCHIVELOG.
- Estar familiarizado con Usar una base de datos de Oracle como origen para AWS DMS
- Familiaridad con el uso de Oracle como origen para AWS SCT.

Limitaciones

- Límite de tamaño de la base de datos: 64 TB

Versiones de producto

- Todas las ediciones de las bases de datos de Oracle para las versiones 10.2 y posteriores, 11g y versiones posteriores a la 12.2 y 18c. Para ver la lista actualizada de versiones compatibles,

consulte Uso de una base de datos de Oracle como fuente para AWS DMS y la tabla de versiones de AWS SCT en la documentación de AWS.

- Amazon RDS es compatible con las versiones 10.3, 10.4, 10.5 y 10.6 de MariaDB Server Community Server. Para ver la lista más reciente de las versiones admitidas, consulte la documentación de Amazon RDS.

Arquitectura

Pila de tecnología de origen

- Una base de datos Oracle en una instancia EC2

Pila de tecnología de destino

- Amazon RDS para MariaDB

Arquitectura de migración de datos

Arquitectura de destino

Tools (Herramientas)

- La Herramienta de conversión de esquemas de AWS (AWS SCT) hace que las migraciones de bases de datos heterogéneas sean predecibles al convertir automáticamente el esquema de la base de datos de origen y la mayoría de los objetos de código de la base de datos (incluidas las vistas, los procedimientos almacenados y las funciones) a un formato compatible con la base de datos de destino. Tras convertir el esquema de la base de datos y los objetos de código mediante AWS SCT, puede utilizar AWS DMS para migrar los datos de la base de datos de origen a la base de datos de destino para completar sus proyectos de migración. Para obtener más información, consulte Uso de Oracle como fuente de AWS SCT en la documentación de AWS SCT.
- AWS Database Migration Service (AWS DMS) le ayuda a migrar bases de datos a AWS de forma rápida y segura. La base de datos de origen permanece totalmente operativa durante la migración, minimizando así el tiempo de inactividad de las aplicaciones que dependen de ella. AWS DMS puede migrar sus datos desde y hasta las bases de datos comerciales y de código abierto más usadas. AWS DMS admite migraciones homogéneas, como de Oracle a Oracle, así

como migraciones heterogéneas entre diferentes plataformas de bases de datos, como de Oracle o Microsoft SQL Server a Amazon Aurora. Para obtener más información sobre la migración de bases de datos de Oracle, consulte Uso de una base de datos de Oracle como origen para AWS DMS en la documentación de AWS DMS.

Epics

Planificar la migración

Tarea	Descripción	Habilidades requeridas
Identifique las versiones y los motores de bases de datos.	Identifique las versiones y motores de la base de datos de origen y destino.	Administrador de base de datos, desarrollador
Identifique la instancia de replicación.	Identifique la instancia de replicación de AWS DMS.	Administrador de base de datos, desarrollador
Identifique los requisitos de almacenamiento.	Identifique el tipo y la capacidad de almacenam iento.	Administrador de base de datos, desarrollador
Identifique requisitos de red.	Identifique la latencia y el ancho de banda de la red.	Administrador de base de datos, desarrollador
Identifique los requisitos de hardware.	Identifique los requisitos de hardware para las instancia s del servidor de origen y destino (según la lista de compatibilidad de Oracle y los requisitos de capacidad).	Administrador de base de datos, desarrollador
Identifique los requisitos de seguridad.	Identifique los requisitos de seguridad de acceso a la red de las bases de datos de origen y destino.	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
Instalar controladores.	Instale los controladores AWS SCT y Oracle más recientes.	Administrador de base de datos, desarrollador
Determine una estrategia de copia de seguridad.		Administrador de base de datos, desarrollador
Determine los requisitos de disponibilidad.		Administrador de base de datos, desarrollador
Elija una migration/switchover estrategia de aplicación.		Administrador de base de datos, desarrollador
Seleccione el tipo de instancia .	Seleccione el tipo de instancia adecuado en función de la capacidad, el almacenamiento y las características de la red.	Administrador de base de datos, desarrollador

Configure el entorno

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).	Las instancias de origen, destino y replicación deben estar en la misma VPC y en la misma zona de disponibilidad (recomendado).	Desarrollador
Cree grupos de seguridad.	Cree los grupos de seguridad necesarios para el acceso a la base de datos.	Desarrollador
Genere un par de claves.	Genere y configure un par de claves.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Configure otros recursos.	Configure las subredes, las zonas de disponibilidad y los bloques CIDR.	Desarrollador

Configurar el origen

Tarea	Descripción	Habilidades requeridas
Lanza la EC2 instancia.	Para obtener instrucciones, consulta la EC2 documentación de Amazon.	Desarrollador
Instalar la base de datos de Oracle.	Instale la base de datos Oracle en la EC2 instancia , con los usuarios y roles necesarios.	Administrador de base de datos
Siga los pasos de la descripción de la tarea para acceder a Oracle desde fuera de la EC2 instancia.	1. Cambie el host local `tnsnames` al DNS EC2 público de Amazon. 2. Cambie el host local `listener` al DNS EC2 público de Amazon. 3. Detenga y vuelva a iniciar el oyente.	Administrador de base de datos
Actualiza el DNS EC2 público de Amazon.	Una vez reiniciada la EC2 instancia, el DNS público cambia. Asegúrese de actualizar el DNS EC2 público de Amazon en `tnsnames` y`listener`, o utilice una dirección IP elástica.	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
Configure el grupo de seguridad de la EC2 instancia.	Configure el grupo de seguridad de EC2 instancia s para que la instancia de replicación y los clientes necesarios puedan acceder a la base de datos de origen.	Administrador de base de datos, desarrollador

Configurar el entorno de destino de Amazon RDS para MariaDB

Tarea	Descripción	Habilidades requeridas
Inicie la instancia de base de datos de RDS.	Configure e inicie la instancia de la base de datos de Amazon RDS para MariaDB.	Desarrollador
Cree espacios de trabajo.	Cree los espacios de tabla necesarios en la base de datos MariaDB de Amazon RDS MariaDB.	Administrador de base de datos
Configurar un grupo de seguridad.	Configure un grupo de seguridad para que la instancia de replicación y los clientes necesarios puedan acceder a la base de datos de destino.	Desarrollador

Configurar AWS SCT

Tarea	Descripción	Habilidades requeridas
Instalar controladores.	Instale los controladores AWS SCT y Oracle más recientes.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Connect (Conectar).	Introduzca los parámetros adecuados y, a continuac ión, conéctese al origen y al destino.	Desarrollador
Genere un informe de conversión de esquemas.	Genere un informe de conversión del esquemas de AWS SCT.	Desarrollador
Corrija el código y el esquema según sea necesario.	Realice las correcciones necesarias en el código y el esquema (especialmente los espacios de tabla y las comillas).	Administrador de base de datos, desarrollador
Valide el esquema.	Valide el esquema en el origen en comparación con el de destino antes de cargar los datos.	Desarrollador

Migración de datos utilizando AWS DMS

Tarea	Descripción	Habilidades requeridas
Defina un atributo de conexión.	Para cargar completamente y capturar datos de cambios (CDC) o simplemente para CDC, debe configurar un atributo de conexión adicional. Para obtener más información, consulte la documentación de Amazon RDS.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Habilitar el registro suplement ario.	Habilitar el registro suplement ario en la base de datos de origen.	Administrador de base de datos, desarrollador
Habilite el modo de registro de archivos.	Para los CDC de carga completa (o solo para los CDC), habilite el modo de registro de archivos en la base de datos de origen.	Administrador de base de datos
Cree y pruebe puntos de conexión.	Cree puntos de conexión de origen y destino y pruebe las conexiones. Para obtener más información, consulte la documentación de Amazon DMS.	Desarrollador
Cree una tarea de replicación.	Cuando los puntos de conexión estén conectados correctamente, cree una tarea de replicación. Para obtener más información, consulte la documentación de Amazon DMS.	Desarrollador
Elija el tipo de replicación.	Elija Solo CDC o Carga completa más CDC en la tarea para capturar los cambios solo para la replicación continua, o para carga completa y cambios continuos, respectiv amente.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Inicie y monitoree la tarea.	Inicie la tarea de replicación y supervise CloudWatch los registros de Amazon. Para obtener más información, consulte la documentación de Amazon DMS.	Desarrollador
Valide los datos.	Valide los datos en las bases de datos de origen y destino.	Desarrollador

Migración de aplicaciones y cómo realizar la transición a la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Siga la estrategia de migración de aplicaciones elegida.		Administrador de base de datos, propietario de la aplicación, desarrollador
Siga la cutover/switchover estrategia de aplicación elegida.		Administrador de base de datos, propietario de la aplicación, desarrollador

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Valide el esquema y los datos.	Asegúrese de que el esquema y los datos se validen correctamente en el origen en comparación con el destino antes de cerrar el proyecto.	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
Recopile métricas.	Recopile métricas para tiempo de migración, porcentaj e de tareas manuales en comparación con las tareas de herramientas, ahorro de costos y otros criterios similares.	Administrador de base de datos, propietario de la aplicación, desarrollador
Revise la documentación.	Revise los documentos y artefactos del proyecto.	Administrador de base de datos, propietario de la aplicación, desarrollador
Cierre los recursos.	Cerrar los recursos temporale s de AWS.	Administrador de base de datos, desarrollador
Cierre el proyecto.	Cierre el proyecto de migración y envíe sus comentarios.	Administrador de base de datos, propietario de la aplicación, desarrollador

Recursos relacionados

- Información general sobre MariaDB de Amazon RDS
- Detalles del producto de Amazon RDS para MariaDB
- Uso de una base de datos de Oracle como origen para AWS DMS
- Estrategias para migrar bases de datos de Oracle a AWS
- Concesión de licencias de software de Oracle en el entorno de computación en la nube
- Amazon RDS para Oracle FAQs
- Información general sobre AWS DMS
- Publicaciones del blog de AWS DMS
- EC2 Descripción general de Amazon
- Amazon EC2 FAQs
- Documentación de AWS SCT

Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para MySQL con AWS DMS y AWS SCT

Sergey Dmitriev y Naresh Damera, Amazon Web Services

Resumen

Este patrón le guía a través de la migración de una base de datos de Oracle en las instalaciones a una Amazon Relational Database Service (Amazon RDS) para una instancia de base de datos de MySQL. Utiliza AWS Database Migration Service (AWS DMS) para migrar los datos y la Herramienta de conversión de esquemas de AWS (AWS SCT) para convertir el esquema y los objetos de la base de datos de origen a un formato compatible con Amazon RDS para MySQL.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de origen de Oracle en un centro de datos en las instalaciones

Limitaciones

- Límite de tamaño de la base de datos: 64 TB

Versiones de producto

- Todas las ediciones de bases de datos de Oracle para las versiones 11g (versiones 11.2.0.3.v1 y posteriores) y hasta la 12.2, y 18c. Para ver la lista actualizada de versiones compatibles, consulte Uso de una base de datos de Oracle como origen para AWS DMS. Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características. Para obtener información sobre las versiones de bases de datos de Oracle compatibles con AWS SCT, consulte la Documentación de AWS SCT.
- AWS DMS es actualmente compatible con las versiones 5.5, 5.6 y 5.7 de MySQL. Para ver la lista actualizada de versiones compatibles, consulte Uso de una base de datos compatible con MySQL como destino para las versiones de AWS DMS en la documentación de AWS.

Arquitectura

Pila de tecnología de origen

- Base de datos de Oracle en las instalaciones

Pila de tecnología de destino

- Instancia de base de datos de Amazon RDS para MySQL

Arquitectura de migración de datos

Tools (Herramientas)

- AWS DMS: AWS Database Migration Services (AWS DMS) facilita la migración de bases de datos relacionales, almacenamiento de datos, bases de datos NoSQL y otros tipos de almacenes de datos. Puede utilizar AWS DMS para migrar datos a la nube de AWS, entre instancias en las instalaciones (a través de una configuración de nube de AWS) o entre combinaciones de configuraciones en las instalaciones y en la nube.
- AWS SCT: la Herramienta de conversión de esquemas de AWS (AWS SCT) se utiliza para convertir su esquema de base de datos existente de un motor de base de datos a otro. El código personalizado que convierte la herramienta incluye vistas, procedimientos almacenados y funciones. Cualquier código que la herramienta no pueda convertir automáticamente está claramente marcado para que pueda convertirlo usted mismo.

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Valide la versión y el motor de la base de datos de origen y de destino.		Administrador de base de datos
Identifique los requisitos de hardware de la instancia del servidor de destino.		DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
Identifique los requisitos de almacenamiento (el tipo y la capacidad de almacenam iento).		DBA, SysAdmin
Elija el tipo de instancia adecuado en función de la capacidad, las características de almacenamiento y las características de red.		DBA, SysAdmin
Identifique los requisitos de seguridad de acceso a la red para las bases de datos de origen y destino.		DBA, SysAdmin
Identificar la estrategia de migración de aplicaciones.		DBA, propietario de la SysAdmin aplicación

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC) y subredes.		SysAdmin
Cree los grupos de seguridad y las listas de control de acceso a la red (ACLs).		SysAdmin
Configure e inicie una instancia de base de datos de Amazon RDS.		DBA, SysAdmin

Migración de datos

Tarea	Descripción	Habilidades requeridas
Migre el esquema de la base de datos mediante AWS SCT.		Administrador de base de datos
Migre los datos mediante AWS DMS.		Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Utilizar AWS SCT para analizar y convertir el código SQL dentro del código de la aplicación.	Para obtener más informaci ón, consulte https://docs.aws.a mazon.com/SchemaCo nversionTool/ latest/userguide/ CHAP _Converting.app.html.	Propietario de la aplicación
Seguir la estrategia de migración de aplicaciones.		SysAdminDBA, propietario de la aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Cambie los clientes de la aplicación a la nueva infraestr uctura.		DBA, propietario de la SysAdmin aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.		DBA, SysAdmin
Revise y valide los documentos del proyecto.		DBA, SysAdmin
Recopile métricas sobre el tiempo de migración, el porcentaje de migraciones manuales en comparación con las realizadas con herramientas, el ahorro de costos, etc.		DBA, SysAdmin
Cerrar el proyecto y enviar comentarios.		

Recursos relacionados

Referencias

- Documentación de AWS DMS
- Documentación de AWS SCT
- Precios de Amazon RDS

Tutoriales y videos

- Introducción a AWS DMS
- Introducción a Amazon RDS
- AWS DMS (video)
- Amazon RDS (video)

Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para PostgreSQL mediante Oracle Bystander y AWS DMS

Cady Motyka, Amazon Web Services

Resumen

Este patrón describe cómo puede migrar una base de datos de Oracle en las instalaciones a cualquiera de los siguientes servicios de bases de datos de AWS compatibles con PostgreSQL con un tiempo de inactividad mínimo:

- Amazon Relational Database Service (Amazon RDS) para PostgreSQL
- Edición de Amazon Aurora compatible con PostgreSQL

La solución utiliza AWS Database Migration Service (AWS DMS) para migrar los datos, la Herramienta de conversión de esquemas de AWS (AWS SCT) para convertir el esquema de la base de datos y una base de datos de Oracle Bystander para ayudar a gestionar la migración. En esta implementación, el tiempo de inactividad se limita al tiempo necesario para crear o validar todas las claves externas de la base de datos.

La solución también utiliza instancias de Amazon Elastic Compute Cloud (Amazon EC2) con una base de datos de observadores de Oracle para ayudar a controlar el flujo de datos a través de AWS DMS. Puede pausar temporalmente la replicación en streaming desde la base de datos de Oracle en las instalaciones a Oracle Bystander para activar AWS DMS y ponerse al día con la validación de datos o para utilizar otra herramienta de validación de datos. La instancia de base de datos de Amazon RDS para PostgreSQL o la instancia de base de datos compatible con Aurora PostgreSQL y la base de datos de bystander tendrán los mismos datos cuando AWS DMS termine de migrar los cambios actuales.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de origen de Oracle en un centro de datos en las instalaciones con Active Data Guard configurado en modo de espera
- AWS Direct Connect, configurado entre el centro de datos en las instalaciones y AWS Secrets Manager para almacenar los secretos de la base de datos

- Controladores de conectividad de bases de datos Java (JDBC) para conectores SCT de AWS, instalados en una máquina local o en la instancia en la EC2 que está instalado AWS SCT
- Estar familiarizado con el Uso de una base de datos de Oracle como origen para AWS DMS
- Estar familiarizado con el uso de una base de datos de PostgreSQL como destino para AWS DMS

Limitaciones

- Límite de tamaño de la base de datos: 64 TB

Versiones de producto

- AWS DMS es compatible con todas las ediciones de bases de datos de Oracle para las versiones 10.2 y posteriores (para versiones 10.x), 11g y hasta 12.2, 18c y 19c. Para ver la lista actualizada de versiones compatibles, consulte Uso de una base de datos de Oracle como origen para AWS DMS. Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características. Para obtener información sobre las versiones de bases de datos de Oracle compatibles con AWS SCT, consulte la documentación de AWS SCT.
- AWS DMS es compatible con PostgreSQL versión 9.4 y posterior (para las versiones 9.x), 10.x, 11.x, 12.x y 13.x Para obtener más información, consulte Uso de una base de datos PostgreSQL como destino para AWS DMS en la documentación de AWS.

Arquitectura

Pila de tecnología de origen

- Una base de datos de Oracle en las instalaciones
- EC2 Instancia que aloja a un espectador de la base de datos de Oracle

Pila de tecnología de destino

- Instancia de Amazon RDS para PostgreSQL o Aurora PostgreSQL, PostgreSQL 9.3 y versiones posteriores

Arquitectura de destino

El siguiente diagrama muestra un ejemplo de flujo de trabajo para migrar una base de datos de Oracle a una base de datos de AWS compatible con PostgreSQL mediante AWS DMS y un bystander de Oracle:

Tools (Herramientas)

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- La Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado, lo que incluye las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.

Epics

Convertir el esquema de base de datos de Oracle a PostgreSQL

Tarea	Descripción	Habilidades requeridas
Configure AWS SCT.	Cree un informe nuevo y conéctese a Oracle como origen y a PostgreSQL como destino. En la Configuración del proyecto, vaya a la pestaña SQL Scripting. Cambie el Script SQL de destino a Varios archivos. Estos archivos se utilizarán más adelante y se denominarán de la siguiente manera: • create_database.sql • create_sequence.sql • create_table.sql	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	• create_view.sql • create_function.sql	
Convertir el esquema de base de datos de Oracle.	En la pestaña Acción, elija Generar informe. A continuación, elija Convertir esquema y seleccione Guardar como SQL.	Administrador de base de datos
Modifique los scripts.	Por ejemplo, es posible que desee modificar el script si un número del esquema de origen se ha convertido a formato numérico en PostgreSQL, pero prefiera utilizar BIGINT en su lugar para obtener un mejor rendimiento.	Administrador de base de datos

Creación y configuración de la instancia de base de datos de Amazon RDS

Tarea	Descripción	Habilidades requeridas
Creación de una instancia de base de datos de Amazon RDS	En la región de AWS correcta, cree una nueva instancia de base de datos de PostgreSQL. Para obtener más información, consulte Creación de una instancia de base de datos PostgreSQL y conexión a una base de datos en una instancia de base de datos PostgreSQL en la documentación de Amazon RDS.	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Configure las especificaciones de la instancia de base de datos.	Especifique la versión del motor de base de datos, la clase de instancia de base de datos, la implement ación Multi-AZ, el tipo de almacenamiento y el almacenamiento asignado. Introduzca el identificador de la instancia de base de datos, un nombre de usuario principal y una contraseña principal.	AWS SysAdmin, administrador de bases de datos
Configurar la red y la seguridad.	Especifique la nube privada virtual (VPC), el grupo de subredes, la accesibilidad pública, la preferencia de zona de disponibilidad y los grupos de seguridad.	DBA, SysAdmin
Configurar las opciones de la base de datos.	Especifique el nombre, el puerto, el grupo de parámetro s, el cifrado y la clave KMS.	AWS SysAdmin, administrador de bases de datos
Configure copias de seguridad .	Especifique el período de retención de la copia de seguridad, la ventana de copia de seguridad, la hora de inicio, la duración y si desea copiar las etiquetas a las instantán eas.	AWS SysAdmin, administrador de bases de datos
Configure las opciones de monitoreo.	Active o desactive los conocimientos mejorados de supervisión y rendimiento.	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Configurar las opciones de mantenimiento.	Especifique la actualización automática de versiones secundarias, el período de mantenimiento y el día, la hora y la duración de inicio.	AWS SysAdmin, administrador de bases de datos
Ejecute los scripts previos a la migración desde AWS SCT.	En la instancia de Amazon RDS, ejecute los siguientes scripts generados por AWS SCT: • create_database.sql • create_sequence.sql • create_table.sql • create_view.sql • create_function.sql	AWS SysAdmin, administrador de bases de datos

Configurar el Oracle bystander en Amazon EC2

Tarea	Descripción	Habilidades requeridas
Configura la red para Amazon EC2.	Creación de la nueva VPC, subredes, puerta de enlace de Internet, tablas de enrutamie nto y grupos de seguridad.	AWS SysAdmin
Crea la EC2 instancia.	En la región de AWS correspondiente, cree una nueva EC2 instancia . Seleccione la imagen de máquina de Amazon (AMI), elija el tamaño de la instancia y configure los detalles de la instancia: la cantidad de	AWS SysAdmin

Tarea	Descripción	Habilidades requeridas
	instancias (1), la VPC y la subred del paso anterior, la asignación automática de la IP pública y otras opciones. Agregue almacenamiento, configure grupos de seguridad y lance. Cuando se le pida, cree y guarde un par de claves para el siguiente paso.	
Conecte la base de datos de origen de Oracle a la EC2 instancia.	Copie la dirección IP IPv4 pública y el DNS en un archivo de texto y conéctese mediante SSH de la siguiente manera: ssh -i «your_file.pem» ec2-user@<your-IP - -DNS>. address-or-public	AWS SysAdmin
Configura el anfitrión inicial para un transeúnte en Amazon. EC2	Configure las claves SSH, el perfil bash, ORATAB y los enlaces simbólicos. Cree directorios Oracle.	AWS SysAdmin, administrador de Linux
Configurar la copia de la base de datos para un espectador en Amazon EC2	Utilice RMAN para crear una copia de la base de datos, habilitar el registro adicional y crear el archivo de control en espera. Una vez completada la copia, coloque la base de datos en modo de recuperac ión.	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Configurar Oracle Data Guard.	Modifique el archivo listener.ora e inicie el oyente. Configure un nuevo destino de archivo. Coloque al espectador en modo de recuperación, sustituya los archivos temporales para evitar futuros daños, instale un crontab si es necesario para evitar que el directorio de archivos se quede sin espacio y edite el manage-trclog-files-oraclearchivo.cfg para el archivo de origen y el modo de espera.	AWS SysAdmin, administrador de bases de datos
Prepare la base de datos de Oracle para sincronizar los envíos.	Añada los archivos de registro en espera y cambie el modo de recuperación. Cambie el envío de registros a SYNC AFFIRM tanto en la fuente principal como en la fuente en espera. Active los registros principales, confirme mediante el registro de alertas de Amazon EC2 Bystander que está utilizando los archivos de registro en espera y confirme que la retransmisión está fluyendo en SYNC.	AWS SysAdmin, administrador de bases de datos

Migre datos con AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación en AWS DMS.	Complete los campos para el nombre, la clase de instancia, la VPC (igual que la EC2 instancia de Amazon), la zona de disponibilidad múltiple y la accesibilidad pública. En Avanzado, especifique el almacenamiento asignado, el grupo de subredes, la zona de disponibilidad, los grupos de seguridad de VPC y la clave de AWS Key Management Service (AWS KMS).	AWS SysAdmin, administrador de bases de datos
Cree el punto de conexión de origen de la base de datos.	Especifique el nombre, el tipo, el motor de origen (Oracle), el nombre del servidor (nombre DNS EC2 privado de Amazon), el puerto, el modo SSL, el nombre de usuario, la contraseña, el SID, la VPC (especifique la VPC que tiene la instancia de replicación) y la instancia de replicación. Para probar la conexión, seleccione Ejecutar prueba y, a continuación, cree el punto de conexión. También puede configurar los siguientes ajustes avanzados: maxFileSizey numberDataType Scale.	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Conecte AWS DMS a Amazon RDS para PostgreSQL.	Cree un grupo de seguridad de migración para todas VPCs las conexiones.	AWS SysAdmin, administrador de bases de datos
Cree puntos de conexión de base de datos de destino.	Especifique el nombre del punto de conexión, el tipo, el motor de origen (PostgreSQL), el nombre del servidor (punto de conexión de Amazon RDS), el puerto, el modo SSL, el nombre de usuario, la contraseña, el nombre de la base de datos, la VPC (especifique la VPC que tiene la instancia de replicación) y la instancia de replicación. Para probar la conexión, seleccione Ejecutar prueba y, a continuac ión, cree el punto de conexión. También puede configurar los siguientes ajustes avanzados : maxFileSize y numberDat aTypeScale.	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Cree una tarea de replicación de AWS DMS.	Especifique el nombre de la tarea, la instancia de replicación, los puntos de conexión de origen y destino y la instancia de replicaci ón. Para tipo de migración, seleccione la opción Migrate existing data and replication ongoing changes (Migració n de los datos existentes y réplica de los cambios en curso). Desactive la casilla de verificación Iniciar la tarea al crearla.	AWS SysAdmin, administrador de bases de datos
Configure la configuración de la tarea de replicación de AWS DMS.	Para el modo de preparación de la tabla de destino, elija No hacer nada. Detenga la tarea cuando se complete la carga completa (para crear las claves principales). Especifiq ue el modo LOB limitado o completo y habilite las tablas de control. Si lo desea, puede configurar la configuración CommitRateavanzada.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Configure el mapeo de tablas.	En la sección Table mappings (Mapeo de tablas), cree una regla de Inclusión para todas las tablas de todos los esquemas incluidos en la migración y, a continuación, cree una regla de Exclusión . Agregue tres reglas de transformación para convertir los nombres del esquema, la tabla y las columnas a minúsculas y añada cualquier otra regla necesaria para esta migración específica.	Administrador de base de datos
Iniciar la tarea.	Iniciar la tarea de replicación. Asegúrese de que la carga completa está ejecutando. Ejecute ALTER SYSTEM SWITCH LOGFILE en la base de datos principal de Oracle para iniciar la tarea.	Administrador de base de datos
Ejecute los scripts de la migración intermedia desde AWS SCT.	En Amazon RDS para PostgreSQL, ejecute los siguientes scripts generados por AWS SCT: • create_index.sql • create_constraint.sql	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Reinicie la tarea para continuar con la captura de datos de cambio (CDC).	Ejecute VACUUM en la instancia de base de datos Amazon RDS para PostgreSQL y reinicie la tarea de AWS DMS para aplicar los cambios de CDC en caché.	Administrador de base de datos

Realizar la transición a la base de datos de PostgreSQL

Tarea	Descripción	Habilidades requeridas
Revise los registros y las tablas de validación de AWS DMS para ver si hay algún error.	Compruebe y corrija cualquier error de replicación o validación.	Administrador de base de datos
Detenga todas las dependencias de Oracle.	Detenga todas las dependencias de Oracle, cierre los oyentes de la base de datos de Oracle y ejecute ALTER SYSTEM SWITCH LOGFILE. Detenga la tarea de AWS DMS cuando no muestre actividad.	Administrador de base de datos
Ejecute los scripts posteriores a la migración desde AWS SCT.	En Amazon RDS para PostgreSQL, ejecute los siguientes scripts generados por AWS SCT: • create_foreign_key_constraint.sql • create_triggers.sql	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Complete los pasos adicionales de Amazon RDS para PostgreSQL.	Aumente las secuencias para que coincidan con las de Oracle si es necesario, ejecute VACUUM y ANALYZE y tome una instantánea para comprobar la conformidad.	Administrador de base de datos
Abra las conexiones hacia Amazon RDS para PostgreSQL.	Elimine los grupos de seguridad de AWS DMS de Amazon RDS para PostgreSQL, añada grupos de seguridad de producción y dirija sus aplicaciones a la nueva base de datos.	Administrador de base de datos
Limpie los objetos de AWS DMS.	Elimine los puntos finales, las tareas de replicación, las instancias de replicación y la EC2 instancia.	SysAdmin, DBA

Recursos relacionados

- Documentación de AWS DMS
- Documentación de AWS SCT
- Precio de Amazon RDS para PostgreSQL

Migración de una base de datos de Oracle a Amazon Redshift con AWS DMS y AWS SCT

Piyush Goyal y Brian Motzer, Amazon Web Services

Resumen

Este patrón proporciona orientación para migrar las bases de datos de Oracle a un data warehouse en la nube de Amazon Redshift en la nube de Amazon Web Services (AWS) mediante AWS Database Migration Service (AWS DMS) y la Herramienta de conversión de esquemas de AWS (AWS SCT). El patrón cubre las bases de datos Oracle de origen que están en las instalaciones o instaladas en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). También incluye Amazon Relational Database Service (Amazon RDS) para bases de datos de Oracle.

Requisitos previos y limitaciones

Requisitos previos

- Una base de datos de Oracle que se ejecuta en un centro de datos en las instalaciones o en la nube de AWS
- Una cuenta de AWS activa
- Estar familiarizado con el uso de una base de datos de Oracle como origen para AWS DMS
- Familiaridad con el uso de una base de datos Amazon Redshift como objetivo para AWS DMS
- Conocimiento de Amazon RDS, Amazon Redshift, las tecnologías de bases de datos aplicables y SQL
- Controladores de conectividad de bases de datos Java (JDBC) para conectores de AWS SCT, donde está instalado AWS SCT

Versiones de producto

- Para las bases de datos de Oracle autogestionadas, AWS DMS admite todas las ediciones de bases de datos de Oracle para las versiones 10.2 y posteriores (para las versiones 10.x), 11g y hasta 12.2, 18c y 19c. En el caso de las bases de datos de Amazon RDS para Oracle que administra AWS, AWS DMS admite todas las ediciones de bases de datos de Oracle para las versiones 11g (versiones 11.2.0.4 y posteriores) y hasta 12.2, 18c y 19c. Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características.

Arquitectura

Pila de tecnología de origen

Uno de los siguientes:

- Una base de datos de Oracle en las instalaciones
- Una base de datos de Oracle en una EC2 instancia
- Una instancia de base de datos de Amazon RDS para Oracle

Pila de tecnología de destino

- Amazon Redshift

Arquitectura de destino

De una base de datos de Oracle que se ejecuta en la nube de AWS a Amazon Redshift:

Desde una base de datos de Oracle que se ejecuta en un centro de datos interno hasta Amazon Redshift:

Tools (Herramientas)

- AWS DMS: AWS Database Migration Service (AWS DMS) le ayuda a migrar bases de datos a AWS de forma rápida y segura. La base de datos de origen permanece totalmente operativa durante la migración, minimizando así el tiempo de inactividad de las aplicaciones que dependen de ella. AWS DMS puede migrar sus datos desde y hasta las bases de datos comerciales y de código abierto más usadas.
- AWS SCT: la herramienta de conversión de esquemas de AWS (AWS SCT) puede utilizarse para convertir su esquema de base de datos existente de un motor de base de datos a otro. Es compatible con varios motores de bases de datos, incluidos Oracle, SQL Server y PostgresSQL, como orígenes.

Epics

Preparación para la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos.	Valide las versiones de las bases de datos de origen y destino y asegúrese de que son compatibles con AWS DMS. Para información sobre las versiones de bases de datos de Oracle compatibles, consulte Uso de una base de datos de Oracle como fuente para AWS DMS. Para obtener información acerca del uso de Amazon Redshift como destino, consulte Uso de una base de datos de Amazon Redshift como destino de AWS DMS.	Administrador de base de datos
Crear una VPC y un grupo de seguridad.	En su cuenta de AWS, cree una nube privada virtual (VPC), si no existe. Cree un grupo de seguridad para el tráfico saliente para las bases de datos de origen y destino. Para más informaci ón, consulte la documenta ción de Amazon Virtual Private Cloud (Amazon VPC).	Administrador de sistemas
Instale AWS SCT.	Descargue e instale la versión más reciente de AWS SCT y sus controladores correspon dientes. Para más informaci	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	ón, consulte Instalación, verificación y actualización de AWS SCT.	
Cree un usuario para la tarea de AWS DMS.	Cree un usuario de AWS DMS en la base de datos de origen y concédale privilegios de LECTURA. AWS SCT y AWS DMS utilizarán este usuario.	Administrador de base de datos
Pruebe la conectividad de la base de datos.	Probar la conectividad con la instancia de base de datos de Oracle.	Administrador de base de datos
Cree un proyecto nuevo en AWS SCT.	Abra la herramienta AWS SCT y cree un proyecto nuevo.	Administrador de base de datos
Analice el esquema de Oracle que se va a migrar.	Utilice AWS SCT para analizar el esquema que se va a migrar y generar un informe de evaluación de la migración de la base de datos. Para obtener más información, consulte Creación de un informe de evaluación de la migración de bases de datos en la documentación de AWS SCT.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Revise el informe de evaluación.	Revise el informe para comprobar la viabilidad de la migración. Es posible que algunos objetos de base de datos requieran una conversión manual. Para más información sobre el informe, consulte Ver el informe de evaluación en la documentación de AWS SCT.	Administrador de base de datos

Prepare la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Crear un clúster de Amazon Redshift.	Cree un clúster de Amazon Redshift en la VPC que creó anteriormente. Para obtener más información, consulte Clústeres de Amazon Redshift en la documentación de Amazon Redshift.	Administrador de base de datos
Cree usuarios de bases de datos.	Extraiga la lista de usuarios, roles y concesiones de la base de datos de origen de Oracle. Cree usuarios en la base de datos Amazon Redshift de destino y aplique las funciones del paso anterior.	Administrador de base de datos
Evaluar los parámetros de la base de datos.	Revise las opciones, los parámetros, los archivos de red y los enlaces a las bases de datos de la base de datos	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de origen de Oracle y evalúe su aplicabilidad al destino.	
Aplique cualquier configuración pertinente a la base de datos de destino.	Para obtener más información acerca de este paso, consulte Referencia de configuración en la documentación de Amazon Redshift.	Administrador de base de datos

Crear usuarios en la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Cree un usuario de AWS DMS en la base de datos de destino.	Cree un usuario de AWS DMS en la base de datos de destino y concédale privilegios de lectura y escritura. Valide la conectividad desde AWS SCT.	Administrador de base de datos
Convierta el esquema, revise el informe SQL y guarde los errores o advertencias.	Para obtener más información, consulte Convertir esquemas de bases de datos mediante AWS SCT en la documentación de AWS SCT.	Administrador de base de datos
Aplique los cambios de esquema a la base de datos de destino o guárdelos como un archivo .sql.	Para obtener instrucciones, consulte Guardar y aplicar el esquema convertido en AWS SCT en la documentación de AWS SCT.	Administrador de base de datos
Valide los objetos de la base de datos de destino.	Valide los objetos que se crearon en el paso anterior en la base de datos de destino.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Reescriba o rediseñe los objetos que no se hayan convertido correctamente.	
Deshabilite las claves y los desencadenadores externos.	Deshabilite cualquier clave y desencadenador externo. Esto puede provocar problemas de carga de datos durante el proceso de carga completa cuando se ejecuta AWS DMS.	Administrador de base de datos

Migración de datos utilizando AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación de AWS DMS.	Inicie sesión en la Consola de administración de AWS y abra la consola de AWS DMS. En el panel de navegación, seleccione Instancias de replicación y Crear instancia de replicación. Para obtener instrucciones detalladas, consulte el paso 1 de la Introducción a AWS DMS en la documentación de AWS DMS.	Administrador de base de datos
Cree puntos de conexión de origen y destino.	Cree puntos de conexión de origen y destino, pruebe la conexión desde la instancia de replicación a los puntos de conexión de origen y destino. Para obtener instrucciones detalladas, consulte el paso	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	2 de la Introducción a AWS DMS en la documentación de AWS DMS.	
Cree una tarea de replicación.	Cree una tarea de replicación y seleccione el método de migración adecuado. Para obtener instrucciones detalladas, consulte el paso 3 de la Introducción a AWS DMS en la documentación de AWS DMS.	Administrador de base de datos
Iniciar la tarea de replicación.	Inicie la tarea de replicación y supervise los registros para detectar cualquier error.	Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Cree servidores de aplicaciones.	Cree los nuevos servidores de aplicaciones en AWS.	Propietario de la aplicación
Migre el código de la aplicación.	Migre el código de la aplicación a los nuevos servidores.	Propietario de la aplicación
Configure los servidores de aplicaciones.	Configure el servidor de aplicaciones para los controladores y la base de datos de destino.	Propietario de la aplicación
Optimice el código de la aplicación.	Optimice el código de la aplicación para la base de datos de destino.	Propietario de la aplicación

Realizar la transición a la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Valide a los usuarios.	En la base de datos de Amazon Redshift de destino, valide a los usuarios y asígneles funciones y privilegios.	Administrador de base de datos
Valide que la aplicación esté bloqueada.	Asegúrese de que la aplicación esté bloqueada para evitar más cambios.	Propietario de la aplicación
Valide los datos.	Valide los datos de la base de datos Amazon Redshift de destino.	Administrador de base de datos
Habilite las claves y los desencadenadores externos.	Habilite las claves y los desencadenadores externos en la base de datos de Amazon Redshift de destino.	Administrador de base de datos
Conéctese a la nueva base de datos.	Configure la aplicación para conectarse a la nueva base de datos de Amazon Redshift.	Propietario de la aplicación
Realice las comprobaciones finales.	Realice una comprobación final y exhaustiva del sistema antes de la puesta en marcha.	Administrador de base de datos, propietario de la aplicación
Realice la puesta en marcha.	Póngalo en marcha con la base de datos de Amazon Redshift de destino.	Administrador de base de datos

Cerrar el proyecto de migración

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.	Cierre los recursos temporales de AWS, como la instancia de replicación de AWS DMS y la EC2 instancia utilizada para AWS SCT.	Administrador de base de datos, administrador de sistemas
Revise los documentos.	Revise y valide los documentos del proyecto de migración.	Administrador de base de datos, administrador de sistemas
Recopile métricas.	Recopile información sobre el proyecto de migración, como el tiempo de migración, el porcentaje de tareas manuales en comparación con las tareas automatizadas y el ahorro total de costos.	Administrador de base de datos, administrador de sistemas
Cerrar el proyecto.	Cerrar el proyecto y enviar comentarios.	Administrador de base de datos, administrador de sistemas

Recursos relacionados

Referencias

- Guía del usuario de AWS DMS
- Guía del usuario de AWS SCT
- Guía de introducción a Amazon Redshift

Tutoriales y videos

- Conozca en profundidad AWS SCT y AWS DMS (presentación de AWS re:Invent 2019)

- Introducción a AWS Database Migration Service (AWS DMS)

Migración de una base de datos de Oracle a Aurora PostgreSQL con AWS DMS y AWS SCT

Senthil Ramasamy, Amazon Web Services

Resumen

Este patrón describe cómo migrar una base de datos de Oracle a una edición compatible con PostgreSQL de Amazon Aurora mediante AWS Data Migration Service (AWS DMS) y la la Herramienta de conversión de esquemas de AWS (AWS SCT).

El patrón abarca las bases de datos Oracle de origen que se encuentran en las instalaciones, las bases de datos Oracle que están instaladas en instancias de Amazon Elastic Compute Cloud (Amazon EC2) y Amazon Relational Database Service (Amazon RDS) para las bases de datos de Oracle. El patrón convierte estas bases de datos en compatibles con Aurora PostgreSQL.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una base de datos de Oracle en un centro de datos en las instalaciones o en la nube de AWS.
- Los clientes de SQL se instalan en una máquina local o en una EC2 instancia.
- Controladores de conectividad de bases de datos Java (JDBC) para conectores SCT de AWS, instalados en una máquina local o en una instancia en la EC2 que esté instalado AWS SCT.

Limitaciones

- Límite de tamaño de la base de datos: 128 TB
- Si la base de datos de origen es compatible con una aplicación comercial off-the-shelf (COTS) o es específica de un proveedor, es posible que no pueda convertirla a otro motor de base de datos. Antes de usar este patrón, confirme que la aplicación es compatible con Aurora PostgreSQL.

Versiones de producto

- Para las bases de datos de Oracle autogestionadas, AWS DMS admite todas las ediciones de bases de datos de Oracle para las versiones 10.2 y posteriores (para las versiones 10.x), 11g y hasta 12.2, 18c y 19c. Para ver la lista más reciente de las versiones de las bases de datos

de Oracle compatibles (tanto autogestionadas como de Amazon RDS para Oracle), consulte Uso de una base de datos de Oracle como fuente para AWS DMS y Uso de una base de datos PostgreSQL como destino para AWS DMS.

- Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características. Para obtener información sobre las versiones de bases de datos de Oracle compatibles con AWS SCT, consulte la documentación de AWS SCT.
- Aurora es compatible con las versiones de PostgreSQL incluidas en las versiones de Amazon Aurora PostgreSQL y versiones del motor.

Arquitectura

Pila de tecnología de origen

Uno de los siguientes:

- Una base de datos de Oracle en las instalaciones
- Una base de datos Oracle en una instancia EC2
- Una instancia de base de datos de Amazon RDS para Oracle

Pila de tecnología de destino

- Aurora compatible con PostgreSQL

Arquitectura de destino

Arquitectura de migración de datos

- Desde una base de datos de Oracle en ejecución en la nube de AWS

- Desde una base de datos de Oracle en ejecución en un centro de datos en las instalaciones

Tools (Herramientas)

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado a un formato compatible con la base de datos de destino.

Epics

Preparación para la migración

Tarea	Descripción	Habilidades requeridas
Prepare la base de datos de origen.	Para preparar la base de datos de origen, consulte Uso de Oracle Database como un origen para AWS SCT en la documentación de AWS SCT.	Administrador de base de datos
Cree una EC2 instancia para AWS SCT.	Cree y configure una EC2 instancia para AWS SCT, si es necesario.	Administrador de base de datos
Descargue AWS SCT.	Descargue la versión más reciente de AWS SCT y los controladores asociados. Para obtener más información, consulte Instalación, verificación y actualización de AWS SCT en la documentación de AWS SCT.	Administrador de base de datos
Añada usuarios y permisos.	Agregue y valide los usuarios y permisos necesarios en la base de datos de origen.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree un proyecto de AWS SCT.	Cree un proyecto de AWS SCT para la carga de trabajo y conéctese a la base de datos de origen. Para obtener instrucciones, consulte Creación de un proyecto de AWS SCT y Cómo añadir servidores de bases de datos en la documentación de AWS SCT.	Administrador de base de datos
Evalúe la viabilidad.	Genere un informe de evaluación que resuma las medidas a tomar en el caso de los esquemas que no se pueden convertir automátic amente y proporcione estimaciones de los esfuerzos de conversión manual. Para obtener más información, consulte Creación y revisión del informe de evaluación de la migración de bases de datos en la documentación de AWS SCT.	Administrador de base de datos

Prepare la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Crear una instancia de base de datos de Amazon RDS de destino.	Cree una instancia de base de datos de Amazon RDS de destino con Amazon Aurora como motor de base de datos.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS en la documentación de Amazon RDS.	
Extraiga usuarios, roles y permisos.	Extraiga la lista de usuarios, roles y permisos de la base de datos de origen.	Administrador de base de datos
Asigne usuarios.	Asigne los usuarios existentes de la base de datos a los nuevos usuarios de la base de datos.	Propietario de la aplicación
Cree usuarios.	Cree usuarios en la base de datos de destino.	Administrador de base de datos, propietario de la aplicación
Aplique roles.	Aplique los roles del paso anterior a la base de datos de destino.	Administrador de base de datos
Compruebe las opciones, los parámetros, los archivos de red y los enlaces a las bases de datos.	Revise la base de datos de origen para ver las opciones, los parámetros, los archivos de red y los enlaces a la base de datos y, a continuación, evalúe su aplicabilidad a la base de datos de destino.	Administrador de base de datos
Aplique la configuración.	Aplique cualquier configuración relevante a la base de datos de destino.	Administrador de base de datos

Transferir objetos

Tarea	Descripción	Habilidades requeridas
Configure la conectividad de AWS SCT.	Configure la conectividad de AWS SCT con la base de datos de destino.	Administrador de base de datos
Convierta el esquema con AWS SCT.	AWS SCT convierte automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado a un formato compatible con la base de datos de destino. El código que la herramienta no puede convertir automáticamente está marcado de forma clara para que pueda convertirlo manualmente.	Administrador de base de datos
Revise el informe.	Revise el informe SQL generado y guarde los errores y advertencias.	Administrador de base de datos
Aplique cambios de esquema automatizados.	Aplique los cambios de esquema automatizados a la base de datos de destino o guárdelos como un archivo .sql.	Administrador de base de datos
Valide objetos.	Valide que AWS SCT haya creado los objetos en el destino.	Administrador de base de datos
Gestione los elementos que no se hayan convertido.	Reescriba, rechace o rediseñe manualmente cualquier elemento que no se haya	Administrador de base de datos, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	podido convertir automátic amente.	
Aplique permisos de usuario y rol.	Aplique los permisos de usuario y rol generados, y revise las excepciones.	Administrador de base de datos

Migración de datos

Tarea	Descripción	Habilidades requeridas
Determine el método.	Determine el método para migrar los datos.	Administrador de base de datos
Cree una instancia de replicaci ón.	Cree una instancia de replicaci ón desde la consola de AWS DMS. Para obtener más información, consulte Cómo trabajar con una instancia de replicación de AWS DMS en la documentación de AWS DMS.	Administrador de base de datos
Cree los puntos de conexión de origen y de destino.	Para crear puntos de conexión, siga las instrucci ones de Creación de puntos de conexión de origen y destino en la documentación de AWS DMS.	Administrador de base de datos
Cree una tarea de replicación.	Para crear una tarea, consulte Trabajar con tareas de AWS DMS en la documentación de AWS DMS.	Administrador de base de datos
Inicie la tarea de replicación y supervise los registros.	Para obtener más informaci ón sobre este paso, consulte	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Monitorización de las tareas de AWS DMS en la documentación de AWS DMS.	

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Analice y convierta los elementos SQL en el código de la aplicación.	Use AWS SCT para analizar y convertir los elementos de SQL en el código de la aplicación. Al convertir su esquema de base de datos de un motor a otro, también deberá actualizar el código SQL de las aplicaciones para interactuar con el nuevo motor de base de datos en lugar del antiguo. Puede ver, analizar, editar y guardar el código SQL convertido.	Propietario de la aplicación
Cree servidores de aplicaciones.	Cree los nuevos servidores de aplicaciones en AWS.	Propietario de la aplicación
Migre el código de la aplicación.	Migre el código de la aplicación a los nuevos servidores.	Propietario de la aplicación
Configure los servidores de aplicaciones.	Configure los servidores de aplicaciones para los controladores y la base de datos de destino.	Propietario de la aplicación
Corrija el código.	Corrija cualquier código específico del motor de base	Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	de datos de origen de su aplicación.	
Optimice el código.	Optimice el código de su aplicación para el motor de base de datos de destino.	Propietario de la aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Realizar la transición a la base de datos de destino.	Realice la transición a la nueva base de datos.	Administrador de base de datos
Bloquee la aplicación.	Bloquee la aplicación frente a cualquier cambio.	Propietario de la aplicación
Valide los cambios.	Valide que todos los cambios se hayan propagado a la base de datos de destino.	Administrador de base de datos
Redirigir a la base de datos de destino.	Apunte los nuevos servidores de la aplicación hacia la base de datos de destino.	Propietario de la aplicación
Compruebe todo.	Realice una verificación final y exhaustiva del sistema.	Propietario de la aplicación
Realice la puesta en marcha	Complete las tareas finales de la transición.	Propietario de la aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.	Cierre los recursos temporales de AWS, como la instancia de replicación de AWS DMS y la EC2 instancia utilizada para AWS SCT.	Administrador de base de datos, propietario de la aplicación
Actualice los comentarios.	Actualice los comentarios sobre el proceso de AWS DMS para los equipos internos.	Administrador de base de datos, propietario de la aplicación
Revise el proceso y las plantillas.	Revise el proceso de AWS DMS y mejore la plantilla si es necesario.	Administrador de base de datos, propietario de la aplicación
Valide los documentos.	Revise y valide los documentos del proyecto.	Administrador de base de datos, propietario de la aplicación
Recopile métricas.	Recopile métricas para evaluar el tiempo de migración, el porcentaje de esfuerzo manual en comparación con el automatizado, el ahorro de costos, etc.	Administrador de base de datos, propietario de la aplicación
Cierre el proyecto.	Cierre el proyecto de migración y envíe comentarios a las partes interesadas.	Administrador de base de datos, propietario de la aplicación

Recursos relacionados

Referencias

- Uso de una base de datos de Oracle como origen para AWS DMS
- Utilizar una base de datos PostgreSQL como objetivo para el servicio de migración de bases de datos de AWS
- Manual de migración de Oracle Database 11g/12c a Amazon Aurora con compatibilidad con PostgreSQL (9.6.x)
- Manual de migración de la base de datos de Oracle 19c a Amazon Aurora con compatibilidad con PostgreSQL (12.4)
- Migración de una base de datos de Amazon RDS para Oracle a una edición compatible con Amazon Aurora PostgreSQL
- AWS Data Migration Service
- Herramienta de conversión de esquemas de AWS
- Migración de Oracle a Amazon Aurora
- Precios de Amazon RDS

Tutoriales y videos

- Tutoriales sobre la migración de bases de datos Step-by-Step
- Introducción a AWS DMS
- Introducción a Amazon RDS
- AWS Data Migration Service (video)
- Migración de una base de datos de Oracle a PostgreSQL (video)

Información adicional

.

Migración de datos de una base de datos de Oracle en las instalaciones a Aurora PostgreSQL

Michelle Deng y Shunan Xiang, Amazon Web Services

Resumen

Este patrón proporciona orientación para la migración de datos de una base de datos de Oracle en las instalaciones a una edición de Amazon Aurora compatible con PostgreSQL. Se basa en una estrategia de migración de datos en línea con un tiempo de inactividad mínimo para bases de datos de Oracle de varios terabytes que contienen tablas grandes con un alto nivel de actividad de lenguaje de manipulación de datos (DML). Emplea una base de datos en espera de Oracle Active Data Guard como fuente para reducir la migración de datos de la base de datos principal. La replicación de la base de datos principal de Oracle a la base de datos en espera se puede suspender durante la carga completa para evitar errores ORA-01555.

Las columnas de la tabla en claves principales (PKs) o claves externas (FKs), con el tipo de datos NUMBER, se utilizan normalmente para almacenar números enteros en Oracle. Le recomendamos que los convierta a INT o BIGINT en PostgreSQL para obtener un mejor rendimiento. Puede usar la Herramienta de conversión de esquemas de AWS (AWS SCT) para cambiar la asignación de tipos de datos por defecto en las columnas PK y FK. (Para obtener más información, consulte la entrada del AWS blog Convertir el tipo de datos NUMBER de Oracle a PostgreSQL). La migración de datos de este patrón usa AWS Database Migration Service (AWS DMS) tanto para la captura de datos a carga completa como para la captura de datos de cambios (CDC).

También puede usar este patrón para migrar una base de datos Oracle local a Amazon Relational Database Service (Amazon RDS) para PostgreSQL, o una base de datos Oracle alojada en Amazon Elastic Compute Cloud (Amazon) a EC2 Amazon RDS para PostgreSQL o compatible con Aurora PostgreSQL.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de origen de Oracle en un centro de datos en las instalaciones con Active Data Guard configurado en modo de espera
- AWS Direct Connect, configurado entre el centro de datos en las instalaciones y la nube de AWS

- Estar familiarizado con el uso de una base de datos de Oracle como origen para AWS DMS
- Estar familiarizado con el uso de una base de datos de PostgreSQL como destino para AWS DMS

Limitaciones

- Los clústeres de bases de datos de Amazon Aurora se pueden crear con hasta 128 TiB de almacenamiento. Las instancias de bases de datos de Amazon RDS para PostgreSQL se pueden crear con hasta 64 TiB de almacenamiento. Para obtener la información de almacenamiento más reciente, consulte Almacenamiento y fiabilidad de Amazon Aurora y Almacenamiento de instancias de base de datos de Amazon RDS en la documentación de AWS.

Versiones de producto

- AWS DMS es compatible con todas las ediciones de bases de datos de Oracle para las versiones 10.2 y posteriores (para versiones 10.x), 11g y hasta 12.2, 18c y 19c. Para ver la lista actualizada de versiones compatibles, consulte Uso de una base de datos de Oracle como origen para AWS DMS en la documentación de AWS.

Arquitectura

Pila de tecnología de origen

- Bases de datos de Oracle en las instalaciones con Oracle Active Data Guard standby configurado

Pila de tecnología de destino

- Aurora compatible con PostgreSQL

Arquitectura de migración de datos

Tools (Herramientas)

- AWS DMS: AWS Database Migration Service (AWS DMS) admite varias bases de datos de origen y destino. Consulte Uso de una base de datos de Oracle como fuente para AWS DMS, en la documentación de AWS DMS, para obtener una lista de las versiones y ediciones de bases de datos de origen y destino de Oracle compatibles. Si AWS DMS no admite la base de datos de

origen, debe seleccionar otro método para migrar los datos en la fase 6 (en la sección Epics). Nota importante: dado que se trata de una migración heterogénea, primero debe comprobar si la base de datos admite una aplicación comercial off-the-shelf (COTS). Si la aplicación es COTS, consulte al proveedor para confirmar que es compatible con Aurora PostgreSQL antes de continuar. Para obtener más información, consulte los tutoriales de Step-by-Step migración a AWS DMS en la documentación de AWS.

- AWS SCT: la Herramienta de conversión de esquemas de AWS (AWS SCT) facilita las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado a un formato compatible con la base de datos de destino. El código personalizado que convierte la herramienta incluye vistas, procedimientos almacenados y funciones. Cualquier código que la herramienta no pueda convertir automáticamente está claramente marcado para que pueda convertirlo usted mismo.

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.		Administrador de base de datos
Instale AWS SCT y los controladores.		Administrador de base de datos
Agregue y valide la base de datos de origen de concesion es y usuarios de requisitos previos de AWS SCT.		Administrador de base de datos
Cree un proyecto de AWS SCT para la carga de trabajo y conéctese a la base de datos de origen.		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Genere un informe de evaluación y evalúe la viabilidad.		Administrador de base de datos, propietario de la aplicación

Prepare la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Cree una base de datos de destino de Aurora compatible con PostgreSQL.		Administrador de base de datos
Extraiga la lista de concesiones, usuarios y roles de la base de datos de origen.		Administrador de base de datos
Asigne los usuarios existentes de la base de datos a los nuevos usuarios de la base de datos.		Propietario de la aplicación
Cree usuarios en la base de datos de destino.		Administrador de base de datos
Aplique los roles del paso anterior a la base de datos de Aurora compatible con PostgreSQL de destino.		Administrador de base de datos
Revise las opciones, los parámetros, los archivos de red y los enlaces de la base de datos de origen, y evalúe su aplicabilidad a la base de datos de destino.		Administrador de base de datos, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Aplique cualquier configura ción relevante a la base de datos de destino.		Administrador de base de datos

Prepare para la conversión del código de objetos de la base de datos

Tarea	Descripción	Habilidades requeridas
Configure la conectividad de AWS SCT con la base de datos de destino.		Administrador de base de datos
Convierta el esquema en AWS SCT y guarde el código convertido como archivo .sql.		Administrador de base de datos, propietario de la aplicación
Convierta manualmente cualquier objeto de base de datos que no se haya podido convertir automáticamente.		Administrador de base de datos, propietario de la aplicación
Optimice la conversión del código de la base de datos.		Administrador de base de datos, propietario de la aplicación
Divida el archivo .sql en varios archivos .sql según el tipo de objeto.		Administrador de base de datos, propietario de la aplicación
Valide los scripts SQL en la base de datos de destino.		Administrador de base de datos, propietario de la aplicación

Prepárese para la migración de datos

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación de AWS DMS.		Administrador de base de datos
Cree los puntos de conexión de origen y de destino.	Si el tipo de datos de PKs and FKs se convierte de NUMBER en Oracle a BIGINT en PostgreSQL, considere la posibilidad de especificar el atributo `numberDataTypeScale=-2` de conexión al crear el punto final de origen.	Administrador de base de datos

Migración de datos: carga completa

Tarea	Descripción	Habilidades requeridas
Cree el esquema y las tablas en la base de datos de destino.		Administrador de base de datos
Cree tareas de carga completa de AWS DMS agrupando tablas o dividiendo una tabla grande en función de su tamaño.		Administrador de base de datos
Detenga las aplicaciones en las bases de datos de Oracle de origen durante un breve período.		Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Compruebe que la base de datos en espera de Oracle esté sincronizada con la base de datos principal y detenga la replicación de la base de datos principal a la base de datos en espera.		Administrador de base de datos, propietario de la aplicación
Inicie las aplicaciones en la base de datos de Oracle de origen.		Propietario de la aplicación
Inicie las tareas de carga completa de AWS DMS en paralelo desde la base de datos en espera de Oracle hasta la base de datos de Aurora compatible con PostgreSQL.		Administrador de base de datos
Cree PKs índices secundarios una vez completada la carga completa.		Administrador de base de datos
Valide los datos.		Administrador de base de datos

Migración de datos: CDC

Tarea	Descripción	Habilidades requeridas
Cree tareas de replicación continua de AWS DMS especificando la hora de inicio de CDC o el número		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
de cambio de sistema (SCN) personalizados cuando el modo de espera de Oracle se sincronizó con la base de datos principal y antes de que se reiniciaran las aplicaciones en la tarea anterior.		
Inicie las tareas de AWS DMS en paralelo para replicar los cambios en curso de la base de datos en espera Oracle a la base de datos Aurora compatible con PostgreSQL.		Administrador de base de datos
Restablezca la replicación de la base de datos principal de Oracle a la base de datos en espera.		Administrador de base de datos
Supervise los registros y detenga las aplicaciones en la base de datos de Oracle cuando la base de datos de destino de Aurora compatibl e con PostgreSQL esté casi sincronizada con la base de datos de Oracle de origen.		Administrador de base de datos, propietario de la aplicación
Detenga las tareas de AWS DMS cuando el destino esté completamente sincroniz ado con la base de datos de Oracle de origen.		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree FKs y valide los datos en la base de datos de destino.		Administrador de base de datos
Cree funciones, vistas, desencadenantes, secuencias y otros tipos de objetos en la base de datos de destino.		Administrador de base de datos
Aplique las concesiones de funciones en la base de datos de destino.		Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Use AWS SCT para analizar y convertir las instrucciones SQL del código de la aplicación.		Propietario de la aplicación
Cree nuevos servidores de aplicaciones en AWS.		Propietario de la aplicación
Migre el código de la aplicación a los nuevos servidores.		Propietario de la aplicación
Configure el servidor de aplicaciones para los controladores y la base de datos de destino.		Propietario de la aplicación
Corrija cualquier código específico del motor de base		Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
de datos de origen de la aplicación.		
Optimice el código de la aplicación para la base de datos de destino.		Propietario de la aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Apunte el nuevo servidor de la aplicación hacia la base de datos de destino.		Administrador de base de datos, propietario de la aplicación
Realice comprobaciones de estado.		Administrador de base de datos, propietario de la aplicación
Realice la puesta en marcha.		Administrador de base de datos, propietario de la aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.		Administrador de base de datos, administrador de sistemas
Revise y valide los documentos del proyecto.		Administrador de base de datos, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Recopile métricas sobre el tiempo necesario para migrar, el porcentaje de uso manual en comparación con el uso de herramientas, el ahorro de costos y datos similares.		Administrador de base de datos, propietario de la aplicación
Cerrar el proyecto y enviar comentarios.		Administrador de base de datos, propietario de la aplicación

Recursos relacionados

Referencias

- Base de datos de Oracle a Aurora compatible con PostgreSQL: manual de procedimientos para la migración
- Migración de una base de datos de Amazon RDS para Oracle a Amazon Aurora MySQL
- Sitio web de AWS DMS
- Documentación de AWS DMS
- Sitio web de AWS SCT
- Documentación de AWS SCT
- Migración de Oracle a Amazon Aurora

Tutoriales

- Introducción a AWS DMS
- Introducción a Amazon RDS
- Step-by-StepTutoriales de AWS Database Migration Service

Migración de SAP ASE a Amazon RDS para SQL Server utilizando AWS DMS

Amit Kumar, Amazon Web Services

Resumen

Este patrón proporciona orientación para migrar una base de datos de SAP Adaptive Server Enterprise (ASE) a una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) que ejecute Microsoft SQL Server. La base de datos de origen puede estar ubicada en un centro de datos local o en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). El patrón utiliza AWS Database Migration Service (AWS DMS) para migrar datos y (de forma opcional) herramientas de ingeniería de software asistida por computadora (CASE) para convertir el esquema de base de datos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos SAP ASE en un centro de datos local o en una instancia EC2
- Una base de datos de Amazon RDS para SQL Server de destino que esté en funcionamiento

Limitaciones

- Límite de tamaño de la base de datos: 64 TB

Versiones de producto

- Solo para SAP ASE, versión 15.7 o 16.x. Para obtener la información más reciente, consulte Uso de una base de datos de SAP como origen para AWS DMS.
- Para las bases de datos de destino de Amazon RDS, AWS DMS admite las versiones de Microsoft SQL Server en Amazon RDS para las ediciones Enterprise, Standard, Web y Express. Para obtener la información más reciente sobre las versiones compatibles, consulte la documentación de AWS DMS. Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características.

Arquitectura

Pila de tecnología de origen

- Una base de datos SAP ASE que se encuentra en las instalaciones o en una EC2 instancia de Amazon

Pila de tecnología de destino

- Instancia de base de datos de Amazon RDS para SQL Server

Arquitectura de origen y destino

Desde una base de datos SAP ASE en Amazon EC2 hasta una instancia de base de datos de Amazon RDS for SQL Server:

De una base de datos SAP ASE en las instalaciones a una instancia de base de datos de Amazon RDS para SQL Server:

Tools (Herramientas)

- AWS Database Migration Service (AWS DMS) es un servicio web que puede utilizar para migrar datos de una base de datos local, de una instancia de base de datos de Amazon RDS o de una base de datos de una EC2 instancia a una base de datos de un servicio de AWS, como Amazon RDS for SQL Server, o una instancia. EC2 Puede también migrar desde una base de datos de un servicio de AWS a otra base de datos local. Puede migrar datos entre motores de bases de datos heterogéneos u homogéneos.
- Para las conversiones de esquemas, si lo desea, puede utilizar Erwin Data Modeler o SAP. PowerDesigner

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Identifique los requisitos de almacenamiento (el tipo y la capacidad de almacenam iento).		DBA, SysAdmin
Elija el tipo de instancia adecuado en función de la capacidad, las características de almacenamiento y las características de red.		DBA, SysAdmin
Identifique los requisitos de seguridad de acceso a la red para las bases de datos de origen y destino.		DBA, SysAdmin
Identificar la estrategia de migración de aplicaciones.		DBA, propietario de la SysAdmin aplicación

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC) y subredes.		SysAdmin
Cree grupos de seguridad y listas de control de acceso a la red (ACLs).		SysAdmin
Configure e inicie una instancia de base de datos de Amazon RDS.		SysAdmin

Migración de datos: opción 1

Tarea	Descripción	Habilidades requeridas
Migre el esquema de la base de datos manualmente o utilice una herramienta CASE como Erwin Data Modeler o SAP. PowerDesigner		Administrador de base de datos

Migración de datos: opción 2

Tarea	Descripción	Habilidades requeridas
Migre datos utilizando AWS DMS.		Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de migración de aplicaciones.		DBA, SysAdmin propietario de la aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Cambie los clientes de la aplicación a la nueva infraestr uctura.		DBA, propietario de la SysAdmin aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.		DBA, SysAdmin
Revise y valide los documentos del proyecto.		DBA, propietario de la SysAdmin aplicación
Recopile métricas como el tiempo de migración, el porcentaje de esfuerzo manual en comparación con el automatizado y el ahorro de costos.		DBA, propietario de la SysAdmin aplicación
Cerrar el proyecto y enviar comentarios.		DBA, propietario de la SysAdmin aplicación

Recursos relacionados

Referencias

- Sitio web de AWS DMS
- Precios de Amazon RDS
- Uso de una base de datos SAP ASE como origen para AWS DMS
- Limitaciones de RDS Custom for SQL Server

Tutoriales y videos

- Introducción a AWS DMS
- Introducción a Amazon RDS
- AWS DMS (video)
- Amazon RDS (video)

Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon Redshift mediante AWS DMS

Marcelo Fernandes, Amazon Web Services

Resumen

Este patrón proporciona orientación para migrar una base de datos de Microsoft SQL Server en las instalaciones a Amazon Redshift mediante AWS Data Migration Service (AWS DMS).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de origen de Microsoft SQL Server en un centro de datos en las instalaciones
- Requisitos previos cumplidos para usar una base de datos de Amazon Redshift como destino para AWS DMS, tal y como se describe en la documentación de AWS DMS

Versiones de producto

- Ediciones SQL Server 2005-2019, Enterprise, Standard, Workgroup, Developer y Web. Para ver la lista actualizada de versiones compatibles, consulte Usar una base de datos de Microsoft SQL Server como origen de AWS DMS en la documentación de AWS.

Arquitectura

Pila de tecnología de origen

- Base de datos de Microsoft SQL Server en las instalaciones

Pila de tecnología de destino

- Amazon Redshift

Arquitectura de migración de datos

Tools (Herramientas)

- AWS DMS es un servicio de migración de datos que admite varios tipos de bases de datos de origen y destino. Para obtener información sobre las versiones y ediciones de bases de datos de Microsoft SQL Server que se admiten para su uso con AWS DMS, consulte Uso de una base de datos de Microsoft SQL Server como fuente de AWS DMS en la documentación de AWS DMS. Si AWS DMS no es compatible con su base de datos de origen, debe seleccionar un método alternativo para la migración de datos.

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Valide la versión y el motor de la base de datos de origen y de destino.		Administrador de base de datos
Identifique los requisitos de hardware de la instancia del servidor de destino.		Administrador de base de datos, administrador de sistemas
Identifique los requisitos de almacenamiento (el tipo y la capacidad de almacenam iento).		Administrador de base de datos, administrador de sistemas
Elija el tipo de instancia adecuado en función de la capacidad, las características de almacenamiento y las características de red.		Administrador de base de datos, administrador de sistemas
Identifique los requisitos de seguridad de acceso a la red para las bases de datos de origen y destino.		Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Identificar la estrategia de migración de aplicaciones.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).	Para obtener más informaci ón, consulte Trabajar con una instancia de base de datos en una VPC en la documentación de AWS.	Administrador de sistemas
Cree grupos de seguridad.		Administrador de sistemas
Configure e inicie un clúster de Amazon Redshift.	Para obtener más información, consulte Crear un clúster de muestra de Amazon Redshift en la documentación de Amazon Redshift.	Administrador de base de datos, administrador de sistemas

Migración de datos

Tarea	Descripción	Habilidades requeridas
Migre los datos de la base de datos de Microsoft SQL Server mediante AWS DMS.		Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de migración de aplicaciones.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Cambie los clientes de la aplicación a la nueva infraestructura.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cierre los recursos temporales.		Administrador de base de datos, administrador de sistemas
Revise y valide los documentos del proyecto.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Recopile métricas como el tiempo de migración, el porcentaje de esfuerzo manual en comparación con		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
el automatizado y el ahorro de costos.		
Cerrar el proyecto y enviar comentarios.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Recursos relacionados

Referencias

- Documentación de AWS DMS
- Documentación de Amazon Redshift
- Precios de Amazon Redshift

Tutoriales y videos

- Introducción a AWS DMS
- Introducción a Amazon Redshift
- Uso de una base de datos de Amazon Redshift como objetivo de AWS Database Migration Service (AWS DMS)
- AWS DMS (video)

Migración de una base de datos en las instalaciones de Microsoft SQL Server a Amazon Redshift mediante agentes de extracción de datos de AWS SCT

Neha Thakur, Amazon Web Services

Resumen

Este patrón describe los pasos para migrar una base de datos de origen de Microsoft SQL Server en las instalaciones a una base de datos de destino de Amazon Redshift mediante los agentes de extracción de datos de la herramienta de conversión de esquemas de AWS (AWS SCT). Un agente es un programa externo que se integra con AWS SCT, pero que lleva a cabo la transformación de datos en otro lugar e interactúa con otros servicios de AWS en su nombre.

Requisitos previos y limitaciones

Requisitos previos

- Una base de datos de origen de Microsoft SQL Server utilizada para la carga de trabajo del almacenamiento de datos en un centro de datos en las instalaciones
- Una cuenta de AWS activa

Versiones de producto

- Microsoft SQL Server versión 2008 o posterior. Consulte la documentación de AWS SCT para ver una lista de las versiones compatibles más reciente..

Arquitectura

Pila de tecnología de origen

- Una base de datos de Microsoft SQL Server en las instalaciones

Pila de tecnología de destino

- Amazon Redshift

Arquitectura de migración de datos

Tools (Herramientas)

- La Herramienta de conversión de esquemas de AWS (AWS SCT) gestiona las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado a un formato compatible con la base de datos de destino. Cuando las bases de datos de origen y destino son muy diferentes, puede utilizar un agente SCT de AWS para realizar una transformación de datos adicional. Para obtener más información, consulte Migrar datos de un almacén de datos en las instalaciones a Amazon Redshift en la documentación de AWS.

Prácticas recomendadas

- Prácticas recomendadas para AWS SCT
- Prácticas recomendadas para Amazon Redshift

Epics

Preparación para la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.		Administrador de base de datos
Identifique los requisitos de hardware de la instancia del servidor de destino.		DBA, SysAdmin
Identifique los requisitos de almacenamiento (como el tipo y la capacidad de almacenam iento).		DBA, SysAdmin
Elija el tipo de instancia apropiado (capacidad,		DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
características de almacenamiento y características de red).		
Identifique los requisitos de seguridad de acceso a la red de las bases de datos de origen y destino.		DBA, SysAdmin
Elija una estrategia de migración de aplicaciones.		DBA, propietario de la SysAdmin aplicación

Configurar la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC) y subredes.		SysAdmin
Cree grupos de seguridad.		SysAdmin
Configure e inicie el clúster de Amazon Redshift.		SysAdmin

Migración de datos

Tarea	Descripción	Habilidades requeridas
Migre los datos con los agentes de extracción de datos de AWS SCT.		Administrador de base de datos

Migración de aplicaciones

Tarea	Descripción	Habilidades requeridas
Siga la estrategia de migración de aplicaciones elegida.		DBA, propietario de la SysAdmin aplicación

Realizar la transición a la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Cambie las aplicaciones cliente a la nueva infraestr uctura.		DBA, propietario de la SysAdmin aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporale s de AWS.		DBA, SysAdmin
Revise y valide los documento s del proyecto.		DBA, propietario de la SysAdmin aplicación
Recopile métricas como el tiempo de migración, el porcentaje de esfuerzo manual en comparación con el automatizado y el ahorro de costos.		DBA, propietario de la SysAdmin aplicación
Cierre el proyecto y envíe sus comentarios.		DBA, propietario de la SysAdmin aplicación

Recursos relacionados

Referencias

- Guía del usuario de AWS SCT
- Uso de agentes de extracción de datos
- Precios de Amazon Redshift

Tutoriales y videos

- Introducción a la Herramienta de conversión de esquemas de AWS
- Introducción a Amazon Redshift

Migración de aplicaciones heredadas de Oracle Pro*C a ECPG

Sai Parthasaradhi y Mahesh Balumuri, Amazon Web Services

Resumen

La mayoría de las aplicaciones antiguas que tienen código SQL integrado utilizan el precompilador Pro*C de Oracle para acceder a la base de datos. Al migrar estas bases de datos de Oracle a Amazon Relational Database Service (Amazon RDS) para PostgreSQL o a una edición compatible con Amazon Aurora PostgreSQL, debe convertir el código de la aplicación a un formato que sea compatible con el precompilador de PostgreSQL, que se denomina ECPG. Este patrón describe cómo convertir el código de Oracle Pro*C a su equivalente en PostgreSQL ECPG.

Para obtener más información sobre Pro*C, consulte la documentación de Oracle. Para obtener una breve introducción al ECPG, consulte la sección Información adicional.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos compatible con Amazon RDS para PostgreSQL o Aurora PostgreSQL
- Una base de datos de Oracle que se ejecuta en las instalaciones

Tools (Herramientas)

- Los paquetes de PostgreSQL que se enumeran en la siguiente sección.
- AWS CLI: la interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto para interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos. Con una configuración mínima, puede ejecutar comandos de la CLI de AWS que implementan una funcionalidad equivalente a la proporcionada por la consola de administración de AWS basada en navegador desde un símbolo del sistema.

Epics

Configurar el entorno de compilación en CentOS o RHEL

Tarea	Descripción	Habilidades requeridas

Instale los paquetes de PostgreSQL.	Instale los paquetes PostgreSQL necesarios utilizando los siguientes comandos.
	`yum update -y`
	`yum install -y yum-utils`
	`rpm -ivh https://download.postgresql.org/pub/repos/yum/reporpms/EL-8-x86_64/pgdg-redhat-repo-latest.noarch.rpm`
	`dnf -qy module disable postgresql`
		Desarrollador de aplicaciones, DevOps ingeniero

Instale los archivos de encabezado y las bibliotecas.	Instale el paquete `postgresql12-devel` , que contiene bibliotecas y archivos de encabezado, mediante los siguientes comandos. Instale el paquete tanto en el entorno de desarrollo como en el de tiempo de ejecución para evitar errores en el entorno de ejecución.
	`dnf -y install postgresql12-devel`
	`yum install ncompress zip ghostscript jq unzip wget git -y`
		Desarrollador de aplicaciones, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	Solo para el entorno de desarrollo, ejecute también los siguientes comandos.
	`yum install zlib-devel make -y`
	`ln -s /usr/pgsql-12/bin/ecpg /usr/bin/`	

Configure la variable de ruta del entorno.	Establezca la ruta del entorno para las bibliotecas cliente de PostgreSQL. `export PATH=$PATH:/usr/pgsql-12/bin`	Desarrollador de aplicaciones, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Instale software adicional según sea necesario.	Si es necesario, instale PGLoader como reemplazo de SQL*Loader en Oracle.
	`wget -O /etc/yum.repos.d/pgloader-ccl.repo https://dl.packager.io/srv/opf/pgloader-ccl/master/installer/el/7.repo`
	`yum install pgloader-ccl -y`
	`ln -s /opt/pgloader-ccl/bin/pgloader /usr/bin/`
	Si llama a alguna aplicación Java desde un módulo Pro*C, instale Java.
	`yum install java -y`
	Instale ant para compilar el código Java.
	`yum install ant -y`
		Desarrollador de aplicaciones, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Instale la AWS CLI.	Instale la CLI de AWS para ejecutar comandos que interactúen con servicios de AWS de como AWS Secrets Manager y Amazon Simple Storage Service (Amazon S3) desde sus aplicaciones.
	`cd /tmp/`
	`curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"`
	`unzip awscliv2.zip`
	`./aws/install -i /usr/local/aws-cli -b /usr/local/bin --update`
		Desarrollador de aplicaciones, DevOps ingeniero

Identifique los programas que se convertirán.	Identifique las aplicaciones que desea convertir de Pro*C a ECPG.	Desarrollador de aplicaciones, propietario de la aplicación

Convertir el código Pro*C a ECPG

Tarea	Descripción	Habilidades requeridas
Elimine los encabezados no deseados.	Elimine los encabezados `include` que no sean necesarios en PostgreSQL, como `oci.h`, `oratypes` y `sqlda`.	Propietario de la aplicación, desarrollador de la aplicación
Actualice las declaraciones de variables.	Agregue instrucciones `EXEC SQL` para todas las declaraciones de variables que se	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	utilizan como variables de host. Elimine de la aplicación las declaraciones `EXEC SQL VAR` como las siguientes. `EXEC SQL VAR query IS STRING(2048);`	

Tarea	Descripción	Habilidades requeridas

Actualice la funcionalidad ROWNUM.	La función `ROWNUM` no está disponible en PostgreSQL. Sustituya esto con la función de ventana `ROW_NUMBER` en las consultas SQL.
	
	Código Pro*C:
	
	`SELECT SUBSTR(RT RIM(FILE_NAME,'.tx t'),12) INTO :gcpclFil eseq FROM (SELECT FILE_NAME FROM DEMO_FILES_TABLE WHERE FILE_NAME LIKE '%POC%' ORDER BY FILE_NAME DESC) FL2 WHERE ROWNUM <=1 ORDER BY ROWNUM;`
	
	Código ECPG:
	
	`SELECT SUBSTR(RT RIM(FILE_NAME,'.tx t'),12) INTO :gcpclFil eseq FROM (SELECT FILE_NAME , ROW_NUMBE R() OVER (ORDER BY FILE_NAME DESC) AS ROWNUM FROM demo_sche ma.DEMO_FILES_TABLE WHERE FILE_NAME LIKE '%POC%' ORDER BY FILE_NAME DESC) FL2`
		Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	`WHERE ROWNUM <=1 ORDER BY ROWNUM;`	

Actualice los parámetros de la función para usar variables de alias.	En PostgreSQL, los parámetros de las funciones no se pueden usar como variables de host. Sobrescríbalos mediante una variable de alias.
	
	Código Pro*C:
	
	`int processData(int referenceId){ EXEC SQL char col_val[100]; EXEC SQL select column_name INTO :col_val from table_name where col=:referenceId; }`
	
	Código ECPG:
	
	`int processData(int referenceIdParam){ EXEC SQL int referenceId = referenceIdParam; EXEC SQL char col_val[100]; EXEC SQL select column_name INTO :col_val from table_name where col=:referenceId; }`
		Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Actualice los tipos de estructura.	Defina los tipos de `struct` en los boques `EXEC SQL BEGIN` y `END` con `typedef` si las variables de tipo `struct` se utilizan como variables de host. Si los tipos de `struct` están definidos en los archivos de encabezado (`.h`), incluya los archivos con instrucciones `EXEC SQL include`. Código Pro*C: Archivo de encabezado (`demo.h`) `struct s_partition_ranges { char sc_table_group[31]; char sc_table_name[31]; char sc_range_value[10]; }; struct s_partition_ranges_ind { short ss_table_group; short ss_table_name; short ss_range_value; };` Código ECPG:	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas

	Archivo de encabezado (`demo.h`)
	
	`EXEC SQL BEGIN DECLARE SECTION;`
	`typedef struct`
	`{`
	`  char  sc_table_group[31];`
	`  char  sc_table_name[31];`
	`  char  sc_range_value[10];`
	`} s_partition_ranges;`
	`typedef struct`
	`{`
	`  short  ss_table_group;`
	`  short  ss_table_name;`
	`  short  ss_range_value;`
	`} s_partition_ranges_ind;`
	`EXEC SQL END DECLARE SECTION;`
	
	Archivo Pro*C (`demo.pc`)
	
	`#include "demo.h"`
	`struct s_partition_ranges gc_partition_data[MAX_PART_TABLE] ;`
	`struct s_partition_ranges_ind gc_partition_data_ind[MAX_PART_TABLE] ;`
	
	Archivo ECPG (`demo.pc`)	

Tarea	Descripción	Habilidades requeridas
	`exec sql include "demo.h" EXEC SQL BEGIN DECLARE SECTION; s_partition_ranges gc_partition_data[ MAX_PART_TABLE] ; s_partition_ranges_ind gc_partition_data_ ind[MAX_PART_TABLE] ; EXEC SQL END DECLARE SECTION;`	

Tarea	Descripción	Habilidades requeridas

Modifique la lógica para extraerla de los cursores.	Para obtener varias filas de los cursores mediante variables de matriz, cambie el código que se va a utilizar `FETCH FORWARD`.
	
	Código Pro*C:
	
	`EXEC SQL char  aPoeFiles [MAX_FILES][FILENAME_LENGTH]; EXEC SQL FETCH filename_cursor into :aPoeFiles;`
	
	Código ECPG:
	
	`EXEC SQL char  aPoeFiles [MAX_FILES][FILENAME_LENGTH]; EXEC SQL int fetchSize = MAX_FILES; EXEC SQL FETCH FORWARD :fetchSize filename_cursor into :aPoeFiles;`
		Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas

Modifique las llamadas a paquetes que no tienen valores de retorno.	Las funciones de los paquetes de Oracle que no tienen valores de retorno se deben llamar con una variable indicadora. Si la aplicación incluye varias funciones que tienen el mismo nombre o si las funciones de tipo desconocido generan errores de tiempo de ejecución, clasifique los valores en los tipos de datos.
	
	Código Pro*C:
	
	`void ProcessData (char *data , int id) { EXEC SQL EXECUTE BEGIN pkg_demo.process_data (:data, :id); END; END-EXEC; }`
	
	Código ECPG:
	
	`void ProcessData (char *dataParam, int idParam ) {`
		Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas

	<pre>EXEC SQL char *data = dataParam;
	EXEC SQL int id = idParam;
	EXEC SQL short rowInd;
	EXEC SQL short rowInd = 0;
	EXEC SQL SELECT pkg_demo.process_data (
	inp_data => :data::text,
	inp_id => :id)
	INTO :rowInd;
	}</pre>	

Tarea	Descripción	Habilidades requeridas

Reescriba las variables SQL_CURSOR.	Reescriba la variable `SQL_CURSOR` y su implementación.
	
	Código Pro*C:
	
	`/* SQL Cursor */`
	`SQL_CURSOR`
	` demo_cursor;`
	`EXEC SQL`
	` ALLOCATE :demo_cursor;`
	`EXEC SQL EXECUTE`
	`  BEGIN`
	`  pkg_demo.`
	`get_cursor(`
	`  demo_cur=`
	`>:demo_cursor`
	`  );`
	`  END;`
	`END-EXEC;`
	
	Código ECPG:
	
	`EXEC SQL DECLARE`
	` demo_cursor CURSOR FOR`
	` SELECT`
	`  * from`
	`  pkg_demo.open_file`
	`name_rc(`
	`  demo_cur=`
	`>refcursor`
	`  ) ;`
	`EXEC SQL char open_file`
	`name_rcInd[100];`
	`# As the below function`
	` returns cursor_name`
	` as`
	`# return we need to`
	` use char[] type as`
	` indicator.`
		Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	`EXEC SQL SELECT pkg_demo.get_cursor ( demo_cur= >'demo_cursor' ) INTO :open_filename_rcInd;`	

Tarea	Descripción	Habilidades requeridas
Aplique patrones de migración comunes.	• Cambie las consultas SQL para que sean compatibles con PostgreSQL. • Mueva los bloques anónimos a la base de datos cuando no estén admitidos en ECPG. • Elimine la lógica `dbms_application_info` , que no admite PostgreSQL. • Mueva las instrucciones `EXEC SQL COMMIT` después de cerrar el cursor. Si realiza consultas mientras está en el bucle para recuperar los registros del cursor, el cursor se cierra y se muestra un error que indica que el cursor no existe. • Para obtener información sobre la gestión de excepciones en ECPG y códigos de error, consulte Gestión de errores en la documentación de PostgreSQL.	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Habilite la depuración, si fuera necesario.	Para ejecutar el programa ECPG en modo de depuración, añada el siguiente comando dentro del bloque de funciones principal. `ECPGdebug(1, stderr);`	Desarrollador de aplicaciones, propietario de la aplicación

Compilar programas ECPG

Tarea	Descripción	Habilidades requeridas

Cree un archivo ejecutable para ECPG.	Si tiene un archivo fuente de SQL C incrustado denominado `prog1.pgc` , puede crear un programa ejecutable mediante el siguiente Script.
	`ecpg prog1.pgc`
	`cc -I/usr/local/pgsql/include -c prog1.c`
	`cc -o prog1 prog1.o -L/usr/local/pgsql/lib -lecpg`
		Desarrollador de aplicaciones, propietario de la aplicación

Cree un archivo de creación para su compilación.	Cree un archivo make para compilar el programa ECPG, tal como se muestra en el siguiente archivo de ejemplo.
	`CFLAGS ::= $(CFLAGS) -I/usr/pgsql-12/include -g -Wall`
	`LDFLAGS ::= $(LDFLAGS) -L/usr/pgsql-12/li`
		Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas

	`b -Wl,-rpath,/usr/pgsql-12/lib`
	`LDLIBS ::= $(LDLIBS) -lecpg`
	`PROGRAMS = test`
	`.PHONY: all clean`
	`%.c: %.pgc`
	`ecpg $<`
	`all: $(PROGRAMS)`
	`clean:`
	`rm -f $(PROGRAMS) $(PROGRAMS:%=%.c) $(PROGRAMS:%=%.o)`	

Pruebe la aplicación

Tarea	Descripción	Habilidades requeridas
Pruebe el código.	Pruebe el código de la aplicación que se convertirá para asegurarse de que funciona correctamente.	Desarrollador de aplicaciones, propietario de la aplicación, ingeniero de pruebas

Recursos relacionados

- ECPG: SQL integrado en C (documentación de PostgreSQL)
- Gestión de errores (documentación de PostgreSQL)
- Por qué utilizar el precompilador Pro*C/C++ de Oracle (documentación de Oracle)

Información adicional

PostgreSQL tiene un precompilador SQL integrado, ECPG, que es equivalente al precompilador Pro*C de Oracle. El ECPG convierte los programas en C que tienen instrucciones SQL incorporadas en código C estándar sustituyendo las llamadas SQL por llamadas a funciones especiales. Luego,

los archivos de salida se pueden procesar con cualquier cadena de herramientas del compilador de C.

Archivos de entrada y salida

ECPG convierte cada archivo de entrada que especifique en la línea de comandos en el archivo de salida C correspondiente. Si el nombre de un archivo de entrada no tiene una extensión de archivo, se asume la extensión .pgc. La extensión del archivo se sustituye por `.c` para construir el nombre del archivo de salida. Sin embargo, puede anular el nombre del archivo de salida predeterminado utilizando la opción `-o`.

Si utiliza un guión (`-`) como nombre del archivo de entrada, ECPG lee el programa desde la entrada estándar y escribe en la salida estándar, a menos que lo anule mediante la opción `-o`.

Archivos de encabezado

Cuando el compilador de PostgreSQL compila los archivos de código C preprocesados, busca los archivos de cabecera ECPG en el directorio de PostgreSQL `include`. Por lo tanto, puede que tenga que usar la opción `-I` para dirigir el compilador al directorio correcto (por ejemplo, `-I/usr/local/pgsql/include`).

Bibliotecas

Los programas que utilizan código C con SQL incorporado tienen que estar enlazados a la biblioteca `libecpg`. Por ejemplo, puede utilizar las opciones `-L/usr/local/pgsql/lib -lecpg` del enlazador.

Las aplicaciones ECPG convertidas llaman a las funciones de la `libpq` biblioteca a través de la biblioteca SQL integrada (`ecpglib`) y se comunican con el servidor PostgreSQL mediante el protocolo estándar. frontend/backend

Migración de columnas generadas de forma virtual de Oracle a PostgreSQL

Veeranjaneyulu Grandhi, Rajesh Madiwale y Ramesh Pathuri, Amazon Web Services

Resumen

En la versión 11 y anteriores, PostgreSQL no proporciona una característica que sea directamente equivalente a una columna virtual de Oracle. Gestionar las columnas generadas de forma virtual al migrar de Oracle Database a la versión 11 o anterior de PostgreSQL resulta difícil por dos motivos:

- Las columnas virtuales no están visibles durante la migración.
- PostgreSQL no admite la expresión `generate` antes de la versión 12.

Sin embargo, existen soluciones alternativas para emular una funcionalidad similar. Cuando utilice AWS Database Migration Service (AWS DMS) para migrar datos desde Oracle Database a la versión 11 y anteriores de PostgreSQL, puede utilizar las funciones de activación para rellenar los valores de las columnas generadas de forma virtual. Este patrón proporciona ejemplos de código PostgreSQL y Oracle Database que puede utilizar para este fin. En AWS, puede utilizar Amazon Relational Database Service (Amazon RDS) para PostgreSQL o la Edición compatible con PostgreSQL de Amazon Aurora para la base de datos de PostgreSQL.

A partir de la versión 12 de PostgreSQL, se admiten las columnas generadas. Las columnas generadas pueden calcularse sobre la marcha a partir de otros valores de columna o calcularse y almacenarse. Las columnas generadas por PostgreSQL son similares a las columnas virtuales de Oracle.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Base de datos de origen de Oracle
- Bases de datos PostgreSQL de destino (en Amazon RDS para PostgreSQL o Aurora compatible con PostgreSQL)
- Experiencia en codificación PL/pgSQL

Limitaciones

- Solo se aplica a las versiones de PostgreSQL anteriores a la versión 12.
- Se aplica a la versión 11g o posterior de Oracle Database.
- Las columnas virtuales no se admiten en las herramientas de migración de datos.
- Solo se aplica a las columnas definidas en la misma tabla.
- Si una columna generada de forma virtual hace referencia a una función determinista definida por el usuario, no se puede utilizar como columna clave de partición.
- El resultado de la expresión debe ser un valor escalar. No puede devolver un tipo de datos proporcionado por Oracle, un tipo definido por el usuario, `LOB` o `LONG RAW`.
- Los índices que se definen en columnas virtuales equivalen a los índices basados en funciones en PostgreSQL.
- Se deben recopilar las estadísticas de las tablas.

Tools (Herramientas)

- pgAdmin 4 es una herramienta de gestión de código abierto para PostgreSQL. Esta herramienta proporciona una interfaz gráfica que simplifica la creación, el mantenimiento y el uso de los objetos de la base de datos.
- Oracle SQL Developer es un entorno de desarrollo integrado y gratuito para trabajar con SQL en bases de datos de Oracle, tanto en implementaciones tradicionales como en la nube.

Epics

Cree tablas de bases de datos de origen y destino

Tarea	Descripción	Habilidades requeridas
Cree una tabla de base de datos de Oracle de origen.	En Oracle Database, cree una tabla con columnas generadas de forma virtual mediante la siguiente declaración. `CREATE TABLE test.generated_column ( CODE NUMBER, STATUS VARCHAR2(12) DEFAULT 'PreOpen',`	Administrador de base de datos, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	``` FLAG CHAR(1) GENERATED ALWAYS AS (CASE UPPER(STATUS) WHEN 'OPEN' THEN 'N' ELSE 'Y' END) VIRTUAL VISIBLE); ``` En esta tabla de origen, los datos de la columna `STATUS` se migran a través de AWS DMS a la base de datos de destino. Sin embargo, la columna `FLAG` se rellena mediante la funcionalidad `generate by`, por lo que AWS DMS no podrá verla durante la migración. Para implementar la funcionalidad de `generated by`, debe utilizar activadores y funciones de la base de datos de destino para rellenar los valores de la columna `FLAG`, como se muestra en la siguiente epopeya.	

Tarea	Descripción	Habilidades requeridas
Cree una tabla PostgreSQL de destino en AWS.	Cree una tabla de PostgreSQL en AWS con la siguiente instrucción. `CREATE TABLE test.generated_column ( code integer not null, status character varying(12) not null , flag character(1) );` En esta tabla, la columna `status` es una columna estándar. La columna `flag` será una columna generada en función de los datos de la columna `status`.	Administrador de base de datos, desarrollador de aplicaciones

Cree una función de activación para gestionar la columna virtual en PostgreSQL

Tarea	Descripción	Habilidades requeridas
Cree un activador de PostgreSQL.	En PostgreSQL, cree un activador. `CREATE TRIGGER tgr_gen_column AFTER INSERT OR UPDATE OF status ON test.generated_column FOR EACH ROW`	Administrador de base de datos, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`EXECUTE FUNCTION test.tgf_gen_column();`	

Tarea	Descripción	Habilidades requeridas
Cree una función de activación de PostgreSQL.	En PostgreSQL, cree una función para el activador. Esta función rellena una columna virtual que la aplicación o AWS DMS insertan o actualizan y valida los datos. `CREATE OR REPLACE FUNCTION test.tgf_gen_column() RETURNS trigger AS $VIRTUAL_COL$ BEGIN IF (TG_OP = 'INSERT') THEN IF (NEW.flag IS NOT NULL) THEN RAISE EXCEPTION 'ERROR: cannot insert into column "flag"' USING DETAIL = 'Column "flag" is a generated column.'; END IF; END IF; IF (TG_OP = 'UPDATE') THEN IF (NEW.flag::VARCHAR != OLD.flag::varchar) THEN RAISE EXCEPTION 'ERROR: cannot update column "flag"' USING DETAIL = 'Column "flag" is a generated column.'; END IF; END IF; IF TG_OP IN ('INSERT','UPDATE') THEN`	Administrador de base de datos, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`IF (old.flag is NULL) OR (coalesce(old.status,'') != coalesce(new.status,'')) THEN UPDATE test.generated_column SET flag = (CASE UPPER(status) WHEN 'OPEN' THEN 'N' ELSE 'Y' END) WHERE code = new.code; END IF; END IF; RETURN NEW; END $VIRTUAL_COL$ LANGUAGE plpgsql;`	

Pruebe la migración de datos mediante AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación.	Para crear una instancia de replicación, siga las instrucciones de la documentación de AWS DMS. La instancia de replicación debe estar en la misma nube privada virtual (VPC) que las bases de datos de origen y destino.	Administrador de base de datos, desarrollador de aplicaciones
Cree puntos de conexión de origen y destino.	Para crear los puntos de conexión, siga las instrucciones de la documentación de AWS DMS.	Administrador de base de datos, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Probar los puntos de conexión.	Puede probar las conexiones de conexión especificando la VPC y la instancia de replicación y seleccionando Ejecutar prueba.	Administrador de base de datos, desarrollador de aplicaciones
Cree e inicie una tarea de carga completa.	Para obtener instrucciones, consulte Creación de una tarea y Configuración de tareas de carga completa en la documentación de AWS DMS.	Administrador de base de datos, desarrollador de aplicaciones
Valide los datos de la columna virtual.	Compare los datos de la columna virtual en las bases de datos de origen y destino. Puede validar los datos manualmente o escribir un script para este paso.	Administrador de base de datos, desarrollador de aplicaciones

Recursos relacionados

- Introducción a AWS Database Migration Service (AWS DMS) (documentación de AWS DMS)
- Uso de una base de datos de Oracle como fuente para AWS DMS (documentación de AWS DMS)
- Uso de una base de datos PostgreSQL como destino para AWS DMS (documentación de AWS DMS)
- Columnas generadas en PostgreSQL (documentación de PostgreSQL)
- Funciones de activación (documentación de PostgreSQL)
- Columnas virtuales en Oracle Database (documentación de Oracle)

Configure la funcionalidad UTL_FILE de Oracle en Aurora compatible con PostgreSQL

Rakesh Raghav y Anuradha Chintha, Amazon Web Services

Resumen

Como parte de su migración de Oracle a una edición compatible con PostgreSQL de Amazon Aurora en la nube de Amazon Web Services (AWS), es posible que se enfrente a varios desafíos. Por ejemplo, migrar el código que se basa en la utilidad de Oracle `UTL_FILE` siempre es un desafío. En Oracle PL/SQL, el paquete `UTL_FILE` se utiliza para operaciones de archivos, como lectura y escritura, junto con el sistema operativo subyacente. La utilidad `UTL_FILE` funciona tanto para los sistemas de servidor como para los de máquinas cliente.

Amazon Aurora PostgreSQL es una oferta de bases de datos administradas. Por este motivo, no es posible acceder a los archivos del servidor de la base de datos. Este patrón le guía a través de la integración de Amazon Simple Storage Service (Amazon S3) y Amazon Aurora PostgreSQL para lograr un subconjunto de funciones de `UTL_FILE`. Con esta integración, podemos crear y consumir archivos sin utilizar herramientas o servicios de extracción, transformación y carga (ETL) de terceros.

Si lo desea, puede configurar la CloudWatch supervisión de Amazon y las notificaciones de Amazon SNS.

Recomendamos probar exhaustivamente esta solución antes de implementarla en un entorno de producción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Experiencia en AWS Database Migration Service (AWS DMS)
- Experiencia en codificación PL/pgSQL
- Clúster de Amazon Aurora compatible con PostgreSQL
- Un bucket de S3

Limitaciones

Este patrón no proporciona la funcionalidad necesaria para reemplazar la utilidad de Oracle `UTL_FILE`. Sin embargo, los pasos y el código de muestra se pueden mejorar aún más para lograr sus objetivos de modernización de la base de datos.

Versiones de producto

- Edición 11.9 de Amazon Aurora compatible con PostgreSQL

Arquitectura

Pila de tecnología de destino

- Amazon Aurora compatible con PostgreSQL
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon S3

Arquitectura de destino

En el siguiente diagrama se muestra una representación de alto nivel de la solución.

1. Los archivos se cargan de la aplicación en el bucket de S3.
2. La extensión `aws_s3` accede a los datos mediante PL/pgSQL y los carga en una aplicación compatible con Aurora PostgreSQL.

Tools (Herramientas)

- Compatible con Amazon Aurora PostgreSQL: Amazon Aurora PostgreSQL Edition es un motor de bases de datos relacionales, completamente administrado, compatible con PostgreSQL y conforme a ACID. Combina la velocidad y la fiabilidad de las bases de datos comerciales de gama alta con la rentabilidad de las bases de datos de código abierto.
- AWS CLI: la interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta unificada para administrar los servicios de AWS. Con una única herramienta para descargar y configurar, puede controlar varios servicios de AWS desde la línea de comando y automatizarlos mediante scripts.
- Amazon CloudWatch: Amazon CloudWatch supervisa los recursos y el uso de Amazon S3.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet. En este patrón, Amazon S3 proporciona una capa de almacenamiento para recibir y

almacenar archivos para su consumo y transmisión hacia y desde el clúster compatible con Aurora PostgreSQL.

- aws_s3: la extensión `aws_s3` integra Amazon S3 y Aurora compatible con PostgreSQL.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y administra la entrega o el envío de mensajes entre publicadores y clientes. En este patrón, Amazon SNS se usa para enviar notificaciones.
- pgAdmin: pgAdmin es una herramienta de administración de código abierto para Postgres. pgAdmin 4 proporciona una interfaz gráfica para crear, mantener y utilizar objetos de bases de datos.

Código

Para lograr la funcionalidad requerida, el patrón crea varias funciones con nombres similares a `UTL_FILE`. La sección de información adicional contiene el código base de estas funciones.

En el código, sustituya `testaurorabucket` por el nombre del bucket de S3 de prueba. Sustituya `us-east-1` por la región de AWS de donde está ubicado su bucket de S3 de prueba.

Epics

Integre Amazon S3 y Aurora PostgreSQL

Tarea	Descripción	Habilidades requeridas
Configurar políticas de IAM.	Cree una política de AWS Identity and Access Management (políticas de IAM) que conceda acceso a un bucket de S3 y sus objetos. Para ver el código, consulte la sección de información adicional.	Administrador de AWS, Administrador de base de datos
Añada funciones de acceso de Amazon S3 a Aurora PostgreSQL.	Cree dos roles de IAM: un rol para el acceso de lectura y otro para el acceso de escritura a Amazon S3.	Administrador de AWS, Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Adjunte los dos roles al clúster compatible con Aurora PostgreSQL: • Un rol para la característica S3Export • Un rol para la característica S3Import Para obtener más información, consulte la documentación compatible con Aurora PostgreSQL sobre la importación y la exportación de datos a Amazon S3.	

Configurar las extensiones en Aurora PostgreSQL

Tarea	Descripción	Habilidades requeridas
Cree la extensión aws_commons.	La extensión `aws_commons` es una dependencia de la extensión `aws_s3`.	Administrador de base de datos, desarrollador
Cree la extensión aws_s3.	La extensión `aws_s3` interactúa con Amazon S3.	Administrador de base de datos, desarrollador

Valide la integración compatible con Amazon S3 y Aurora PostgreSQL

Tarea	Descripción	Habilidades requeridas
Prueba de importación de archivos de Amazon S3 en Aurora PostgreSQL.	Para probar la importación de archivos a un entorno compatible con Aurora	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	PostgreSQL, cree un archivo CSV de muestra y cárguelo en el bucket de S3. Cree una definición de tabla basada en el archivo CSV y cargue el archivo en la tabla mediante la función `aws_s3.table_import_from_s3` .	
Pruebe a exportar archivos de Aurora PostgreSQL a Amazon S3.	Para probar la exportación de archivos compatibles con Aurora PostgreSQL, cree una tabla de prueba, llénela con datos y, a continuación, exporte los datos mediante la función `aws_s3.query_export_to_s3` .	Administrador de base de datos, desarrollador

Para imitar la utilidad UTL_FILE, cree funciones envolventes

Tarea	Descripción	Habilidades requeridas
Cree el esquema utl_file_utility.	El esquema mantiene unidas las funciones envolventes. Ejecute el siguiente comando para crear el esquema. `CREATE SCHEMA utl_file_utility;`	Administrador de base de datos, desarrollador
Cree el tipo file_type.	Para crear el tipo `file_type` , utilice el siguiente código. `CREATE TYPE utl_file_utility.file_type AS (`	Administrador de base de datos/desarrollador

Tarea	Descripción	Habilidades requeridas
	`p_path character varying(30), p_file_name character varying );`	
Cree la función init.	La función `init` inicializa una variable común como `bucket` o `region`. Para ver el código, consulte la sección de información adicional.	Administrador de base de datos/desarrollador
Cree las funciones.	Cree las funciones envolventes `fopen`, `put_line`, y `fclose`. Para ver el código, consulte la sección de información adicional.	Administrador de base de datos, desarrollador

Pruebe las funciones de la capa

Tarea	Descripción	Habilidades requeridas
Pruebe las funciones del contenedor en modo escritura.	Para probar las funciones del contenedor en modo de escritura, utilice el código que se proporciona en la sección Información adicional.	Administrador de base de datos, desarrollador
Pruebe las funciones del contenedor en el modo de adición.	Para probar las funciones del contenedor en el modo de adición, utilice el código proporcionado en la sección Información adicional.	Administrador de base de datos, desarrollador

Recursos relacionados

- Integración de Amazon S3
- Amazon S3
- Aurora
- Amazon CloudWatch
- Amazon SNS

Información adicional

Configurar políticas de IAM

Cree las políticas siguientes.

Nombre de la política	JSON
S3 IntRead	`{ "Version": "2012-10-17", "Statement": [ { "Sid": "S3integrationtest", "Effect": "Allow", "Action": [ "s3:GetObject", "s3:ListBucket" ], "Resource": [ "arn:aws:s3:::testaurorabucket/*", "arn:aws:s3:::testaurorabucket" ] } ] }`
S3 IntWrite	`{ "Version": "2012-10-17",`

```
    "Statement": [
        {
            "Sid": "S3integrationtest
",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",

                "s3:ListBucket"
            ],
            "Resource": [
    "arn:aws:s3:::testaurorabucket/
*",                "arn:aws:s3:::test
aurorabucket"
            ]
        }
    ]
}
```

Creación de la función init

Para inicializar variables comunes, como `bucket` o `region`, cree la función `init` mediante el siguiente código.

```
CREATE OR REPLACE FUNCTION utl_file_utility.init(
    )
    RETURNS void
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
BEGIN
      perform set_config
      ( format( '%s.%s','UTL_FILE_UTILITY', 'region' )
      , 'us-east-1'::text
      , false );

      perform set_config
      ( format( '%s.%s','UTL_FILE_UTILITY', 's3bucket' )
      , 'testaurorabucket'::text
      , false );
```

```
END;
$BODY$;
```

Cree las funciones envolventes

Cree las funciones envolventes `fopen`, `put_line` y `fclose`.

fopen

```
CREATE OR REPLACE FUNCTION utl_file_utility.fopen(
    p_file_name character varying,
    p_path character varying,
    p_mode character DEFAULT 'W'::bpchar,
    OUT p_file_type utl_file_utility.file_type)
    RETURNS utl_file_utility.file_type
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
declare
    v_sql character varying;
    v_cnt_stat integer;
    v_cnt integer;
    v_tabname character varying;
    v_filewithpath character varying;
    v_region character varying;
    v_bucket character varying;

BEGIN
    /*initialize common variable */
    PERFORM utl_file_utility.init();
    v_region := current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 'region' ) );
    v_bucket :=  current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 's3bucket' ) );

    /* set tabname*/
    v_tabname := substring(p_file_name,1,case when strpos(p_file_name,'.') = 0 then
 length(p_file_name) else strpos(p_file_name,'.') - 1 end );
    v_filewithpath := case when NULLif(p_path,'') is null then p_file_name else
 concat_ws('/',p_path,p_file_name) end ;
    raise notice 'v_bucket %, v_filewithpath % , v_region %', v_bucket,v_filewithpath,
 v_region;
```

```
   /* APPEND MODE HANDLING; RETURN EXISTING FILE DETAILS IF PRESENT ELSE CREATE AN
EMPTY FILE */
   IF p_mode = 'A' THEN
       v_sql := concat_ws('','create temp table if not exists ', v_tabname,' (col1
text)');
       execute v_sql;

       begin
       PERFORM aws_s3.table_import_from_s3
           ( v_tabname,
           '',
           'DELIMITER AS ''#''',
           aws_commons.create_s3_uri
           (     v_bucket,
               v_filewithpath ,
               v_region)
           );
       exception
           when others then
            raise notice 'File load issue ,%',sqlerrm;
            raise;
       end;
       execute concat_ws('','select count(*) from ',v_tabname) into v_cnt;

       IF v_cnt > 0
       then
           p_file_type.p_path := p_path;
           p_file_type.p_file_name := p_file_name;
       else
           PERFORM aws_s3.query_export_to_s3('select ''''',
                           aws_commons.create_s3_uri(v_bucket, v_filewithpath,
v_region)
                             );

           p_file_type.p_path := p_path;
           p_file_type.p_file_name := p_file_name;
       end if;
       v_sql := concat_ws('','drop table ', v_tabname);
       execute v_sql;
   ELSEIF p_mode = 'W' THEN
           PERFORM aws_s3.query_export_to_s3('select ''''',
                           aws_commons.create_s3_uri(v_bucket, v_filewithpath,
v_region)
                             );
```

```
            p_file_type.p_path := p_path;
            p_file_type.p_file_name := p_file_name;
    END IF;

EXCEPTION
        when others then
            p_file_type.p_path := p_path;
            p_file_type.p_file_name := p_file_name;
            raise notice 'fopenerror,%',sqlerrm;
            raise;
END;
$BODY$;
```

put_line

```
CREATE OR REPLACE FUNCTION utl_file_utility.put_line(
    p_file_name character varying,
    p_path character varying,
    p_line text,
    p_flag character DEFAULT 'W'::bpchar)
    RETURNS boolean
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
/*****************************************************************************
* Write line, p_line in windows format to file, p_fp - with carriage return
* added before new line.
*****************************************************************************/
declare
    v_sql varchar;
    v_ins_sql varchar;
    v_cnt INTEGER;
    v_filewithpath character varying;
    v_tabname  character varying;
    v_bucket character varying;
    v_region character varying;

BEGIN
 PERFORM utl_file_utility.init();

/* check if temp table already exist */
```

```
 v_tabname := substring(p_file_name,1,case when strpos(p_file_name,'.') = 0 then
 length(p_file_name) else strpos(p_file_name,'.') - 1 end );

 v_sql := concat_ws('','select count(1) FROM pg_catalog.pg_class c LEFT JOIN
 pg_catalog.pg_namespace n ON n.oid = c.relnamespace where n.nspname like ''pg_temp_
%'''
                        ,' AND pg_catalog.pg_table_is_visible(c.oid) AND
 Upper(relname) = Upper( '''
                        ,  v_tabname ,''' ) ');

 execute v_sql into v_cnt;

  IF v_cnt = 0 THEN
         v_sql := concat_ws('','create temp table ',v_tabname,' (col text)');
        execute v_sql;
        /* CHECK IF APPEND MODE */
        IF upper(p_flag) = 'A' THEN
            PERFORM utl_file_utility.init();
            v_region := current_setting( format( '%s.%s', 'UTL_FILE_UTILITY',
 'region' ) );
            v_bucket :=  current_setting( format( '%s.%s', 'UTL_FILE_UTILITY',
 's3bucket' ) );

            /* set tabname*/
            v_filewithpath := case when NULLif(p_path,'') is null then p_file_name else
 concat_ws('/',p_path,p_file_name) end ;

            begin
               PERFORM aws_s3.table_import_from_s3
                     ( v_tabname,
                          '',
                       'DELIMITER AS ''#''',
                        aws_commons.create_s3_uri
                           ( v_bucket,
                               v_filewithpath,
                               v_region    )
                     );
            exception
                when others then
                    raise notice  'Error Message : %',sqlerrm;
                    raise;
            end;
        END IF;
```

```
    END IF;
    /* INSERT INTO TEMP TABLE */
    v_ins_sql := concat_ws('','insert into ',v_tabname,' values(''',p_line,''')');
    execute v_ins_sql;
    RETURN TRUE;
    exception
            when others then
                raise notice  'Error Message : %',sqlerrm;
                raise;
END;
$BODY$;
```

fclose

```
CREATE OR REPLACE FUNCTION utl_file_utility.fclose(
    p_file_name character varying,
    p_path character varying)
    RETURNS boolean
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
DECLARE
    v_filewithpath character varying;
    v_bucket character varying;
    v_region character varying;
    v_tabname character varying;
    v_sql character varying;
BEGIN
      PERFORM utl_file_utility.init();

    v_region := current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 'region' ) );
    v_bucket :=  current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 's3bucket' ) );

    v_tabname := substring(p_file_name,1,case when strpos(p_file_name,'.') = 0 then
 length(p_file_name) else strpos(p_file_name,'.') - 1 end );
    v_filewithpath := case when NULLif(p_path,'') is null then p_file_name else
 concat_ws('/',p_path,p_file_name) end ;

    raise notice 'v_bucket %, v_filewithpath % , v_region %', v_bucket,v_filewithpath,
 v_region ;
```

```
    /* exporting to s3 */
    perform aws_s3.query_export_to_s3
        (concat_ws('','select * from ',v_tabname,'  order by ctid asc'),
            aws_commons.create_s3_uri(v_bucket, v_filewithpath, v_region)
        );
    v_sql := concat_ws('','drop table ', v_tabname);
    execute v_sql;
    RETURN TRUE;
EXCEPTION
       when others then
     raise notice 'error fclose %',sqlerrm;
     RAISE;
END;
$BODY$;
```

Pruebe sus funciones de configuración y envoltura

Utilice los siguientes bloques de código anónimos para comprobar su configuración.

Pruebe el modo de escritura

El siguiente código escribe un archivo llamado `s3inttest` en el bucket de S3.

```
do $$
declare
l_file_name varchar := 's3inttest' ;
l_path varchar := 'integration_test' ;
l_mode char(1) := 'W';
l_fs utl_file_utility.file_type ;
l_status boolean;

begin
select * from
utl_file_utility.fopen( l_file_name, l_path , l_mode ) into l_fs ;
raise notice 'fopen : l_fs : %', l_fs;

select * from
utl_file_utility.put_line( l_file_name, l_path ,'this is test file:in s3bucket: for
 test purpose', l_mode ) into l_status ;
raise notice 'put_line : l_status %', l_status;

select * from utl_file_utility.fclose( l_file_name , l_path ) into l_status ;
raise notice 'fclose : l_status %', l_status;
```

```
end;
$$
```

Pruebe el modo de adición

El siguiente código añade líneas al archivo `s3inttest` que se creó en la prueba anterior.

```
do $$
declare
l_file_name varchar := 's3inttest' ;
l_path varchar := 'integration_test' ;
l_mode char(1) := 'A';
l_fs utl_file_utility.file_type ;
l_status boolean;

begin
select * from
utl_file_utility.fopen( l_file_name, l_path , l_mode ) into l_fs ;
raise notice 'fopen : l_fs : %', l_fs;


select * from
utl_file_utility.put_line( l_file_name, l_path ,'this is test file:in s3bucket: for
 test purpose : append 1', l_mode ) into l_status ;
raise notice 'put_line : l_status %', l_status;

select * from
utl_file_utility.put_line( l_file_name, l_path ,'this is test file:in s3bucket : for
 test purpose : append 2', l_mode ) into l_status ;
raise notice 'put_line : l_status %', l_status;

select * from utl_file_utility.fclose( l_file_name , l_path ) into l_status ;
raise notice 'fclose : l_status %', l_status;

end;
$$
```

Notificaciones de Amazon SNS

Si lo desea, puede configurar la CloudWatch supervisión de Amazon y las notificaciones de Amazon SNS en el bucket de S3. Para obtener más información, consulte Supervisión de Amazon S3 y Configuración de las notificaciones de Amazon SNS.

Validar los objetos de la base de datos después de migrar de Oracle a Amazon Aurora PostgreSQL

Venkatramana Chintha y Eduardo Valentim, Amazon Web Services

Resumen

Este patrón describe un step-by-step enfoque para validar objetos después de migrar una base de datos de Oracle a una edición compatible con PostgreSQL de Amazon Aurora.

Este patrón describe los escenarios de uso y los pasos para la validación de objetos de bases de datos; para obtener información más detallada, consulte Validación de objetos de bases de datos después de la migración con AWS SCT y AWS DMS en el blog sobre bases de datos de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una base de datos de Oracle local que se migró a una base de datos compatible con Aurora PostgreSQL.
- Credenciales de inicio de sesión a las que se ha aplicado la RDSData FullAccess política de Amazon, para la base de datos Aurora compatible con PostgreSQL.
- Este patrón utiliza el editor de consultas para los clústeres de bases de datos Aurora Serverless, que está disponible en la consola de Amazon Relational Database Service (Amazon RDS). Sin embargo, puede utilizar este patrón con cualquier otro editor de consultas.

Limitaciones

- Los objetos SYNONYM de Oracle no están disponibles en PostgreSQL, pero se pueden validar parcialmente mediante vistas o consultas SET search_path.
- El editor de consultas de Amazon RDS solo está disponible en determinadas regiones de AWS y para determinadas versiones de MySQL y PostgreSQL.

Arquitectura

Tools (Herramientas)

Herramientas

- Edición compatible con Amazon Aurora PostgreSQL: Aurora PostgreSQL-Compatible es un motor de bases de datos relacionales, completamente administrado, compatible con PostgreSQL y conforme a ACID, que combina la velocidad y la fiabilidad de las bases de datos comerciales de tecnología avanzada con la sencillez y la rentabilidad de las bases de datos de código abierto.
- Amazon RDS: Amazon Relational Database Service (Amazon RDS) facilita la configuración, el funcionamiento y el escalado de una base de datos relacional en la nube de AWS. Proporciona una capacidad rentable y de tamaño ajustable para una base de datos relacional estándar y se ocupa de las tareas de administración de bases de datos comunes.
- Editor de consultas para Aurora Severless: el editor de consultas le ayuda a ejecutar consultas SQL en la consola de Amazon RDS. Puede ejecutar cualquier declaración SQL válida en el clúster de base de datos de Aurora Serverless, incluidas las declaraciones de manipulación y definición de datos.

Para validar los objetos, utilice los scripts completos del archivo “Object validation scripts” de la sección “Adjuntos”. Utilice la siguiente tabla como referencia.

Objeto de Oracle	Script a utilizar
Paquetes	Consulta 1
Tablas	Consulta 3
Vistas	Consulta 5
Secuencias	Consulta 7
Desencadenadores	Consulta 9
Claves principales	Consulta 11
Índices	Consulta 13
Restricciones de comprobación	Consulta 15
Claves externas	Consulta 17

Objeto PostgreSQL	Script a utilizar
Paquetes	Consulta 2
Tablas	Consulta 4
Vistas	Consulta 6
Secuencias	Consulta 8
Desencadenadores	Consulta 10
Claves principales	Consulta 12
Índices	Consulta 14
Restricciones de comprobación	Consulta 16
Claves externas	Consulta 18

Epics

Valide los objetos de la base de datos de Oracle de origen

Tarea	Descripción	Habilidades requeridas
Ejecute la consulta de validación de “paquetes” en la base de datos de Oracle de origen.	Descargue y abra el archivo “Object validation scripts” de la sección “Adjuntos”. Conéctese a la base de datos de Oracle de origen a través de su programa cliente. Ejecute el script de validacio nes “Query 1” desde el archivo “Object validation scripts”. Importante: Introduzca su nombre de usuario de Oracle en lugar de “your_schema” en las consultas. Asegúrese de	Desarrollador, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	registrar los resultados de la consulta.	
Ejecute la consulta de validación “tables”.	Ejecute el script “Query 3” desde el archivo “Object validation scripts”. Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación “views”.	Ejecute el script “Query 5” desde el archivo “Object validation scripts”. Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la validación del recuento “sequences”.	Ejecute el script “Query 7” desde el archivo “Object validation scripts”. Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación “triggers”.	Ejecute el script “Query 9” desde el archivo “Object validation scripts”. Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación “primary keys”.	Ejecute el script “Query 11” desde el archivo “Object validation scripts”. Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Ejecute la consulta de validación “indexes”.	Ejecute el script de validació n “Query 13” desde el archivo “Object validation scripts”. Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación “check constraints”.	Ejecute el script “Query 15” desde el archivo “Object validation scripts”. Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación “foreign keys”.	Ejecute el script de validació n “Query 17” desde el archivo “Object validation scripts”. Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos

Validar objetos en la base de datos compatible con Aurora PostgreSQL de destino

Tarea	Descripción	Habilidades requeridas
Conectar a la base de datos Aurora compatibl e con PostgreSQL de destino mediante el editor de consultas.	Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon RDS. En la esquina superior derecha, elija la región de AWS en la que creó la base de datos Aurora PostgreSQ L. En el panel de navegación, elija “Bases de datos” y elija la base de datos compatible con Aurora PostgreSQL de destino. En “Acciones”, elija “Consulta”. Importante: si no	Desarrollador, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	se ha conectado a la base de datos antes, se abre la página “Conectarse a la base de datos”. A continuación, debe introducir la informaci ón de la base de datos, como el nombre de usuario y la contraseña.	
Ejecute la consulta de validación “packages”	Ejecute el script “Query 2” desde el archivo “Object validation scripts” de la sección “Adjuntos”. Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación “tables”.	Vuelva al editor de consultas de la base de datos compatibl e con Aurora PostgreSQL y ejecute el script “Query 4” desde el archivo “Object validation scripts”. Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación “views”.	Vuelva al editor de consultas de la base de datos compatibl e con Aurora PostgreSQL y ejecute el script “Query 6” desde el archivo “Object validation scripts”. Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Ejecute la validación del recuento “sequences”.	Vuelva al editor de consultas de la base de datos compatible con Aurora PostgreSQL y ejecute el script “Query 8” desde el archivo “Object validation scripts”. Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación “triggers”.	Vuelva al editor de consultas de la base de datos compatible con Aurora PostgreSQL y ejecute el script “Query 10” desde el archivo “Object validation scripts”. Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación “primary keys”.	Vuelva al editor de consultas de la base de datos compatible con Aurora PostgreSQL y ejecute el script “Query 12” desde el archivo “Object validation scripts”. Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación “indexes”.	Vuelva al editor de consultas de la base de datos compatible con Aurora PostgreSQL y ejecute el script “Query 14” desde el archivo “Object validation scripts”. Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Ejecute la consulta de validación “check constraints”.	Ejecute el script “Query 16” desde el archivo “Object validation scripts”. Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación “foreign keys”.	Ejecute el script de validació n “Query 18” desde el archivo “Object validation scripts”. Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos

Compare los registros de validación de las bases de datos de origen y destino

Tarea	Descripción	Habilidades requeridas
Compare y valide los resultados de ambas consultas.	Compare los resultados de las consultas de las bases de datos compatibles con Oracle y Aurora PostgreSQL para validar todos los objetos. Si todos coinciden, significa que todos los objetos se han validado correctamente.	Desarrollador, administrador de base de datos

Recursos relacionados

- Validación de objetos de bases de datos después de una migración mediante AWS SCT y AWS DMS
- Características de Amazon Aurora: edición compatible con PostgreSQL

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Volver a alojar

Temas

- Acelere el descubrimiento y la migración de las cargas de trabajo de Microsoft a AWS
- Cree un proceso de aprobación para las solicitudes de firewall durante una migración de rehospedaje a AWS
- Incorpore y migre instancias de EC2 Windows a una cuenta de AWS Managed Services
- Migrar una base de datos de Couchbase Server a Amazon EC2
- Migre Db2 for LUW a Amazon EC2 mediante el envío de registros para reducir el tiempo de interrupción
- Migración de Db2 para LUW a Amazon EC2 con recuperación de desastres de alta disponibilidad
- Migre IIS-hosted aplicaciones a Amazon EC2 mediante appcmd.exe
- Migre una base de datos local de Microsoft SQL Server a Amazon EC2 mediante MGN
- Migre una carga de trabajo de F5 BIG-IP a F5 BIG-IP VE en Nube de AWS
- Migración de una aplicación web Go en las instalaciones a AWS Elastic Beanstalk mediante el método binario
- Migre un servidor SFTP local para utilizar AWS AWS Transfer for SFTP
- Migre una máquina virtual local a Amazon EC2 mediante AWS Application Migration Service
- Migre pequeños conjuntos de datos del entorno local a Amazon S3 mediante AWS SFTP
- Migre una base de datos Oracle local a Oracle on Amazon EC2
- Migre una base de datos Oracle local a Amazon EC2 mediante Oracle Data Pump
- Migración de los sistemas BYOL de RHEL a instancias con licencia incluida de AWS mediante AWS MGN
- Migre una base de datos local de Microsoft SQL Server a Amazon EC2
- Vuelva a alojar las cargas de trabajo en las instalaciones en la nube de AWS: lista de verificación de migración
- Configure una infraestructura Multi-AZ para una FCI Always On de SQL Server mediante Amazon FSx
- Utilice las consultas de BMC Discovery para extraer datos de migración para planificar la migración

Acelere el descubrimiento y la migración de las cargas de trabajo de Microsoft a AWS

Ali Alzand, Amazon Web Services

Resumen

Este patrón le muestra cómo usar el PowerShell módulo Migration Validator Toolkit para detectar y migrar sus cargas de trabajo de Microsoft a AWS. El módulo funciona realizando múltiples comprobaciones y validaciones para tareas comunes asociadas a cualquier carga de trabajo de Microsoft. Por ejemplo, el módulo busca instancias que puedan tener varios discos conectados o instancias que usen muchas direcciones IP. Para obtener una lista completa de las comprobaciones que puede realizar el módulo, consulte la sección Comprobaciones de la página del módulo. GitHub

El PowerShell módulo Migration Validator Toolkit puede ayudar a su organización a reducir el tiempo y el esfuerzo necesarios para descubrir qué aplicaciones y servicios se ejecutan en sus cargas de trabajo de Microsoft. El módulo también puede servirle de ayuda para identificar las configuraciones de sus cargas de trabajo para que pueda averiguar si sus configuraciones son compatibles con AWS. El módulo también proporciona recomendaciones sobre los próximos pasos y las acciones de mitigación, de modo que puede evitar cualquier error de configuración antes, durante o después de la migración.

Requisitos previos y limitaciones

Requisitos previos

- Cuenta de administrador local
- PowerShell 4.0

Limitaciones

- Solo funciona con instancias de Microsoft Windows Server 2012 R2 o versiones posteriores.

Tools (Herramientas)

Herramientas

- PowerShell 4.0

Repositorio de código

El PowerShell módulo Migration Validator Toolkit para este patrón está disponible en el GitHub migration-validator-toolkit-for repositorio -microsoft-workloads.

Epics

Ejecute el módulo Migration Validator Toolkit en un único destino PowerShell

Tarea	Descripción	Habilidades requeridas

Descargue, extraiga, importe e invoque el módulo.	Elija uno de los siguientes métodos para descargar e implementar el módulo:
	• Ejecute el script PowerShell
	• Descargue y extraiga el archivo .zip
	• Clona el GitHub repositorio
	
	Ejecute el PowerShell script
	
	En PowerShell, ejecute el siguiente código de ejemplo:
	
	`#MigrationValidatorToolkit`
	`$uri = 'https://github.com/aws-samples/migration-validator-toolkit-for-microsoft-workloads/archive/refs/heads/main.zip'`
	`$destination = (Get-Location).Path`
	`if ((Test-Path -Path "$destination\MigrationValidatorToolkit.zip" -PathType Leaf) -or (Test-Path -Path "$destination\Migr`
		Administrador de sistemas

Tarea	Descripción	Habilidades requeridas

	ationValidatorTool
	kit")) {
	    write-host "File
	 $destination\Migra
	tionValidatorToolk
	it.zip or folder
	 $destination\Migra
	tionValidatorToolkit
	 found, exiting"
	}else {
	    Write-host "Enable
	 TLS 1.2 for this
	 PowerShell session
	 only."
	    [Net.ServicePointM
	anager]::SecurityP
	rotocol = [Net.Secu
	rityProtocolType]:
	:Tls12
	    $webClient =
	 New-Object System.Ne
	t.WebClient
	    Write-host
	 "Downloading Migration
	ValidatorToolkit.zip"
	    $webClient.Downloa
	dFile($uri, "$destina
	tion\MigrationVali
	datorToolkit.zip")
	    Write-host
	 "MigrationValidato
	rToolkit.zip download
	 successfully"
	    Add-Type -Assembly
	 "system.io.compres
	sion.filesystem"
	    [System.IO.Compres
	sion.ZipFile]::Ext
	ractToDirectory("$
	destination\Migrat
	ionValidatorToolki
	t.zip","$destinati	

Tarea	Descripción	Habilidades requeridas

	<pre>on\MigrationValida
	torToolkit")
	    Write-host
	 "Extracting Migration
	ValidatorToolkit.zip
	 complete successfully"
	    Import-Module
	 "$destination\Migr
	ationValidatorToolkit
	\migration-validator-
	toolkit-for-microsoft
	-workloads-main\Mi
	grationValidatorTo
	olkit.psm1"; Invoke-
	MigrationValidatorTo
	olkit
	}</pre>
	El código descarga el módulo de un archivo.zip. A continuación, el código extrae, importa e invoca el módulo.
	
	Descargue y extraiga el archivo .zip
	
	1. Descargue el archivo .zip (descargar).
	2. Descomprima el archivo .zip.
	3. Siga los pasos de la sección sobre cómo invocar el módulo manualmente en esta guía.
	
	Clona el GitHub repositorio	

Tarea	Descripción	Habilidades requeridas
	1. Para clonar el repositorio GitHub migration-validator-toolkit-for-microsoft-workloads, ejecuta el siguiente comando Git en una ventana de terminal: `git clone https://github.com/aws-samples/migration-validator-toolkit-for-microsoft-workloads.git` 2. Siga los pasos de la sección sobre cómo invocar el módulo manualmente en esta guía.	

Tarea	Descripción	Habilidades requeridas

Invoque el módulo manualmente.	1. Vaya al directorio en el que está almacenado el módulo descargado.
	2. Para generar el resultado que prefieras, ejecuta uno de los siguientes comandos como administrador en: PowerShell
	
	Formato Format-Table:
	
	`Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit`
	
	Formato Format-List:
	
	`Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit -List`
	
	GridViewFormato de salida:
	
	`Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit -GridView`
	
	ConvertTo-Formato CSV:
	
	`Import-Module .\MigrationValidatorToolkit`
		Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	`.psm1;Invoke-Migra tionValidatorToolkit -csv`	

Ejecute el módulo Migration Validator Toolkit PowerShell en varios objetivos

Tarea	Descripción	Habilidades requeridas
Descargue el archivo.zip o clone el repositorio. GitHub	Elija una de las siguientes opciones: • Descargue el archivo zip. (descargar). • Para clonar el repositorio GitHub migration-validator-toolkit-for-microsoft-workloads, ejecuta el siguiente comando Git en una ventana de terminal: `git clone https://github.com/aws-samples/migration-validator-toolkit-for-microsoft-workloads.git`	Administrador de sistemas
Actualice la lista server.csv.	Si descargó el archivo .zip, siga estos pasos: 1. Descomprima el archivo .zip. 2. Vaya al directorio `MigrationValidator Toolkit\Inputs\` .	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	3. Actualice `serverlist.csv` con el nombre de host de los equipos de destino.	
Invoque el módulo.	Puede utilizar cualquier equipo del dominio que utilice un usuario del dominio que tenga acceso de administrador a los equipos de destino. 1. Descargue el código fuente como un archivo .zip y extraiga el archivo. 2. Como administrador en PowerShell, ejecuta el siguiente comando: `Import-Module .\MigrationValidatorToolkit.psm1;Invoke-DomainComputers` El archivo.csv de salida se guarda en `MigrationValidatorToolkit\Outputs\folder` con el nombre del prefijo `DomainComputers_MigrationAutomations_YYYY-MM-DDTHH-MM-SS` .	Administrador de sistemas

Resolución de problemas

Problema	Solución
`MigrationValidatorToolkit` escribe información sobre las ejecuciones, comandos y errores en los archivos de registro del host en ejecución.	Puede ver los registros manualmente en la siguiente ubicación: 1. Vaya al directorio `MigrationValidatorToolkit\logs\` . 2. Busque el archivo de registro. El formato del nombre del archivo de registro es: `ComputerName_MigrationValidatorToolkit_YYYY-MM-SSTHH-MM-SS.log`

Recursos relacionados

- Opciones, herramientas y prácticas recomendadas para migrar cargas de trabajo de Microsoft a AWS (Recomendaciones de AWS)
- Patrones de migración de Microsoft (Recomendaciones de AWS)
- Servicios gratuitos de migración a la nube en AWS (documentación de AWS)
- Acciones predefinidas posteriores al lanzamiento (documentación de marketing de la aplicación)

Información adicional

Preguntas frecuentes

¿Dónde puedo ejecutar el módulo Migration Validator Toolkit? PowerShell

Puede ejecutar el módulo en Microsoft Windows Server 2012 R2 o posterior.

¿Cuándo ejecuto este módulo?

Le recomendamos que ejecute el módulo durante la fase de evaluación del proceso de migración.

¿El módulo modifica mis servidores actuales?

No. Todas las acciones del módulo son de solo lectura.

¿Cuánto tiempo se tarda en ejecutar el módulo?

La ejecución del módulo suele tardar entre 1 y 5 minutos, pero depende de la asignación de recursos del servidor.

¿Qué permisos necesita el módulo para ejecutarse?

Debe ejecutar el módulo desde una cuenta de administrador local.

¿Puedo ejecutar el módulo en servidores físicos?

Sí, siempre que el sistema operativo sea Microsoft Windows Server 2012 R2 o posterior.

¿Cómo puedo ejecutar el módulo a escala para varios servidores?

Para ejecutar el módulo a escala en varios ordenadores unidos a un dominio, siga los pasos del PowerShell módulo Ejecute el kit de herramientas de validación de migración en varios destinos, que se incluye en esta guía. En el caso de ordenadores que no estén unidos a un dominio, utilice una invocación remota o ejecute el módulo de forma local siguiendo los pasos del módulo Ejecute el kit de herramientas PowerShell de validación de migración en un solo destino, épica de esta guía.

Cree un proceso de aprobación para las solicitudes de firewall durante una migración de rehospedaje a AWS

Srikanth Rangavajhala, Amazon Web Services

Resumen

Si quieres usar AWS Transform MGNCloud Migration Factory activado AWS para migrar a un rehost Nube de AWS, uno de los requisitos previos es mantener abiertos los puertos TCP 443 y 1500. Por lo general, la apertura de estos puertos de firewall requiere la aprobación de tu equipo de seguridad de la información (InfoSec).

Este patrón describe el proceso para obtener la aprobación de una solicitud de firewall por parte de un InfoSec equipo durante una migración de rehost a. Nube de AWS Puedes utilizar este proceso para evitar que el InfoSec equipo rechace tu solicitud de firewall, lo que puede resultar caro y llevar mucho tiempo. El proceso de solicitud del firewall consta de dos pasos de revisión y aprobación entre los asesores de AWS migración y los líderes, quienes trabajan con su equipo InfoSec y el de aplicaciones para abrir los puertos del firewall.

Este patrón supone que está planificando una migración de rehospedaje con AWS consultores o especialistas en migración de su organización. Puede utilizar este patrón si su organización no cuenta con un proceso de aprobación de firewall o si no tiene un formulario de aprobación global para solicitar un firewall. Para obtener más información al respecto, consulte la sección Limitaciones de este patrón. Para obtener más información sobre los requisitos de red para MGN, consulte los requisitos de red en la documentación de MGN.

Requisitos previos y limitaciones

Requisitos previos

- Una migración planificada de realojamiento con AWS consultores o especialistas en migración de su organización
- La información de puerto e IP necesaria para migrar la pila
- Diagramas de arquitectura de estados actuales y futuros
- Información de firewall sobre la infraestructura en las instalaciones y de destino, los puertos y el flujo de tráfico de zona a zona
- Una lista de verificación para revisar las solicitudes de firewall (adjunta)
- Un documento de solicitud de firewall, configurado de acuerdo con los requisitos de su organización

- Una lista de contactos para los revisores y aprobadores de firewall, que incluya los siguientes roles:
  - Presentador de la solicitud de firewall: especialista en AWS migración o consultor. El remitente de la solicitud de firewall también puede ser un especialista en migración de su organización.
  - Revisor de solicitudes de firewall: por lo general, es el punto de contacto único (SPOC) desde el que se envía. AWS
  - Aprobador de solicitudes de firewall: miembro InfoSec del equipo.

Limitaciones

- Este patrón describe un proceso genérico de aprobación de una solicitud de firewall. Los requisitos pueden variar de una organización a otra.
- Asegúrese de realizar un seguimiento de los cambios en el documento de solicitud de firewall.

En la tabla siguiente se muestran los casos de uso de este patrón.

¿Cuenta su organización con un proceso de aprobación de firewalls existente?	¿Cuenta su organización con un formulario de solicitud de firewall existente?	Acción sugerida
Sí	Sí	Colabore con AWS consultores o con sus especialistas en migración para implementar el proceso de su organización.
No	Sí	Utilice el proceso de aprobación de firewall de este patrón. Recurra a un AWS consultor o a un especialista en migración de su organización para enviar el formulario de aprobación general de la solicitud de firewall.
No	No	Utilice el proceso de aprobación de firewall de este patrón.

	Recurra a un AWS consultor o a un especialista en migración de su organización para enviar el formulario de aprobació n general de la solicitud de firewall.

Arquitectura

En el siguiente diagrama, se muestran los pasos del proceso de aprobación de solicitudes de firewall.

Tools (Herramientas)

Puede utilizar herramientas de escaneo como Palo Alto Networks o SolarWindsanalizar y validar los firewalls y las direcciones IP.

Epics

Analizar la solicitud de firewall

Tarea	Descripción	Habilidades requeridas
Analice los puertos y las direcciones IP.	El remitente de la solicitud de firewall realiza un análisis inicial para comprender los puertos y las direcciones IP de firewall necesarios. Una vez hecho esto, solicitan que tu InfoSec equipo abra los puertos necesarios y mapee las direcciones IP.	Ingeniero de nube de AWS, especialista en migración

Validar la solicitud de firewall

Tarea	Descripción	Habilidades requeridas
Valide la información de firewall.	El Nube de AWS ingeniero programa una reunión con su InfoSec equipo. Durante esta reunión, el ingeniero examina y valida la información de la solicitud de firewall. Por lo general, el remitente de la solicitud de firewall es la misma persona que el solicitante de firewall. Esta fase de validación puede pasar a ser iterativa en función de los comentarios que dé el responsable de la aprobació n si se observa o recomienda algo.	Ingeniero de nube de AWS, especialista en migración
Actualice el documento de solicitud de firewall.	Una vez que el InfoSec equipo comparte sus comentarios, el documento de solicitud de firewall se edita, se guarda y se vuelve a cargar. Este documento se actualiza después de cada iteración. Se recomienda almacenar este documento en una carpeta de almacenamiento con control de versiones. Esto significa que se realiza un seguimiento de todos	Ingeniero de nube de AWS, especialista en migración

Tarea	Descripción	Habilidades requeridas
	los cambios y se aplican correctamente.	

Enviar la solicitud de firewall

Tarea	Descripción	Habilidades requeridas
Envíe la solicitud de firewall.	Una vez que el aprobador de la solicitud de firewall haya aprobado la solicitud de aprobación general del firewall, el Nube de AWS ingeniero envía la solicitud de firewall. La solicitud especific a los puertos que deben estar abiertos y las direcciones IP que se requieren para asignar y actualizar la Cuenta de AWS. Puede hacer sugerencias o enviar comentarios una vez enviada la solicitud de firewall. Le recomendamos que automatice este proceso de comentarios y envíe cualquier modificación mediante un mecanismo de flujo de trabajo definido.	Ingeniero de nube de AWS, especialista en migración

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Incorpore y migre instancias de EC2 Windows a una cuenta de AWS Managed Services

Anil Kunapareddy y Venkatramana Chintha, Amazon Web Services

Resumen

Este patrón explica el step-by-step proceso de migración e ingestión de instancias de Windows de Amazon Elastic Compute Cloud EC2 (Amazon) en una cuenta de Amazon Web Services (AWS) Managed Services (AMS). AMS puede ayudar a administrar la instancia de manera más eficiente y segura. AMS proporciona flexibilidad operativa, mejora la seguridad y el cumplimiento, y ayuda a optimizar la capacidad y reducir los costos.

Este patrón comienza con una instancia de EC2 Windows que ha migrado a una subred provisional de su cuenta de AMS. Hay varios servicios y herramientas de migración disponibles para realizar esta tarea, como AWS Application Migration Service.

Para realizar un cambio en su entorno administrado por AMS, debe crear y enviar una solicitud de cambio (RFC) para una operación o acción concreta. Con una RFC de incorporación de carga de trabajo de AMS (WIGS), se incorpora la instancia en la cuenta de AMS y se crea una imagen de máquina de Amazon (AMI) personalizada. A continuación, debe crear la EC2 instancia gestionada por AMS enviando otro RFC para crear una pila. EC2 Para obtener más información, consulte AMS Workload Ingest (Incorporación de carga de trabajo de AMS) en la documentación de AMS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa y administrada por AMS
- Una zona de aterrizaje existente
- Permisos para realizar cambios en la VPC administrada por AMS
- Una instancia de Amazon EC2 Windows en una subred provisional de su cuenta AMS
- Cumplimiento de los requisitos previos generales para la migración de cargas de trabajo mediante AMS WIGS
- Cumplimiento de los requisitos previos de Windows para la migración de cargas de trabajo mediante AMS WIGS

Limitaciones

- Este patrón es para las EC2 instancias que utilizan Windows Server. Este patrón no se aplica a las instancias que ejecutan otros sistemas operativos, como Linux.

Arquitectura

Pila de tecnología de origen

Instancia de Amazon EC2 Windows en una subred provisional de su cuenta AMS

Pila de tecnología de destino

Instancia de Amazon EC2 Windows gestionada por AWS Managed Services (AMS)

Arquitectura de destino

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede utilizar Amazon EC2 para lanzar tantos o tan pocos servidores virtuales como necesite, y puede ampliarlos de forma horizontal o horizontal.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Managed Services (AMS) ayuda a operar de manera más eficiente y segura al proporcionar una administración continua de la infraestructura de AWS, que incluye supervisión, administración de incidentes, orientación de seguridad, soporte de parches y respaldo para las cargas de trabajo de AWS.

Otros servicios

- PowerShelles un programa de administración de automatización y configuración de Microsoft que se ejecuta en Windows, Linux y macOS.

Epics

Configurar los ajustes de la instancia

Tarea	Descripción	Habilidades requeridas
Cambie la configuración del cliente DNS.	1. En la EC2 instancia de origen, abra Command Prompt como administrador, escriba `ygpedit.msc` , a continuación, presione Entrar. 2. En el editor de políticas de grupo local, vaya a Computer Configuration (Configuración del equipo), Administrative Templates (Plantillas administrativas), Network (Red) y DNS Client. 3. En Primary DNS suffix (Sufijo DNS principal), seleccione Not configured. 4. En Primary DNS suffix devolution (Devolución del sufijo DNS principal), seleccione Not configured.	Ingeniero de migraciones
Cambie la configuración de Windows Update (actualizaciones de Windows).	1. En el editor de políticas de grupo local, vaya a Computer Configuration (Configuración del equipo), Administrative Templates (Plantillas administrativas), Windows Components (Componentes de Windos),	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	Windows Update (Actualización de Windows). 2. En Specify intranet Microsoft update service location (Especificar la ubicación del servicio de actualización de Microsoft en la intranet), seleccione Not configured. 3. En Configure Automatic Updates (Configurar actualizaciones automáticas), seleccione Not configured. 4. En Automatic Updates detection frequency (Frecuencia de detección de actualizaciones automática), seleccione Not configured. 5. Cierre el editor de políticas de grupo local.	
Habilitar un firewall.	1. En la EC2 instancia de origen, abra Command Prompt como administrador, escriba `yservices.msc` , a continuación, presione Entrar. 2. En los Servicios de Windows, habilite el Firewall. 3. Cierre los Servicios de Windows.	Ingeniero de migraciones

Preparación de la instancia para AMS WIGS

Tarea	Descripción	Habilidades requeridas
Limpie y prepare la instancia.	1. Con un host bastión y credenciales locales, crea una conexión de protocolo de escritorio remoto (RDP) a la EC2 instancia en la subred provisional. 2. Elimine todo el software antiguo, el software antivirus y las soluciones de copia de seguridad que no sean necesarios en AMS.	Ingeniero de migraciones

Repare el archivo sppnp.dll.	1. Vaya a `C:\Windows\System32\sppnp.dll` .
	2. Cambie el nombre de `sppnp.dll` a `sppnp_old.dll` .
	3. Con PowerShell las credenciales de administrador, ingresa los siguientes comandos:
	`dism /online /cleanup-image /restorehealth`
	`sfc /scannnow`
	4. Reinicie la instancia de EC2 Windows.
		Ingeniero de migraciones

Ejecute el script de validación previa a WIG.	1. Descargue el archivo zip de validación previa a la incorporación de Windows	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	WIGS (`windows-prewings-valication.zip`) de la sección Migrating workloads: Windows pre-ingestion validation (Migración de cargas de trabajo: validación previa a la incorporación de Windows), en la documentación de AMS. 2. Ejecute el script de validación previa a WIG de Windows y compruebe los resultados. 3. Si se produce un error en la validación, solucione el problema y vuelva a ejecutar el script de validación hasta que la validación se realice correctamente.	

Tarea	Descripción	Habilidades requeridas
Cree la AMI a prueba de fallos.	Una vez superada la validación previa a WIG, cree una AMI previa a la incorporación de la siguiente manera: 1. Seleccione Deployment (Implementación), Advanced stack components (Componentes de pila avanzados), AMI y Create. 2. Durante la creación, añada una etiqueta `Key=Name, Value=APPLICATION-ID_IngestReady` . 3. Espere a que se cree la AMI antes de continuar. Para obtener más información, consulte AMI | Create (AMI | Crear) en la documentación de AMS.	Ingeniero de migraciones

Incorporar y validar la instancia

Tarea	Descripción	Habilidades requeridas
Envíe la RFC para crear la pila de incorporación de carga de trabajo.	Envíe una solicitud de cambio (RFC) para iniciar AMS WIGS. Para obtener instrucciones, consulte Workload Ingest Stack: Creating (Pila de incorporación de carga de trabajo: creación) en la	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	documentación de AMS. Esto inicia la ingesta de carga de trabajo e instala todo el software requerido por AMS, incluidas las herramientas de respaldo, el software de EC2 administración de Amazon y el software antivirus.	

Tarea	Descripción	Habilidades requeridas
Valide que la migración sea correcta.	Una vez completada la incorporación de carga de trabajo, podrá ver la instancia administrada por AMS y la AMI incorporada por AMS. 1. Inicie sesión en la instancia administrada por AMS con las credenciales de dominio. 2. Valide la unión al dominio de la siguiente manera: a. En Explorador de Windows, haga clic con el botón secundari o en This PC (Esta computadora) y elija Properties (Propieda des). b. En la sección Especific ación del dispositivo, confirme que aparezca el dominio en el Full device name (Nombre completo del dispositivo). 3. Valide las unidades de disco de origen y destino.	Ingeniero de migraciones

Lanzar la instancia en la cuenta AMS de destino

Tarea	Descripción	Habilidades requeridas
Envíe el RFC para crear una pila. EC2	1. Con la AMI ingerida por AMS de la instancia de Windows, prepare una RFC para EC2 una pila de acuerdo con las instrucciones de la sección EC2 Crear instancia de pila en la documentación de AMS. En la EC2 pila RFC, proporciona todos los parámetros, incluidos el nombre del servidor, las etiquetas, la VPC de destino, la subred de destino, el tipo de instancia, los grupos de seguridad de destino, la AMI de ingestión y la función. 2. Envía el RFC de la EC2 pila y, a continuación, espera a que la instancia se cree correctamente.	Ingeniero de migraciones

Recursos relacionados

Recomendaciones de AWS

- Automatización de las actividades previas a la ingesta de cargas de trabajo para AWS Managed Services en Windows
- Automatically create an RFC in AMS using Python (Crear automáticamente una RFC en AMS mediante Python)

Documentación de AMS

- AMS Workload Ingest (Incorporar carga de trabajo de AMS)
- How Migration Changes Your Resource (Cómo la migración cambia el recurso)
- Migrating Workloads: Standard Process (Migración de cargas de trabajo: proceso estándar)

Recursos de marketing

- AWS Managed Services
- AWS Managed Services FAQs
- Recursos de AWS Managed Services
- Características de AWS Managed Services

Migrar una base de datos de Couchbase Server a Amazon EC2

Subhani Shaik, Amazon Web Services

Resumen

Este patrón describe cómo puede migrar Couchbase Server de un entorno local a Amazon Elastic Compute Cloud (Amazon EC2) en adelante. AWS

Couchbase Server es una base de datos NoSQL (documento JSON) distribuida que proporciona capacidades de base de datos relacional. La migración de una base de datos de Couchbase Server AWS puede proporcionar mayor escalabilidad, mejor rendimiento, rentabilidad, seguridad mejorada, administración simplificada y alcance global, lo que puede beneficiar a las aplicaciones que requieren un acceso a los datos de alta disponibilidad y baja latencia. También puede acceder a funciones avanzadas a través de servicios gestionados. AWS

Couchbase Server on AWS ofrece las siguientes funciones clave:

- Arquitectura que prioriza la memoria
- Alta disponibilidad, recuperación ante desastres y equilibrio de carga
- Implementación multimaestro y multirregional para un rendimiento óptimo

Para obtener más información sobre los principales beneficios, consulte la sección Información adicional y el sitio web de Couchbase.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS con una nube privada virtual (VPC), dos zonas de disponibilidad, subredes privadas y un grupo de seguridad. Para obtener instrucciones, consulte Create a VPC en la documentación de Amazon Virtual Private Cloud (Amazon VPC).
- Conectividad activada entre el entorno de origen y de destino. Para obtener información sobre los puertos TCX que utiliza Couchbase Server, consulte la documentación de Couchbase.

Arquitectura

El siguiente diagrama muestra la arquitectura de alto nivel para migrar Couchbase Server a. AWS

Desde el clúster de Couchbase en las instalaciones, los datos se mueven a través de una puerta de enlace de cliente mediante AWS Direct Connect. Los datos pasan a través de un router y una Direct Connect ruta y llegan a la VPC a través de una puerta de enlace AWS Virtual Private Network (Site-to-Site VPN). La VPC contiene una EC2 instancia que ejecuta Couchbase Server. La AWS infraestructura también incluye AWS Identity and Access Management (IAM) para el control de acceso, AWS Key Management Service (AWS KMS) para el cifrado de datos, Amazon Elastic Block Store (Amazon EBS) para el almacenamiento en bloques y Amazon Simple Storage Service (Amazon S3) para el almacenamiento de datos.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática escalable en el Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- AWS Direct Connectconecta su red interna a una Direct Connect ubicación a través de un cable de fibra óptica Ethernet estándar. Con esta conexión, puede crear interfaces virtuales directamente con las públicas y, al Servicios de AWS mismo tiempo, omitir a los proveedores de servicios de Internet en su ruta de red.

Prácticas recomendadas

- Installing and configuring Couchbase en diferentes plataformas operativas
- Mejores prácticas para implementar Couchbase Server en AWS
- Creating a Couchbase cluster
- Performance best practices para aplicaciones de Couchbase
- Security best practices para Couchbase Server
- Storage best practices para bases de datos de Couchbase Server

Epics

Implemente una EC2 instancia de Amazon para Couchbase Server

Tarea	Descripción	Habilidades requeridas
Abre la EC2 consola de Amazon.	Inicia sesión en la EC2 consola de Amazon Consola de administración de AWSy ábrela.	DevOps ingeniero, administrador de Couchbase
Implemente una EC2 instancia de Amazon.	Lance una EC2 instancia que coincida con las configuraciones del servidor Couchbase local. Para obtener más información sobre cómo implementar una EC2 instancia, consulta Lanzar una EC2 instancia de Amazon en la EC2 documentación de Amazon.	DevOps ingeniero, administrador de Couchbase

Instalar y configurar Couchbase Server en Amazon EC2

Tarea	Descripción	Habilidades requeridas
Instale un clúster de Couchbase.	Revisa las pautas de despliegue de Couchbase Server antes de instalar Couchbase Server en Amazon. EC2 Para instalar Couchbase Server, consulte la documentación de Couchbase Server.	Administrador de Couchbase
Configure el clúster.	Para configurar el clúster, consulte Cluster Configuration	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	Options en la documentación de Couchbase.	

Adición de un nuevo nodo y reequilibrio del clúster de Couchbase

Tarea	Descripción	Habilidades requeridas
Agrega un nodo para la instancia. EC2	Agrega la EC2 instancia recién implementada que tiene Couchbase instalado al clúster local existente. Para obtener instrucciones, consulte Add a Node and Rebalance en la documentación de Couchbase Server.	Administrador de Couchbase
Reequilibre el clúster.	El proceso de reequilibrio convierte al nodo recién agregado con la EC2 instancia en un miembro activo del clúster de Couchbase. Para obtener instrucciones, consulte Add a Node and Rebalance en la documenta ción de Couchbase Server.	Administrador de Couchbase

Reconfiguración de las conexiones

Tarea	Descripción	Habilidades requeridas
Elimine los nodos en las instalaciones y reequilibre.	Ahora puede eliminar los nodos en las instalaciones del clúster. Después de eliminar los nodos, siga el	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	proceso de reequilibrio para redistribuir los datos, los índices, el procesamiento de eventos y el procesamiento de consultas entre los nodos disponibles en el clúster. Para obtener instrucciones, consulte Remove a Node and Rebalance en la documenta ción de Couchbase Server.	
Actualice los parámetros de conexión.	Actualiza los parámetros de conexión de tu aplicación para usar la nueva dirección EC2 IP de Amazon, de modo que tu aplicación pueda conectars e al nuevo nodo.	Desarrollador de aplicaciones de Couchbase

Recursos relacionados

- Couchbase Server Services
- Implemente Couchbase Server mediante AWS Marketplace
- Connect to Couchbase Server
- Administre depósitos
- Cross Data Center Replication (XDCR)
- Acuerdo de licencia de Couchbase Inc.

Información adicional

Ventajas principales

La migración de su base de datos de Couchbase a ella AWS ofrece las siguientes ventajas:

Escalabilidad. Puede ampliar o reducir el tamaño de su clúster de Couchbase en función de la demanda sin tener que gestionar el hardware físico, de forma que pueda adaptarse fácilmente a las fluctuaciones de los volúmenes de datos y al uso de las aplicaciones. AWS proporciona:

- Opciones de escalado horizontal y vertical
- Capacidades de implementación global
- Equilibrio de carga entre Regiones de AWS
- Soluciones de escalado de bases de datos
- Optimización de la entrega de contenido

Optimización del rendimiento. AWS proporciona una infraestructura de red de alto rendimiento y tipos de instancias optimizados para garantizar un acceso rápido a los datos y una baja latencia para su base de datos de Couchbase.

- Opciones de computación de alto rendimiento (HPC)
- Entrega de contenido global a través de Amazon CloudFront
- Múltiples opciones de almacenamiento
- Servicios de bases de datos avanzados, como Amazon Relational Database Service (Amazon RDS) y Amazon DynamoDB
- Conexiones de baja latencia con Direct Connect

Optimización de costos: Seleccione el tipo de instancia y la configuración adecuados para equilibrar el rendimiento y el costo en función de su carga de trabajo. Pague solo por los recursos que utilice. Esto puede reducir potencialmente sus costos operativos al eliminar la necesidad de administrar el hardware local y aprovechar Nube de AWS las economías de escala.

- Las instancias reservadas pueden ayudarlo a planificar con antelación y reducir considerablemente sus costos cuando utiliza Couchbase en AWS.
- El escalado automático evita el sobreaprovisionamiento y lo ayuda a optimizar el uso y la rentabilidad.

Seguridad mejorada Aproveche las sólidas funciones de seguridad incluidas AWS, como el cifrado de datos, los controles de acceso y los grupos de seguridad, para ayudar a proteger los datos confidenciales que almacena en Couchbase. Beneficios adicionales:

- El modelo de responsabilidad AWS compartida diferencia claramente entre la seguridad de la nube (AWS responsabilidad) y la seguridad en la nube (responsabilidad del cliente).
- AWS el cumplimiento respalda los principales estándares de seguridad.
- AWS proporciona opciones de cifrado avanzadas.
- AWS Identity and Access Management (IAM) le ayuda a gestionar el acceso seguro a sus recursos.

Administración simplificada. AWS proporciona servicios gestionados para Couchbase, de forma que pueda centrarse en el desarrollo de aplicaciones en lugar de en gestionar la infraestructura subyacente.

Alcance global. Puede implementar su clúster de Couchbase en varios clústeres Regiones de AWS para lograr una baja latencia para los usuarios de todo el mundo. Puede implementar las bases de datos completamente en la nube o en un entorno híbrido. Puede proteger los datos con una seguridad empresarial integrada y una sincronización bidireccional rápida y eficiente de los datos desde la periferia hasta la nube. Al mismo tiempo, puede simplificar el desarrollo con un modelo de programación coherente para crear aplicaciones web y móviles.

Continuidad empresarial:

- Copia de seguridad y recuperación. Si hubiera algún problema, puede utilizar AWS Backup para garantizar la resiliencia de los datos y una fácil recuperación. Para obtener las opciones de recuperación ante desastres, consulte la documentación del Marco de AWS Well-Architected.
- Despliegue multirregional de Couchbase: para implementar una base de datos de Couchbase en un AWS entorno multirregional, puede suscribirse al servidor de Couchbase en, usar AWS CloudFormationplantillas para crear clústeres de Couchbase independientes en cada región y AWS Marketplace, a continuación, configurar la replicación entre regiones para sincronizar los datos entre las regiones. Esta configuración garantiza una alta disponibilidad y redundancia geográfica en varias regiones. Para obtener más información, consulte Deploy Couchbase Server Using AWS Marketplace en la documentación de Couchbase.

Agilidad de la infraestructura:

- Rápido aprovisionamiento y desaprovisionamiento de recursos
- Alcance de infraestructura global
- Escalado automático en función de la demanda

- Infraestructura como código (IaC) para implementaciones coherentes
- Varios tipos de instancias optimizados para diferentes cargas de trabajo

Habilitación de la innovación:

- Acceso a la tecnología más reciente, como IA y ML, IoT y análisis
- Servicios administrados, que reducen los gastos operativos
- Prácticas de desarrollo de aplicaciones modernas
- Opciones de computación sin servidor

Excelencia operativa:

- Supervisión y registro centralizados
- Administración automatizada de recursos
- Capacidades de mantenimiento predictivo
- Visibilidad mejorada del uso de los recursos
- Procesos de implementación simplificados

Oportunidades de modernización:

- Arquitectura de microservicios
- DevOpsimplementación de prácticas
- Desarrollo de aplicaciones nativas en la nube
- Modernización de aplicaciones heredadas

Ventajas competitivas:

- Tiempo de comercialización más rápido
- Experiencia del cliente mejorada
- Toma de decisiones basada en datos
- Inteligencia empresarial mejorada

Migre Db2 for LUW a Amazon EC2 mediante el envío de registros para reducir el tiempo de interrupción

Feng Cai, Ambarish Satarkar y Saurabh Sharma, Amazon Web Services

Resumen

Cuando los clientes migran sus cargas de trabajo de IBM Db2 for LUW (Linux, UNIX y Windows) a Amazon Web Services (AWS), la forma más rápida es utilizar Amazon Elastic Compute Cloud (Amazon EC2) con el modelo Bring Your Own License (BYOL). Sin embargo, la migración de grandes cantidades de datos de Db2 en las instalaciones a AWS puede ser un desafío, especialmente cuando el periodo de interrupción es corto. Muchos clientes intentan establecer el periodo de interrupción en menos de 30 minutos, lo que deja poco tiempo para la propia base de datos.

Este patrón explica cómo realizar una migración a Db2 con un breve periodo de interrupción mediante el envío del registro de transacciones. Este enfoque se aplica a Db2 en una plataforma Linux little endian.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una instancia de Db2 que se ejecuta en una instancia que coincide con los diseños del EC2 sistema de archivos local
- Un bucket de Amazon Simple Storage Service (Amazon S3) al que pueda acceder la instancia EC2
- Un rol y una política de AWS Identity and Access Management (IAM) para hacer llamadas programáticas a Amazon S3
- Relojes del sistema y zona horaria sincronizados en Amazon EC2 y el servidor local
- La red local conectada a AWS a través de AWS Site-to-Site VPN o AWS Direct Connect

Limitaciones

- La instancia local de Db2 y Amazon EC2 deben estar en la misma familia de plataformas.

- Se debe registrar la carga de trabajo en las instalaciones de Db2. Establezca `blocknonlogged=yes` en la configuración de la base de datos para bloquear cualquier transacción no registrada.

Versiones de producto

- Db2 para LUW, versión 11.5.9 y posteriores

Arquitectura

Pila de tecnología de origen

- Db2 en Linux x86_64

Pila de tecnología de destino

- Amazon EBS
- Amazon EC2
- AWS Identity y Access Management (IAM)
- Amazon S3
- AWS Site-to-Site VPN o Direct Connect

Arquitectura de destino

El siguiente diagrama muestra una instancia de Db2 que se ejecuta localmente con una conexión de red privada virtual (VPN) a Db2 en Amazon. EC2 Las líneas de puntos representan el túnel de VPN entre su centro de datos y la nube de AWS.

Tools (Herramientas)

Servicios de AWS

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.

- AWS Direct Connect vincula su red interna con una ubicación de Direct Connect a través de un cable estándar Ethernet de fibra óptica. Con esta conexión, puede crear interfaces virtuales directamente en servicios públicos de AWS omitiendo a los proveedores de servicios de Internet en su ruta de acceso a la red.
- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento a nivel de bloques para utilizarlos con instancias de Amazon Elastic Compute Cloud (Amazon). EC2
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- La Site-to-SiteVPN de AWS le ayuda a transferir el tráfico entre las instancias que lanza en AWS y su propia red remota.

Otras herramientas

- db2cli es el comando CLI interactivo de Db2.

Prácticas recomendadas

- En la base de datos de destino, utilice los puntos de conexión de puerta de enlace de Amazon S3 para acceder a la imagen de copia de seguridad y a los archivos de registro de la base de datos en Amazon S3.
- En la base de datos de origen, utilice AWS PrivateLink para Amazon S3 para enviar la imagen de respaldo y los archivos de registro de la base de datos a Amazon S3.

Epics

Configuración de las variables de entorno

Tarea	Descripción	Habilidades requeridas
Configure las variables de entorno.	Este patrón utiliza los siguientes nombres:	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	• Nombre de instancia: `db2inst1` • Nombre de la base de datos: `SAMPLE` Puede cambiarlos para adaptarlos a su entorno.	

Configure el servidor Db2 en las instalaciones

Tarea	Descripción	Habilidades requeridas

Configure la CLI de AWS.	Utilice los siguientes comandos para descargar e instalar la versión más reciente de la AWS CLI:
	
	`$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"`
	`unzip awscliv2.zip`
	`sudo ./aws/install`
		Administrador de Linux

Configure un destino en las instalaciones para los registros de archivos de Db2.	Para mantener la base de datos de destino de Amazon EC2 sincronizada con la base de datos de origen local, es necesario recuperar los registros de transacciones más recientes de la fuente. En esta configuración, `/db2logs` se establece como	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	`LOGARCHMETH2` en la fuente como área de almacenam iento provisional. Los registros archivados en este directorio se sincronizarán con Amazon S3 y Db2 en Amazon podrá acceder a ellos. EC2 El patrón usa `LOGARCHMETH2` porque `LOGARCHMETH1` podría haberse configurado para usar una herramienta de un proveedor externo a la que el comando de la CLI de AWS no pudiera acceder. Para recuperar los registros, ejecute el siguiente comando:
	`db2 connect to sample`
	`db2 update db cfg for SAMPLE using LOGARCHMETH2 disk:/db2logs`	

Realice una copia de seguridad de la base de datos en línea.	Haga una copia de seguridad de la base de datos en línea y guárdela en el sistema de archivos de copia de seguridad local: `db2 backup db sample online to /backup`	Administrador de base de datos

Configuración del bucket de S3 y de la política de IAM

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Cree un bucket de S3 para que el servidor en las instalaciones envíe los archivos de registro y las imágenes Db2 de copia de seguridad a AWS. Amazon también accederá al depósito EC2: `aws s3api create-bucket --bucket logshipmig-db2 --region us-east-1`	Administrador de sistemas de AWS
Cree una política de IAM.	El archivo `db2bucket.json` contiene la política de IAM para acceder al bucket de Amazon S3: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "kms:GenerateDataKey", "kms:Decrypt", "s3:PutObject", "s3:GetObject",`	Administrador AWS, administrador de sistemas AWS

Tarea	Descripción	Habilidades requeridas

	<pre>"s3:AbortMultipart
	Upload",
	
	"s3:ListBucket",
	
	"s3:DeleteObject",
	
	"s3:GetObjectVersi
	on",
	
	"s3:ListMultipartU
	ploadParts"
	],
	"Resource":
	[
	
	"arn:aws:s3:::logs
	hipmig-db2/*",
	
	"arn:aws:s3:::logs
	hipmig-db2"
	]
	}
	]
	}</pre> Utilice el siguiente comando de la AWS CLI para crear la política: <pre>aws iam create-policy \
	--policy-name
	db2s3policy \
	--policy-document
	file://db2bucket.j
	son</pre> El resultado de JSON muestra el nombre de recurso de	

Tarea	Descripción	Habilidades requeridas
	Amazon (ARN) para la política, donde `aws_account_id` representa el ID de la cuenta: `"Arn": "arn:aws:iam::aws_account_id:policy/db2s3policy"`	

Tarea	Descripción	Habilidades requeridas
Adjunta la política de IAM a la función de IAM utilizada por la EC2 instancia.	En la mayoría de los entornos de AWS, una EC2 instancia en ejecución tiene un rol de IAM establecido por el administrador del sistema. Si la función de IAM no está configurada, cree la función y elija Modificar la función de IAM en la EC2 consola para asociar la función a la EC2 instancia que aloja la base de datos de Db2. Adjunte la política de IAM al rol de IAM con el ARN de la política: `aws iam attach-role-policy \ --policy-arn "arn:aws:iam::aws_account_id:policy/db2s3policy" \ --role-name db2s3role` Una vez asociada la política, cualquier EC2 instancia asociada a la función de IAM puede acceder al bucket de S3.	Administrador AWS, administrador de sistemas AWS

Envíe los archivos de registro y la imagen de copia de seguridad de la base de datos de origen a Amazon S3

Tarea	Descripción	Habilidades requeridas

Configure la AWS CLI en el servidor de Db2 en las instalaciones.	Configure la AWS CLI con el `Access Key ID` y la `Secret Access Key` que generó en el paso anterior:
	`$ aws configure`
	`AWS Access Key ID [None]: **********`
	`AWS Secret Access Key [None]: ********** **********`
	`Default region name [None]: us-east-1`
	`Default output format [None]: json`
		Administrador AWS, administrador de sistemas AWS

Envíe la imagen de copia de seguridad a Amazon S3.	Anteriormente, se guardó una copia de seguridad de la base de datos en línea en el directorio `/backup` en las instalaciones. Para enviar la imagen de copia de seguridad al bucket de S3, ejecute el siguiente comando: `aws s3 sync /backup s3://logshipmig-db2/SAMPLE_backup`	Administrador de AWS, ingeniero de migraciones
Envíe los registros de archivo Db2 a Amazon S3.	Sincronice los registros del archivo Db2 local con el depósito de S3 al que puede	Administrador de AWS, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	acceder la instancia de Db2 de destino en Amazon: EC2 `aws s3 sync /db2logs s3://logshipmig-db2/ SAMPLE_LOG` Ejecute este comando periódicamente mediante cron u otras herramientas de programación. La frecuenci a depende de la periodicidad con la que la base de datos de origen archiva los archivos de registro de transacciones.	

Conecte Db2 de Amazon EC2 a Amazon S3 e inicie la sincronización de la base de datos

Tarea	Descripción	Habilidades requeridas
Cree un almacén de PKCS12 claves.	Db2 utiliza un almacén de claves de cifrado de estándare s de criptografía de clave pública (PKCS) para mantener la seguridad de la clave de acceso de AWS. Cree un almacén de claves y configure la instancia de Db2 de origen para utilizarlo: `gsk8capicmd_64 -keydb -create -db "/home/db2inst1/.keystore/db2s3.p12" -pw "<password>" -type pkcs12 -stash`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`db2 "update dbm cfg using keystore_location /home/db2inst1/.keystore/db2s3.p12 keystore_type pkcs12"`	

Cree el alias de acceso al almacenamiento de Db2.	Para crear el alias de acceso al almacenamiento, utilice la siguiente sintaxis de script:
	`db2 "catalog storage access alias <alias_name> vendor S3 server <S3 endpoint> container '<bucket_name>'"`
	Por ejemplo, el script podría tener el siguiente aspecto:
	`db2 "catalog storage access alias DB2AWSS3 vendor S3 server s3.us-east-1.amazonaws.com container 'logshipmig-db2'"`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Establece el área de almacenamiento provisional.	De forma predeterminada, Db2 usa `DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH` como área de montaje para cargar y descargar archivos desde y hacia Amazon S3. La ruta predeterminada es `sqllib/tmp/RemoteStorage.xxxx`, en el directorio principal de la instancia, y `xxxx` hace referencia al número de partición de Db2. Tenga en cuenta que el área de montaje debe tener capacidad suficiente para almacenar las imágenes de copia de seguridad y los archivos de registro. Puede usar el registro para apuntar el área de montaje a un directorio diferente. También recomendamos usar `DB2_ENABLE_COS_SDK=ON`, `DB2_OBJECT_STORAGE_SETTINGS=EnableStreamingRestore` y el enlace a la biblioteca de `awssdk` para omitir el área de almacenamiento provisional de Amazon S3 a fin de hacer copias de seguridad de bases de datos y restaurarlas:	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	`#By root:`
	`cp -rp /home/db2inst1/sqllib/lib64/awssdk/RHEL/7.6/* /home/db2inst1/sqllib/lib64/`
	
	`#By db2 instance owner:`
	`db2set DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH=/db2stage`
	`db2set DB2_ENABLE_COS_SDK=ON`
	`Db2set DB2_OBJECT_STORAGE_SETTINGS=EnableStreamingRestore`
	`db2stop`
	`db2start`	

Restaure la base de datos a partir de la imagen de copia de seguridad.	Restaure la base de datos de destino en Amazon EC2 a partir de la imagen de respaldo del bucket S3: `db2 restore db sample from DB2REMOTE://DB2AWSS3/logshipmig-db2/SAMPLE_backup replace existing`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

Restaure la base de datos.	Una vez completada la restauración, la base de datos de destino pasará al estado pendiente de recuperación. Configure `LOGARCHMETH1` y `LOGARCHMETH2` para que Db2 sepa dónde obtener los archivos de registro de transacciones:
	`db2 update db cfg for SAMPLE using LOGARCHMETH1 'DB2REMOTE://DB2AWSS3//SAMPLE_LOGS/'`
	`db2 update db cfg for SAMPLE using LOGARCHMETH2 OFF`
	Inicie la recuperación de la base de datos:
	`db2 ROLLFORWARD DATABASE sample to END OF LOGS`
	Este comando procesa todos los archivos de registro que se han transferido al bucket de S3. Ejecútelo periódicamente en función de la frecuencia del comando `s3 sync` en los servidores Db2 locales. Por ejemplo, si `s3 sync` se ejecuta cada hora y se tarda 10 minutos en sincronizar todos los archivos de registro,
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	configure el comando para que se ejecute 10 minutos después de cada hora.	

Ponga Db2 en Amazon en EC2 línea durante el período de transición

Tarea	Descripción	Habilidades requeridas

Ponga en línea la base de datos de destino.	Durante el periodo de transició n, realice una de las siguiente s acciones:
	• Ponga la base de datos local en `ADMIN MODE` y ejecute el comando `s3 sync` para forzar el archivado del último registro de transacciones.
	• Apague la base de datos.
	
	Una vez sincronizado el último registro de transacciones con Amazon S3, ejecute el comando `ROLLFORWARD` por última vez:
	`db2 rollforward DB sample to END OF LOGS`
	`db2 rollforward DB sample complete`
	
	`Rollforward Status`
	`....`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	`Rollforward status = not pending`
	`....`
	`DB20000I The ROLLFORWARD command completed successfully.`
	
	`db2 activate db sample`
	`DB20000I The ACTIVATE DATABASE command completed successfully.`
	
	Coloque la base de datos de destino en línea y dirija las conexiones de la aplicación a Db2 en Amazon EC2.	

Resolución de problemas

Problema	Solución
Si varias bases de datos tienen el mismo nombre de instancia y nombre de base de datos en diferentes hosts (DEV, QA, PROD), las copias de seguridad y los registros pueden ir al mismo subdirectorio.	Utilice distintos buckets de S3 para DEV, QA y PROD y agregue el nombre de host como prefijo del subdirectorio para evitar confusiones.
Si hay múltiples imágenes de copia de seguridad en la misma ubicación, aparecerá el siguiente error al restaurar: `SQL2522N More than one backup file matches the time stamp value provided for the backed up database image.`	En el comando `restore`, agregue la marca de tiempo de la copia de seguridad: `db2 restore db sample from DB2REMOTE://DB2AWSS3/logshipmig-db2/SAMPLE_backup taken at 20230628164042 replace existing`

Recursos relacionados

- Operaciones de copia de seguridad y restauración de Db2 entre diferentes sistemas operativos y plataformas de hardware
- Configure STORAGE ACCESS ALIAS y REMOTE de Db2 DB2
- Comando Db2 ROLLFORWARD
- Método de archivo de registro secundario de Db2

Migración de Db2 para LUW a Amazon EC2 con recuperación de desastres de alta disponibilidad

Feng Cai, Aruna Gangireddy y Venkatesan Govindan, Amazon Web Services

Resumen

Cuando los clientes migran su carga de trabajo de IBM Db2 de LUW (Linux, UNIX y Windows) a Amazon Web Services (AWS), utilizar Amazon Elastic Compute Cloud (Amazon EC2) con el modelo Traiga su propia licencia (BYOL) es la forma más rápida de hacerlo. Sin embargo, la migración de grandes cantidades de datos de Db2 en las instalaciones a AWS puede ser un desafío, especialmente cuando el periodo de interrupción es corto. Muchos clientes intentan establecer el periodo de interrupción en menos de 30 minutos, lo que deja poco tiempo para la propia base de datos.

Este patrón explica cómo realizar una migración a Db2 con un breve período de interrupción mediante la recuperación de desastres de alta disponibilidad (HADR) de Db2. Este enfoque se aplica a las bases de datos Db2 que se encuentran en la plataforma Linux Little-Endian y no utilizan la característica de particionamiento de datos (DPF).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una instancia de Db2 que se ejecute en una instancia de Amazon EC2 que coincida con los diseños del sistema de archivos en las instalaciones
- Un bucket de Amazon Simple Storage Service (Amazon S3) accesible para la instancia EC2
- Un rol y una política de AWS Identity and Access Management (IAM) para hacer llamadas programáticas a Amazon S3
- Relojes del sistema y zona horaria sincronizados en Amazon EC2 y el servidor en las instalaciones
- La red local conectada a AWS a través de AWS Site-to-Site VPN o AWS Direct Connect
- Comunicación entre el servidor en las instalaciones y Amazon EC2 en los puertos HADR

Limitaciones

- La instancia en las instalaciones de Db2 y Amazon EC2 deben estar en la misma familia de plataformas.

- El HADR no se admite en un entorno de base de datos particionado.
- HADR no admite el uso de archivos sin procesar I/O (acceso directo al disco) para los archivos de registro de la base de datos.
- HADR no admite registros infinitos.
- `LOGINDEXBUILD` debe configurarse como `YES`, lo que aumentará el uso del registro para reconstruir el índice.
- Se debe registrar la carga de trabajo en las instalaciones de Db2. Configure `blocknonlogged=yes` en la configuración de la base de datos para bloquear cualquier transacción no registrada.

Versiones de producto

- Db2 para LUW, versión 11.5.9 y posteriores

Arquitectura

Pila de tecnología de origen

- Db2 en Linux x86_64

Pila de tecnología de destino

- Amazon EC2
- AWS Identity y Access Management (IAM)
- Amazon S3
- Site-to-SiteVPN DE AWS

Arquitectura de destino

En el siguiente diagrama, Db2 en las instalaciones se ejecuta `db2-server1` como principal. Tiene dos objetivos HADR en espera. Hay un objetivo de reserva en las instalaciones y es opcional. El otro objetivo en espera, `db2-ec2`, está en Amazon EC2. Después de efectuar la transición de la base de datos a AWS, `db2-ec2` se convierte en la principal.

1. Los registros se transmiten desde la base de datos en las instalaciones principal a la base de datos en las instalaciones en espera.
2. Con el HADR de Db2, los registros se transmiten desde la base de datos local principal a través de una Site-to-Site VPN a Db2 en Amazon EC2.
3. Los registros de copia de seguridad y archivo de Db2 se envían desde la base de datos en las instalaciones principal al bucket de S3 en AWS.

Tools (Herramientas)

Servicios de AWS

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- AWS Direct Connect vincula su red interna con una ubicación de Direct Connect a través de un cable estándar Ethernet de fibra óptica. Con esta conexión, puede crear interfaces virtuales directamente en servicios públicos de AWS omitiendo a los proveedores de servicios de Internet en su ruta de acceso a la red.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- La Site-to-SiteVPN de AWS le ayuda a transferir el tráfico entre las instancias que lanza en AWS y su propia red remota.

Otras herramientas

- db2cli es el comando CLI interactivo de Db2.

Prácticas recomendadas

- En la base de datos de destino, utilice los puntos de conexión de puerta de enlace de Amazon S3 para acceder a la imagen de copia de seguridad y a los archivos de registro de la base de datos en Amazon S3.
- En la base de datos de origen, utilice AWS PrivateLink para Amazon S3 para enviar la imagen de respaldo y los archivos de registro de la base de datos a Amazon S3.

Epics

Configuración de las variables de entorno

Tarea	Descripción	Habilidades requeridas
Configure las variables de entorno.	Este patrón utiliza los siguientes nombres y puertos: 1. Nombre de host en las instalaciones de Db2: `db2-server1` 2. Nombre de host en espera de HADR: `db2-server2` (si HADR se está ejecutando actualmente en las instalaciones) 3. Nombre de host de Amazon EC2: `db2-ec2` 4. Nombre de instancia: `db2inst1` 5. Nombre de la base de datos: `SAMPLE` 6. Puertos HDR: • `db2-server1: 50010` • `db2-server2: 50011` • `db2-ec2: 50012`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Puede cambiarlos para adaptarlos a su entorno.	

Configure el servidor Db2 en las instalaciones

Tarea	Descripción	Habilidades requeridas

Configure AWS CLI.	Utilice los siguientes comandos para descargar e instalar la versión más reciente de la AWS CLI:
	`$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"`
	`unzip awscliv2.zip`
	`sudo ./aws/install`
		Administrador de Linux

Configure un destino en las instalaciones para los registros de archivos de Db2.	Condiciones como los trabajos por lotes de actualización intensiva y la ralentización de la red pueden provocar un retraso en el servidor HADR en espera. Para ponerse al día, el servidor en espera necesita los registros de transacciones del servidor principal. La secuencia de lugares de los registros de solicitud es la siguiente: • El directorio de registro activo del servidor principal	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	• La ubicación LOGARCHME TH1 o LOGARCHMETH2 en el servidor en espera
	• La ubicación LOGARCHME TH1 o LOGARCHMETH2 en el servidor principal
	
	En esta configuración, /db2logs se establece como LOGARCHMETH2 en la fuente como área de almacenam iento provisional. Los registros archivados en este directorio se sincronizarán con Amazon S3 y Db2 accederá a ellos desde Amazon EC2. El patrón utiliza LOGARCHMETH2 porque LOGARCHMETH1 podría haberse configurado para usar una herramienta de un proveedor externo a la que el comando de la AWS CLI no pudiera acceder:
	
	`db2 connect to sample`
	`db2 update db cfg for SAMPLE using LOGARCHME TH2 disk:/db2logs`	

Tarea	Descripción	Habilidades requeridas
Realice una copia de seguridad de la base de datos en línea.	Haga una copia de seguridad de la base de datos en línea y guárdela en el sistema de archivos de copia de seguridad local: `db2 backup db sample online to /backup`	Administrador de base de datos

Configuración del bucket de S3 y de la política de IAM

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Cree un bucket de S3 para que el servidor en las instalaciones envíe los archivos de registro y las imágenes Db2 de copia de seguridad a AWS. Amazon EC2 accederá al bucket: `aws s3api create-bucket --bucket hadrmig-db2 --region us-east-1`	Administrador de AWS
Cree una política de IAM.	El archivo `db2bucket.json` contiene la política de IAM para obtener acceso al bucket de S3: `{ "Version": "2012-10-17", "Statement": [ {`	Administrador AWS, administrador de sistemas AWS

Tarea	Descripción	Habilidades requeridas
	"Effect": "Allow", "Action": ["kms:GenerateDataKey", "kms:Decrypt", "s3:PutObject", "s3:GetObject", "s3:AbortMultipartUpload", "s3:ListBucket", "s3:DeleteObject", "s3:GetObjectVersion", "s3:ListMultipartUploadParts"], "Resource": ["arn:aws:s3:::hadrmig-db2/*", "arn:aws:s3:::hadrmig-db2"] }] }	

Tarea	Descripción	Habilidades requeridas

	Utilice el siguiente comando de la AWS CLI para crear la política:
	
	`aws iam create-policy \ --policy-name db2s3hapolicy \ --policy-document file://db2bucket.json`
	
	El resultado de JSON muestra el nombre de recurso de Amazon (ARN) para la política, donde `aws_account_id` representa el ID de la cuenta:
	
	`"Arn": "arn:aws:iam::aws_account_id:policy/db2s3hapolicy"`	

Tarea	Descripción	Habilidades requeridas
Adjunte la política de IAM al rol de IAM.	Por lo general, la instancia de EC2 con Db2 en ejecución tendría un rol de IAM asignado por el administr ador de sistemas. Si no se ha asignado ningún rol de IAM, puede elegir Modificar rol de IAM en la consola de Amazon EC2. Adjunte la política de IAM al rol de IAM asociado a la instancia de EC2. Después de adjuntar la política, la instancia de EC2 puede acceder al bucket de S3: `aws iam attach-role-policy --policy-arn "arn:aws:iam::aws_account_id:policy/db2s3hapolicy" --role-name db2s3harole`	

Envíe los archivos de registro y la imagen de copia de seguridad de la base de datos de origen a Amazon S3

Tarea	Descripción	Habilidades requeridas
Configure AWS CLI en el servidor Db2 en las instalaci ones.	Configure la AWS CLI con el `Access Key ID` y la `Secret Access Key` que generó anteriormente: `$ aws configure`	Administrador AWS, administr ador de sistemas AWS

Tarea	Descripción	Habilidades requeridas
	`AWS Access Key ID [None]: ************ AWS Secret Access Key [None]: ********* ********** Default region name [None]: us-east-1 Default output format [None]: json`	
Envíe la imagen de copia de seguridad a Amazon S3.	Anteriormente, se guardó una copia de seguridad de la base de datos en línea en el directorio `/backup` en las instalaciones. Para enviar la imagen de copia de seguridad al bucket de S3, ejecute el siguiente comando: `aws s3 sync /backup s3://hadrmig-db2/SAMPLE_backup`	Administrador AWS, administrador de sistemas AWS

Tarea	Descripción	Habilidades requeridas
Envíe los registros de archivo Db2 a Amazon S3.	Sincronice los registros del archivo de Db2 en las instalaciones con el bucket de Amazon S3 al que puede acceder la instancia de Db2 de destino en Amazon EC2: `aws s3 sync /db2logs s3://hadrmig-db2/SAMPLE_LOGS` Ejecute este comando periódicamente mediante cron u otras herramientas de programación. La frecuencia depende de la periodicidad con la que la base de datos de origen archiva los archivos de registro de transacciones.	

Conecte Db2 de Amazon EC2 a Amazon S3 e inicie la sincronización inicial de la base de datos

Tarea	Descripción	Habilidades requeridas
Cree un PKCS12 almacén de claves.	Db2 utiliza un almacén de claves de cifrado de estándares de criptografía de clave pública (PKCS) para mantener la seguridad de la clave de acceso de AWS. Cree un almacén de claves y configure la Db2 de origen para que lo use:	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	`gsk8capicmd_64 -keydb -create -db "/home/db2inst1/.keystore/db2s3.p12" -pw "<password>" -type pkcs12 -stash`
	
	`db2 "update dbm cfg using keystore_location /home/db2inst1/.keystore/db2s3.p12 keystore_type pkcs12"`	

Tarea	Descripción	Habilidades requeridas

Cree el alias de acceso al almacenamiento de Db2.	Db2 usa un alias de acceso al almacenamiento para acceder a Amazon S3 directamente con los comandos `INGEST`, `LOAD`, `BACKUP DATABASE` o `RESTORE DATABASE`.
	
	Como ha asignado un rol de IAM a la instancia de EC2, `USER` y `PASSWORD` no son necesarios:
	
	`db2 "catalog storage access alias <alias_name> vendor S3 server <S3 endpoint> container '<bucket_name>'"`
	
	Por ejemplo, el script podría tener el siguiente aspecto:
	
	`db2 "catalog storage access alias DB2AWSS3 vendor S3 server s3.us-east-1.amazonaws.com container 'hadrmig-db2'"`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

Establece el área de almacenamiento provisional.	Recomendamos usar `DB2_ENABLE_COS_SDK=ON` , `DB2_OBJECT_STORAGE_SETTINGS=EnableStreamingRestore` y el enlace a la biblioteca de `awssdk` para omitir el área de almacenamiento provisional de Amazon S3 a fin de hacer copias de seguridad de bases de datos y restaurarlas:
	`#By root:`
	`cp -rp /home/db2inst1/sqllib/lib64/awssdk/RHEL/7.6/* /home/db2inst1/sqllib/lib64/`
	
	`#By db2 instance owner:`
	`db2set DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH=/db2stage`
	`db2set DB2_ENABLE_COS_SDK=ON`
	`db2set DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH=/db2stage`
	`db2stop`
	`db2start`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

Restaure la base de datos a partir de la imagen de copia de seguridad.	Restaure la base de datos de destino en Amazon EC2 a partir de la imagen de copia de seguridad del bucket de S3:
	
	`db2 create db sample on /data1`
	`db2 restore db sample from DB2REMOTE://DB2AWSS3/hadrmig-db2/SAMPLE_backup replace existing`
		Administrador de base de datos

Configurar HADR sin HADR en las instalaciones

Tarea	Descripción	Habilidades requeridas
Configure el servidor Db2 en las instalaciones como el principal.	Actualice los ajustes de configuración de la base de datos para el HADR en `db2-server1` (la fuente en las instalaciones) como principal. Establezca `HADR_SYNCMODE` en el modo `SUPERASYNC`, que tiene el menor tiempo de respuesta a las transacciones: `db2 update db cfg for sample using HADR_LOCAL_HOST db2-server1 HADR_LOCAL_SVC 50010 HADR_REMOTE_HOST db2-ec2 HADR_REMOTE_SVC 50012 HADR_REMO`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`TE_INST db2inst1 HADR_SYNCMODE SUPERASYNC DB20000 I The UPDATE DATABASE CONFIGURATION command completed successfu lly` Se esperan algunos retrasos en la red entre el centro de datos en las instalaciones y AWS. (Puede establecer un valor `HADR_SYNCMODE` diferente en función de la fiabilidad de la red. Para obtener más informaci ón, consulte la sección de Recursos relacionados.	
Cambie el destino del archivo de registro de la base de datos de destino.	Cambie el destino del archivo de registros de la base de datos de destino para que coincida con el entorno de Amazon EC2: `db2 update db cfg for SAMPLE using LOGARCHME TH1 'DB2REMOTE://DB2AW SS3//SAMPLE_LOGS/' LOGARCHMETH2 OFF DB20000I The UPDATE DATABASE CONFIGURA TION command completed successfully`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Configure HADR para Db2 en el servidor Amazon EC2.	Actualice la configuración de la base de datos para el HADR en `db2-ec2` como modo de espera: `db2 update db cfg for sample using HADR_LOCAL_HOST db2-ec2 HADR_LOCAL_SVC 50012 HADR_REMOTE_HOST db2-server1 HADR_REMOTE_SVC 50010 HADR_REMOTE_INST db2inst1 HADR_SYNCMODE SUPERASYNC DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

Verifique la configuración de HADR.	Compruebe los parámetros del HADR en los servidores Db2 de origen y destino.
	
	Ejecute el siguiente comando para verificar la configuración en `db2-server1` :
	
	`db2 get db cfg for sample|grep HADR`
	`HADR database role = PRIMARY`
	`HADR local host name (HADR_LOCAL_HOST) = db2-server1`
	`HADR local service name (HADR_LOCAL_SVC) = 50010`
	`HADR remote host name (HADR_REMOTE_HOST) = db2-ec2`
	`HADR remote service name (HADR_REMOTE_SVC) = 50012`
	`HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1`
	`HADR timeout value (HADR_TIMEOUT) = 120`
	`HADR target list (HADR_TARGET_LIST) =`
	`HADR log write synchronization mode`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	(HADR_SYNCMODE) = NEARSYNC
	HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000)
	HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0
	HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0
	HADR SSL certificate label (HADR_SSL_LABEL) =
	HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF
	
	Ejecute el siguiente comando para verificar la configuración en `db2-ec2`:
	
	`db2 get db cfg for sample|grep HADR`
	`HADR database role = STANDBY`
	`HADR local host name (HADR_LOCAL_HOST) = db2-ec2`
	`HADR local service name (HADR_LOCAL_SVC) = 50012`
	`HADR remote host name (HADR_REMOTE_HOST) = db2-server1`	

Tarea	Descripción	Habilidades requeridas
	HADR remote service name (HADR_REMOTE_SVC) = 50010 HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1 HADR timeout value (HADR_TIMEOUT) = 120 HADR target list (HADR_TARGET_LIST) = HADR log write synchronization mode (HADR_SYNCMODE) = SUPERASYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certificate label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF Los parámetros HADR_LOCAL_HOST , HADR_LOCAL_SVC , HADR_REMOTE_HOST y HADR_REMO	

Tarea	Descripción	Habilidades requeridas
	TE_SVC indican una configuración de HADR principal y otra de reserva.	

Inicie la instancia HADR de Db2.	Inicie primero la instancia de HADR de Db2 en el servidor en espera db2-ec2:
	`db2 start hadr on db sample as standby`
	`DB20000I The START HADR ON DATABASE command completed successfully.`
	Inicie el HADR de Db2 en el servidor principal (de origen) db2-server1 :
	`db2 start hadr on db sample as primary`
	`DB20000I The START HADR ON DATABASE command completed successfully.`
	La conexión HADR entre Db2 en las instalaciones y Amazon EC2 ya se ha establecido correctamente. El servidor principal de Db2 db2-server1 comienza a transmitir los registros de transacciones a db2-ec2 en tiempo real.
		Administrador de base de datos

Configure HADR cuando HADR exista en las instalaciones

Tarea	Descripción	Habilidades requeridas
Añada Db2 en Amazon EC2 como reserva auxiliar.	Si el HADR se ejecuta en la instancia de Db2 en las instalaciones, puede agregar Db2 en Amazon EC2 como auxiliar en espera con `HADR_TARGET_LIST` mediante la ejecución de los siguientes comandos en `db2-ec2`: `db2 update db cfg for sample using HADR_LOCAL_HOST db2-ec2 HADR_LOCAL_SVC 50012 HADR_REMOTE_HOST db2-server1 HADR_REMOTE_SVC 50010 HADR_REMOTE_INST db2inst1 HADR_SYNCMODE SUPERASYNC DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. db2 update db cfg for sample using HADR_TARGET_LIST "db2-server1:50010|db2-server2:50011" DB20000I The UPDATE DATABASE CONFIGURATION command`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`completed successfully.`	

Tarea	Descripción	Habilidades requeridas
Agregue la información auxiliar en espera a los servidores en las instalaciones.	Actualice `HADR_TARGET_LIST` en los dos servidores en las instalaciones (principal y en espera). En `db2-server1`, ejecute el siguiente código: `db2 update db cfg for sample using HADR_TARGET_LIST "db2-server2:50011|db2-ec2:50012" DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. SQL1363W One or more of the parameters submitted for immediate modification were not changed dynamically. For these configuration parameters, the database must be shutdown and reactivated before the configuration parameter changes become effective.`  En `db2-server2`, ejecute el siguiente código:  `db2 update db cfg for sample using HADR_TARG`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	ET_LIST "db2-serv er1:50010|db2-ec2: 50012" DB20000I The UPDATE DATABASE CONFIGURATION command completed successfu lly. SQL1363W One or more of the parameter s submitted for immediate modificat ion were not changed dynamically. For these configura tion parameters, the database must be shutdown and reactivated before the configuration parameter changes become effective.	

Tarea	Descripción	Habilidades requeridas

Verifique la configuración de HADR.	Compruebe los parámetros del HADR en los servidores Db2 de origen y destino.
	
	En `db2-server1` , ejecute el siguiente código:
	
	`db2 get db cfg for sample|grep HADR`
	`HADR database role = PRIMARY`
	`HADR local host name (HADR_LOCAL_HOST) = db2-server1`
	`HADR local service name (HADR_LOCAL_SVC) = 50010`
	`HADR remote host name (HADR_REMOTE_HOST) = db2-server2`
	`HADR remote service name (HADR_REMOTE_SVC) = 50011`
	`HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1`
	`HADR timeout value (HADR_TIMEOUT) = 120`
	`HADR target list (HADR_TARGET_LIST) = db2-server2:50011|db2-ec2:50012`	

Tarea	Descripción	Habilidades requeridas
	HADR log write synchronization mode (HADR_SYNCMODE) = NEARSYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certificate label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF En `db2-server2`, ejecute el siguiente código: `db2 get db cfg for sample|grep HADR` HADR database role = STANDBY HADR local host name (HADR_LOCAL_HOST) = db2-server2 HADR local service name (HADR_LOCAL_SVC) = 50011 HADR remote host name (HADR_REMOTE_HOST) = db2-server1	

Tarea	Descripción	Habilidades requeridas
	``` HADR remote service name (HADR_REMOTE_SVC) = 50010 HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1 HADR timeout value (HADR_TIMEOUT) = 120 HADR target list (HADR_TAR GET_LIST) = db2-serve r1:50010|db2-ec2:5 0012 HADR log write synchronization mode (HADR_SYNCMODE) = NEARSYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REP LAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certifica te label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF ``` En `db2-ec2`, ejecute el siguiente código:	

Tarea	Descripción	Habilidades requeridas

	`db2 get db cfg for sample|grep HADR`
	`HADR database role = STANDBY`
	`HADR local host name (HADR_LOCAL_HOST) = db2-ec2`
	`HADR local service name (HADR_LOCAL_SVC) = 50012`
	`HADR remote host name (HADR_REMOTE_HOST) = db2-server1`
	`HADR remote service name (HADR_REMOTE_SVC) = 50010`
	`HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1`
	`HADR timeout value (HADR_TIMEOUT) = 120`
	`HADR target list (HADR_TARGET_LIST) = db2-server1:50010|db2-server2:50011`
	`HADR log write synchronization mode (HADR_SYNCMODE) = SUPERASYNC`
	`HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000)`	

Tarea	Descripción	Habilidades requeridas
	``` HADR log replay delay (seconds) (HADR_REP LAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certifica te label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF ``` Los parámetros `HADR_LOCA L_HOST` , `HADR_LOCA L_SVC` , `HADR_REMO TE_HOST` , `HADR_REMO TE_SVC` y `HADR_TARG ET_LIST` indican una configuración de HADR principal y otra en espera.	

Tarea	Descripción	Habilidades requeridas

Detenga e inicie el Db2 HADR.	`HADR_TARGET_LIST` ya está configurado en los tres servidores. Cada servidor Db2 conoce los otros dos. Detenga y reinicie el HADR (interrup ción breve) para aprovechar la nueva configuración.
	
	En `db2-server1` , ejecute los siguientes comandos:
	
	`db2 stop hadr on db sample`
	`db2 deactivate db sample`
	`db2 activate db sample`
	
	En `db2-server2` , ejecute los siguientes comandos:
	
	`db2 deactivate db sample`
	`db2 start hadr on db sample as standby`
	`SQL1766W The command completed successfully`
	
	En `db2-ec2`, ejecute los siguientes comandos:
	
	`db2 start hadr on db sample as standby`
	`SQL1766W The command completed successfully`
	
	En `db2-server1` , ejecute los siguientes comandos:
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	`db2 start hadr on db sample as primary`
	`SQL1766W The command completed successfully`
	
	La conexión HADR entre Db2 en las instalaciones y Amazon EC2 ya se ha establecido correctamente. El servidor principal de Db2 `db2-server1` comienza a transmitir los registros de transacciones a `db2-server2` y `db2-ec2` en tiempo real.	

Haga que Db2 en Amazon EC2 sea principal durante la ventana de transición

Tarea	Descripción	Habilidades requeridas
Asegúrese de que no haya ningún retraso HADR en el servidor en espera.	Compruebe el estado del HADR desde el servidor principal. `db2-server1` No se alarme cuando `HADR_STATE` esté en estado `REMOTE_CATCHUP`, lo cual es normal cuando `HADR_SYNCMODE` está configurado en `SUPERASYNC`. `PRIMARY_LOG_TIME` y `STANDBY_REPLAY_LOG_TIME` muestran que están sincronizados: `db2pd -hadr -db sample`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	HADR_ROLE = PRIMARY REPLAY_TYPE = PHYSICAL HADR_SYNCMODE = SUPERASYNC STANDBY_ID = 2 LOG_STREAM_ID = 0 HADR_STATE = REMOTE_CATCHUP ..... PRIMARY_LOG_TIME = 10/26/2022 02:11:32.000000 (1666750292) STANDBY_LOG_TIME = 10/26/2022 02:11:32.000000 (1666750292) STANDBY_REPLAY_LOG_TIME = 10/26/2022 02:11:32.000000 (1666750292)	

Tarea	Descripción	Habilidades requeridas

Ejecute la adquisición HADR.	Para completar la migración , especifique `db2-ec2` como la base de datos principal ejecutando el comando de adquisición de HADR. Utilice el comando db2pd para verificar el valor `HADR_ROLE` :
	
	`db2 TAKEOVER HADR ON DATABASE sample`
	`DB20000I The TAKEOVER HADR ON DATABASE command completed successfully.`
	
	`db2pd -hadr -db sample`
	`Database Member 0 -- Database SAMPLE -- Active -- Up 0 days 00:03:25 -- Date 2022-10-26-02.46.45.048988`
	
	`HADR_ROLE = PRIMARY`
	
	`REPLAY_TYPE = PHYSICAL`
	
	Para completar la migración a AWS, dirija las conexiones de la aplicación a Db2 en Amazon EC2.	

Resolución de problemas

Problema	Solución
Si utiliza la NAT por motivos de seguridad y firewall, el host puede tener dos direccion es IP (una interna y otra externa), lo que puede provocar un error de comprobación de dirección IP del HADR. El comando `START HADR ON DATABASE` devolverá el siguiente mensaje: `HADR_LOCAL_HOST:HADR_LOCAL_SVC (-xx-xx-xx-xx.:50011 (xx.xx.xx .xx:50011)) on remote database is different from HADR_REMOTE_HOST:H ADR_REMOTE_SVC (xx-xx-xx- xx.:50011 (x.x.x.x:50011)) on local database.`	Para admitir el HADR en un entorno NAT, puede configurar el `HADR_LOCAL_HOST` con la dirección interna y externa. Por ejemplo, si el servidor Db2 tiene el nombre interno `host1` y el nombre externo `host1E`, `HADR_LOCA L_HOST` puede ser. `HADR_LOCAL_HOST: "host1 | host1E"`

Recursos relacionados

- Operaciones de copia de seguridad y restauración de Db2 entre diferentes sistemas operativos y plataformas de hardware
- Configure Db2 STORAGE ACCESS ALIAS y REMOTE DB2
- Recuperación de desastres de alta disponibilidad de Db2
- hadr_syncmode: modo de sincronización HADR para escrituras de registros en un parámetro de configuración de estado del mismo nivel

Migre IIS-hosted aplicaciones a Amazon EC2 mediante appcmd.exe

Deepak Kumar, Amazon Web Services

Resumen

Al migrar aplicaciones alojadas en Internet Information Services (IIS) a instancias de Amazon Elastic Compute Cloud (Amazon EC2), tiene que abordar distintos desafíos de autenticación. Estos desafíos incluyen volver a ingresar las credenciales de dominio para las identidades de los grupos de aplicaciones y, posiblemente, regenerar las claves de las máquinas para que el sitio web funcione correctamente. Este patrón describe un enfoque de migración limpio que utiliza la funcionalidad de copia de seguridad y restauración de IIS en instancias de Amazon EC2. El enfoque utiliza appcmd.exe para desinstalar y volver a instalar IIS en las instancias Amazon EC2 de destino, lo que permite una migración correcta de IIS-hosted sitios web, identidades de grupos de aplicaciones y claves de máquina.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS para el servidor de destino.
- Un servidor de IIS de origen funcional con sitios web alojados en él.
- Comprensión de los principios de funcionamiento del IIS, como la administración y la configuración.
- Acceso de administrador de sistemas tanto en el servidor de origen como en el de destino.
- Se completó la migración del servidor IIS de origen al de destino Cuenta de AWS. Puede utilizar herramientas de migración AWS Transform MGN, como un enfoque basado en instantáneas de Amazon Machine Image (AMI) u otras herramientas de migración.
- Windows Server 2012 R2 o posterior en los servidores de origen y destino.
- Microsoft.NET Framework 4.5 o posterior instalado en ambos servidores (necesario para las operaciones del contenedor de claves de aspnet_regiis.exe)
- Método para transferir archivos de copia de seguridad y archivos XML clave exportados del servidor de origen al de destino, como Amazon Simple Storage Service (Amazon S3), una unidad de red compartida o una copia segura.
- Las instancias de IIS de origen y de destino deben ejecutar la misma versión de IIS (8.5 o 10.0).

Limitaciones

- Algunas Servicios de AWS no están disponibles en todas Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- IIS 8.5 o IIS 10.0

Arquitectura

Pila de tecnología de origen

- Windows Server con IIS 8.5 o IIS 10.0 instalado

Pila de tecnología de destino

- Windows Server con IIS 8.5 o IIS 10.0 instalado
- AWS Transform MGN

Arquitectura de destino

En el siguiente diagrama se muestran los componentes de la arquitectura y el flujo de trabajo de esta aplicación.

La solución incluye los siguientes pasos:

1. Instale y configure el agente de AWS replicación en el servidor IIS de origen de su centro de datos corporativo. Este agente inicia el proceso de replicación y administra la transferencia de datos a AWS.
2. El agente de AWS replicación establece una conexión segura con MGN y comienza a replicar los datos del servidor de origen, incluidas las configuraciones de IIS, los sitios web y los archivos de aplicaciones.
3. MGN lanza instancias de Amazon EC2 en la subred de aplicaciones con los datos replicados. La instancia Amazon EC2 de destino ejecuta IIS y contiene las aplicaciones migradas con sus

volúmenes de Amazon Elastic Block Store (Amazon EBS) asociados. Tras la replicación inicial, MGN continúa sincronizando los cambios hasta que esté listo para pasarse al nuevo entorno.

Tools (Herramientas)

Servicios de AWS

- AWS Transform MGNle ayuda a realojar (levantar y trasladar) las aplicaciones a una ubicación Nube de AWS sin cambios y con un tiempo de inactividad mínimo.
- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento de nivel de bloque para su uso con instancias de Amazon EC2.
- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.

Otras herramientas

- Internet Information Services (IIS) para Windows Server es un servidor web con una arquitectura abierta y escalable que permite alojar cualquier elemento de la Web. IIS proporciona un conjunto de herramientas de administración, que incluyen herramientas de administración y de línea de comandos (por ejemplo, appcmd.exe), API de código administrado y secuencias de comandos, y compatibilidad con Windows PowerShell .

Prácticas recomendadas

- Proteja los archivos de claves exportados: los archivos XML que contienen las claves privadas exportadas deben transferirse de forma segura (cifrados durante el tránsito) y eliminarse de los servidores de origen y destino tras una migración satisfactoria.
- Realice pruebas en un entorno que no sea de producción: realice el procedimiento de copia de seguridad y restauración en un servidor de prueba antes de ejecutarlo en producción.
- Documente las identidades del grupo de aplicaciones: antes de la migración, registre todas las credenciales de identidad del grupo de aplicaciones, ya que debe volver a introducir las contraseñas después de la restauración.
- Realice copias de seguridad de los certificados SSL por separado: la copia de seguridad de appcmd.exe no incluye los certificados SSL ni TLS. Expórtelos por separado mediante el complemento Certificados (MMC) o PowerShell

- Compruebe los archivos de contenido web: la copia de seguridad de la configuración de IIS no incluye los archivos de aplicaciones web (contenido wwwroot). Asegúrese de que se migren con la imagen del servidor integrada. AWS Transform MGN

Epics

Copia de seguridad de IIS en el origen antes de la migración

Tarea	Descripción	Habilidades requeridas
Cree copias de seguridad de los IIS-hosted sitios web, la clave de configuración y `WAS` la clave.	Para crear copias de seguridad para IIS-hosted sitios web, utilice la clave de configuración (`iisWasKey`) y la `WAS` clave () en el servidor de origen. `iisConfig urationKey` appcmd.exe Utilice los siguientes pasos: 1. Abra un símbolo del sistema como administr ador. 2. Ejecute el comando siguiente: `cd c:\window s\system32\inetsrv` 3. Ejecute el siguiente comando, pero reemplace `<backupname>` por su valor: `appcmd.exe add backup "<backupn ame>` Para exportar la clave de configuración y la clave `WAS`, haga lo siguiente:	Administrador de IIS

Tarea	Descripción	Habilidades requeridas
	1. Cree el directorio de exportación: `mkdir C:\temp` 2. Ejecute el comando siguiente: `cd c:\windows\Microsoft.NET\Framework64\v4.0.30319` 3. Ejecute el comando siguiente: `aspnet_regiis.exe -px "iisConfigurationKey" C:\temp\iisConfKey.xml -pri` 4. Ejecute el comando siguiente: `aspnet_regiis.exe -px "iisWasKey" C:\temp\iisWasKey.xml -pri`	

Desinstalación y reinstalación de IIS en el servidor de destino

Tarea	Descripción	Habilidades requeridas
Desinstale IIS en el servidor de destino.	Para desinstalar IIS en el servidor de destino, siga estos pasos: 1. Inicie sesión en el servidor con derechos de administrador. 2. Vaya a Server manager.	Administrador de IIS

Tarea	Descripción	Habilidades requeridas
	3. Elija Manage, Remove Roles and features, Next y, a continuación, Next. 4. Desactive la casilla Servidor web (IIS) y, a continuac ión, seleccione Siguiente y Siguiente. 5. Seleccione la casilla Restart destination server automatic ally. Cuando se complete el proceso de desinstalación, el sistema se reiniciará. 6. Compruebe que IIS se haya desinstalado correctam ente. Para ello, vaya a `C: \Windows\System3 2\inetsrv` y confirme que la carpeta esté vacía.	

Tarea	Descripción	Habilidades requeridas
Instale IIS en el servidor de destino.	Para instalar IIS en el servidor de destino, siga estos pasos: 1. Inicie sesión en el servidor con derechos de administrador. 2. Vaya a Server manager. 3. Elija Add roles and features, Next, Next, Next y, a continuación, Next. 4. Seleccione la casilla Webserver IIS. Cuando se le pida, elija Add features. 5. Seleccione todas las casillas de verificación que aparecen en Desarrollo de aplicaciones, Añadir funciones y Seleccionar todas las funciones. Puede seleccionar las caracterí sticas de forma detallada justo antes de la confirmac ión. 6. Elija Instalar.	Administrador de IIS

Restauración de la configuración y los sitios web de IIS desde las copias de seguridad

Tarea	Descripción	Habilidades requeridas
Restaure la configuración y los sitios web de IIS.	Para restaurar las copias de seguridad de IIS que creó desde el servidor de origen	Administrador de IIS

Tarea	Descripción	Habilidades requeridas
	en el servidor de destino, siga estos pasos: 1. Cree una carpeta con un nombre `backup` en la `C:\windows\system32\inetsrv` carpeta y, a continuación, coloque la carpeta de copia de seguridad de origen en ella. 2. Abra un símbolo del sistema y ejecútelo como administrador. 3. Ejecute el comando siguiente: `cd C:\windows\system32\inetsrv` 4. Ejecute el comando siguiente: `C:\windows\system32\inetsrv\appcmd.exe list backup` 5. Ejecute el comando siguiente: `C:\windows\system32\inetsrv\appcmd.exe restore backup <sourcebackup>` 6. Ejecute el comando siguiente: `cd c:\windows\Microsoft.NET\Framework64\v4.0.30319`	

Tarea	Descripción	Habilidades requeridas
	7. Ejecute el comando siguiente: `aspnet_regiis.exe -pi "iisConfigurationKey" C:\temp\iisConfKey.xml -exp` 8. Ejecute el comando siguiente: `aspnet_regiis.exe -pi "iisWasKey" C:\temp\iisWasKey.xml -exp` 9. Reinicie IIS y vaya a la configuración avanzada Application Pool Identity and Website para volver a ingresar la contraseña. 10. Abra el Administrador de IIS y compruebe que se hayan restaurado todos los sitios web, grupos de aplicaciones y directorios virtuales. 11. Navegue hasta cada sitio web para confirmar que está publicando el contenido correctamente. 12. Tras confirmar que la restauración se ha realizado correctamente, elimine los archivos clave exportados de `C:\temp`: `del C:\temp\iisConfKey.xml`	

Tarea	Descripción	Habilidades requeridas
	`del C:\temp\isWasKey.xml`	

Recursos relacionados

AWS documentación

- Instalación del agente de AWS replicación (AWS Transform MGN documentación)

AWS Guía prescriptiva

- Migre una máquina virtual local a Amazon EC2 mediante AWS Transform MGN
- Uso de AMI o instantáneas de Amazon EBS para las copias de seguridad

Recursos de Microsoft

- Application pool identities
- Documentación de IIS
- Documentación de appcmd.exe de IIS 8
- Documentación de appcmd.exe de IIS 10
- Powerful Admin Tools

Información adicional

- La copia de seguridad de appcmd.exe incluye: grupos de aplicaciones, sitios, configuración global y esquema de IIS. No incluye archivos de contenido web, certificados SSL ni archivos de configuración compartidos.
- Para migraciones de granjas de IIS a gran escala, considere la posibilidad de utilizar el PowerShell Web-Administration módulo para operaciones de copia de seguridad y restauración mediante scripts.

Migre una base de datos local de Microsoft SQL Server a Amazon EC2 mediante MGN

Senthil Ramasamy, Amazon Web Services

Resumen

Este patrón describe los pasos para migrar una base de datos de Microsoft SQL Server desde un centro de datos en las instalaciones a una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Utiliza el AWS Transform MGN (AWS MGN) para realojar la base de datos mediante una migración automática de tipo levantamiento y cambio. AWS MGN realiza una replicación a nivel de bloque del servidor de base de datos de origen.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Una base de datos de origen Microsoft SQL Server en un centro de datos en las instalaciones

Limitaciones

- El ancho de banda de la red debe estar limitado entre el centro de datos en las instalaciones y AWS.
- AWS MGN se limita a las bases de datos alojadas en servidores independientes con almacenamiento dedicado. No admite la migración de sistemas de bases de datos en clústeres ni sistemas de bases de datos en los que la velocidad de cambio supera el rendimiento de una red.
- Algunas Servicios de AWS no están disponibles en todos. Regiones de AWS Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- Todas las versiones de bases de datos de Microsoft SQL Server
- Sistemas operativos Windows y Linux compatibles con AWS MGN

Arquitectura

Pila de tecnología de origen

Base de datos de Microsoft SQL Server en las instalaciones

Pila de tecnología de destino

Una base de datos de Microsoft SQL Server en una instancia de Amazon EC2

Arquitectura de destino

Esta arquitectura utiliza AWS MGN para replicar datos desde un centro de datos corporativo local a. AWS El diagrama muestra el proceso de replicación de datos, las comunicaciones de la API y las fases de prueba y transición.

1. Replicación de los datos:
   - AWS MGN replica los datos del centro de datos corporativo local AWS e inicia la replicación continua de los cambios.
   - Los servidores de replicación de la subred provisional reciben y procesan los datos.
2. Comunicación de la API:
   - Los servidores de replicación se conectan a los puntos finales de la API de AWS MGN, Amazon EC2 y Amazon Simple Storage Service (Amazon S3) a través del puerto TCP 443.
   - AWS MGN gestiona la migración.
   - Amazon EC2 administra las operaciones de las instancias.
3. Prueba y transición:
   - Las instancias de prueba se lanzan en la subred operativa mediante datos replicados.
   - Tras realizar las pruebas satisfactoriamente, AWS MGN crea instancias transitorias para la migración final.

Tools (Herramientas)

- AWS Transform MGN (AWS MGN) le ayuda a realojar (levantar y trasladar) las aplicaciones a una ubicación Nube de AWS sin cambios y con un tiempo de inactividad mínimo.
- Direct Connect vincula su red interna con una ubicación de Direct Connect a través de un cable estándar Ethernet de fibra óptica. Con esta conexión, puede crear interfaces virtuales directamente

con los AWS servicios públicos y, al mismo tiempo, omitir a los proveedores de servicios de Internet en su ruta de red.

- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Prácticas recomendadas

- Configure puntos de enlace regionales de API para AWS MGN, Amazon EC2 y Amazon S3 en la nube privada virtual (VPC) para prohibir el acceso público desde Internet.
- Configure los ajustes de lanzamiento de AWS MGN para lanzar los servidores de bases de datos de destino en una subred privada.
- Permita solo los puertos necesarios en los grupos de seguridad de bases de datos.
- Siga el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Configuración de AWS MGN

Tarea	Descripción	Habilidades requeridas
Configure MGN AWS .	Busque el AWS Transform MGN en e inicie Consola de administración de AWS el proceso de configuración. Esto creará una plantilla de replicación y lo redirigirá a la página Servidores de origen de la consola de MGN. Al configurar el servicio de MGN,	Administrador de base de datos, ingeniero de migracion es

Tarea	Descripción	Habilidades requeridas
	elija un rol de servicio de la lista generada.	
Agregue el servidor de origen.	Agregue los detalles del servidor de base de datos de origen en las instalaciones y, a continuación, agregue el servidor.	Administrador de base de datos, ingeniero de migraciones
Instale el agente de AWS MGN en el servidor de origen.	Descargue el instalador del agente AWS MGN a su sistema local y transfiéralo al servidor de base de datos de origen. Para validar el hash del instalador, consulte Validating the downloaded AWS Replication Agent installer for Windows 2012.	Administrador de base de datos, ingeniero de migraciones

Instalación del agente de AWS MGN en máquinas de origen

Tarea	Descripción	Habilidades requeridas
Genere las credenciales de IAM del cliente.	Antes de instalar el agente AWS MGN, genere AWS las credenciales creando un nuevo usuario de IAM con los permisos adecuados. Para obtener más información, consulte Políticas administradas por AWS AWS Transform MGN y Generación de las AWS credenciales requeridas.	Administrador de base de datos, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Instale el agente en el servidor de origen.	Instale el agente en la máquina de origen que aloja la base de datos de Microsoft SQL Server. Para obtener más información, consulte Instalación del agente de AWS replicación en servidores Windows. Proporcione las siguientes credenciales de AWS: • Región de AWS • AWS ID de clave de acceso • AWS clave de acceso secreta Sus AWS credenciales únicas permiten al agente de AWS MGN autenticarse y realizar tareas de migración.	Propietario de la aplicación, administrador de bases de datos, ingeniero de migración

Tarea	Descripción	Habilidades requeridas
Elija los discos que se replicarán.	Tras introducir sus AWS credenciales, el instalador comprueba que el servidor cumple los requisitos mínimos para la instalación del agente (por ejemplo, si el servidor tiene suficiente espacio en disco para instalar el agente AWS MGN). El instalador muestra las etiquetas de volumen y los detalles de almacenamiento. Para replicar la base de datos mediante el servicio AWS MGN, seleccione los discos correspondientes en el servidor de origen. Ingrese la ruta de cada disco, separadas por comas. Si desea replicar todos los discos, deje la ruta en blanco. Tras confirmar los discos seleccionados, la instalación continúa.	Administrador de base de datos, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Supervise el progreso de la sincronización.	AWS El agente de replicación inicia el proceso de sincronización tomando primero una instantánea de los discos seleccionados y, a continuación, replicando los datos. Puede supervisar el progreso de la sincronización desde la página del servidor de origen de la consola AWS MGN. Para obtener más información, consulte Monitor the server in the migration lifecycle.	Administrador de base de datos, ingeniero de migraciones

Replicación con AWS MGN

Tarea	Descripción	Habilidades requeridas
Administre el progreso de la replicación.	Tras iniciar la sincronización inicial, el servidor de origen aparece en la consola AWS MGN, donde puede gestionar y supervisar la migración. La consola muestra un tiempo estimado para completar la replicación, que se basa en el tamaño total de los discos seleccionados y ancho de banda de la red disponible.	Administrador de base de datos, ingeniero de migraciones
Verifique la sincronización.	Una vez que los discos del servidor de origen estén completamente sincronizados, compruebe que todos	Propietario de la aplicación, administrador de bases de datos, ingeniero de migración

Tarea	Descripción	Habilidades requeridas
	los discos seleccionados aparezcan como completamente sincronizados y que no se haya registrado ningún error en la consola. A continuación, la consola AWS MGN cambiará automáticamente el estado del ciclo de vida de la migración a Listo para las pruebas, lo que indica que el entorno replicado AWS está preparado para las pruebas de rendimiento y funcionalidad.	

Prueba y transición

Tarea	Descripción	Habilidades requeridas
Configure los ajustes de lanzamiento.	Elija el servidor de origen en la consola AWS MGN y actualice la configuración de inicio de la instancia de prueba de destino. En la página Detalles del servidor de origen, vaya a la pestaña Configuración de lanzamiento para configurar la instancia de prueba. Elija un tipo de instancia rentable y un tipo de volumen de Amazon Elastic Block Store (Amazon EBS) y, a continuación, configure los grupos de	Administrador de base de datos, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	seguridad y los requisitos de red. Para obtener más información, consulte Launch settings.	
Lance la instancia de prueba de destino.	Diríjase a la consola AWS MGN de su máquina fuente sincronizada y lance una instancia de prueba de destino seleccionando Probar y cortar y, a continuación, lanzar instancias de prueba. Esto crea un trabajo de lanzamiento que implement a la instancia de prueba con los ajustes configurados. La instancia se lanza en el entorno del servidor de base de datos de origen Nube de AWS y lo replica. Supervise el progreso del lanzamiento desde la página Historial de lanzamiento, donde puede hacer un seguimiento de la creación de la instancia y solucionar cualquier problema.	Administrador de base de datos, ingeniero de migracion es

Tarea	Descripción	Habilidades requeridas
Valide la instancia de prueba de destino.	Valide el servidor de base de datos de Amazon EC2: 1. Asegúrese de que la consola AWS MGN muestre que la instancia de prueba se está ejecutando correctamente. 2. Utilice un cliente de RDP para iniciar sesión. 3. En el menú Inicio, open Administrador de configuración de SQL Server. 4. Verifique el estado de los servicios de SQL Server, incluidos SQL Server (`MSSQLSERVER`) y Agente de SQL Server para asegurarse de que estén intactos y configurados con el tipo de inicio correcto. 5. Compare los ajustes y las configuraciones del disco entre la instancia de prueba y el servidor de base de datos de origen y confirme que las letras de las unidades, los volúmenes, las asignaciones de discos y los directorios necesarios estén asignados correctamente. 6. Conéctese a SQL Server en la instancia de Amazon	Administrador de base de datos, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	EC2 de prueba y verifique que todas las bases de datos de origen se hayan migrado y aparecen en la lista de bases de datos. Lleve a cabo pruebas de validación para garantizar que la base de datos funcione según lo esperado.	

Tarea	Descripción	Habilidades requeridas

Cambie el nombre del servidor.	AWS La migración a MGN implica una copia a nivel de almacenamiento del servidor de origen local. La instancia de EC2 de SQL Server contiene solo los detalles del servidor de origen original en sus archivos binarios, por lo que debe actualizar la información binaria para que refleje el nombre del nuevo servidor.
	
	1. Utilice SQL Server Management Studio (SSMS) para conectarse a la instancia de EC2 de SQL Server.
	2. Compruebe el nombre del servidor:
	
	`SELECT @@SERVERNAME AS 'Current Server Name';`
	
	3. Para cambiar el nombre de la instancia de SQL Server, sustituya `NEW_SERVER_NAME` por el nombre del servidor:
	
	`EXEC sp_dropserver 'OLD_SERVER_NAME'`
	`EXEC sp_addserver 'NEW_SERVER_NAME', 'local';`
		Administrador de base de datos, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	4. Verifique que el nombre del servidor sea correcto: `SELECT @@SERVERNAME AS 'Updated Server Name';` 5. Reinicie la instancia de SQL Server.	

Tarea	Descripción	Habilidades requeridas
Lance la instancia de transición.	En la consola AWS MGN, en la página Servidores de origen, confirme que el estado del ciclo de vida de la migración del servidor es Listo para la transición. Configure los ajustes de lanzamiento de la instancia de transición y asegúrese de que la configuración refleje el entorno en las instalaciones. Antes de iniciar la transición, cierre la base de datos en las instalaciones, lo que garantiza lo siguiente: • Se han completado todas las transacciones en curso. • No se producirán nuevas transacciones durante el proceso de transición. • La sincronización de datos entre los discos de origen y de destino se ha completado. Inicie la instancia de transición en la consola MGN. AWS Cuando la instancia de transición esté operativa, inicie sesión en la instancia y lleve a cabo las siguientes pruebas:	Propietario de aplicaciones, administrador de base de datos, ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
	1. Asegúrese de que SQL Server se inicie correctamente y de que se pueda acceder a las bases de datos. 2. Valide que los datos estén intactos y sean coherentes con el servidor de origen. 3. Ejecute las pruebas de la aplicación para confirmar que funcione según lo esperado. 4. En la consola AWS MGN, establezca el estado de migración en Cutover complete. 5. Comience a dirigir tráfico a la instancia de EC2.	

Resolución de problemas

Problema	Solución
La sincronización inicial falla en el paso de autenticación.	Se trata de un problema de conectividad de red. El servidor de replicación no se puede conectar a MGN. AWS

Recursos relacionados

Documentación de AWS

- Empezando con AWS Transform MGN
- Migre una base de datos de Microsoft SQL Server local a Amazon EC2

- What is Microsoft SQL Server on Amazon EC2?

Videos

- Performing a Lift and Shift Migration with AWS Transform MGN (video)

Migre una carga de trabajo de F5 BIG-IP a F5 BIG-IP VE en Nube de AWS

Deepak Kumar, Amazon Web Services

Resumen

Las organizaciones buscan migrar a la Nube de AWS para aumentar su agilidad y resiliencia. Tras migrar sus soluciones de seguridad y gestión del tráfico BIG-IP de F5 a la Nube de AWS, podrá centrarse en la agilidad y la adopción de modelos operativos de alto valor en toda la arquitectura empresarial.

Este patrón describe cómo migrar una carga de trabajo de F5 BIG-IP a una carga de trabajo de F5 BIG-IP Virtual Edition (VE) en la Nube de AWS. La carga de trabajo se migrará volviendo a alojar el entorno existente e implementando aspectos de redefinición de la plataforma, como la detección de servicios y las integraciones de la API. Las plantillas de AWS CloudFormation aceleran la migración de la carga de trabajo a la Nube de AWS.

Este patrón está dirigido a los equipos de ingeniería técnica y arquitectura que están migrando las soluciones de seguridad y gestión del tráfico de F5, y se incluye en la guía Migración de F5 BIG-IP a F5 BIG-IP VE, que se encuentra en el sitio web de la Guía prescriptiva. Nube de AWS AWS

Requisitos previos y limitaciones

Requisitos previos

- Una carga de trabajo de F5 BIG-IP existente en las instalaciones.
- Licencias de F5 existentes para las versiones de BIG-IP VE.
- Un activo. Cuenta de AWS
- Una nube privada virtual (VPC) existente configurada con una salida a través de una puerta de enlace NAT o una dirección IP elástica y configurada con acceso a los siguientes puntos de conexión: Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2), () y Amazon AWS Security Token Service .AWS STS CloudWatch También puede modificar el inicio rápido de Arquitectura de VPC modular y escalable como base de sus implementaciones.
- Una o dos zonas de disponibilidad existentes, según sus necesidades.
- Tres subredes privadas existentes en cada zona de disponibilidad.
- AWS CloudFormation plantillas, disponibles en el repositorio de F5. GitHub

Durante la migración, si lo necesita, puede que también deba usar:

- Una extensión de conmutación por error de F5 Cloud para gestionar el mapeo elástico de direcciones IP, el mapeo de IP secundaria y los cambios en la tabla de enrutamiento.
- Si cuenta con varias zonas de disponibilidad, necesitará usar las extensiones de conmutación por error de F5 Cloud para gestionar la asignación de IP elástica a los servidores virtuales.
- Debería considerar la posibilidad de utilizar F5 Application Services 3 (AS3), F5 Application Services Templates (FAST) u otro modelo de infraestructura como código (IaC) para gestionar las configuraciones. La preparación de las configuraciones en un modelo IaC y el uso de repositorios de código le ayudarán en la migración y en las labores de gestión continuada.

Experiencia

- Este patrón requiere estar familiarizado con la forma en que se VPCs pueden conectar uno o más a los centros de datos existentes. Para obtener más información al respecto, consulte las opciones de conectividad de la Network-to-Amazon VPC en la documentación de Amazon VPC.
- También es necesaria cierta familiaridad con los productos y módulos de F5, como Traffic Management Operating System (TMOS), Local Traffic Manager (LTM), Global Traffic Manager (GTM), Access Policy Manager (APM), Application Security Manager (ASM), Advanced Firewall Manager (AFM) y BIG-IQ.

Versiones de producto

- Le recomendamos que use F5 BIG-IP versión 13.1 o posterior, aunque el patrón es compatible con F5 BIG-IP versión 12.1 o posterior.

Arquitectura

Pila de tecnología de origen

- Carga de trabajo de F5 BIG-IP

Pila de tecnología de destino

- Amazon CloudFront
- CloudWatch

- Amazon EC2
- Amazon S3
- Amazon VPC
- AWS Global Accelerator
- AWS STS
- AWS Transit Gateway
- F5 BIG-IP VE

Arquitectura de destino

Tools (Herramientas)

- CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todo el país. Cuentas de AWS Regiones de AWS
- Amazon CloudFront acelera la distribución de tu contenido web al distribuirlo a través de una red mundial de centros de datos, lo que reduce la latencia y mejora el rendimiento.
- Amazon le CloudWatch ayuda a supervisar las métricas de sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática escalable en Nube de AWS el Puede lanzar tantos servidores virtuales como necesite y escalarlos rápidamente hacia arriba o hacia abajo.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Security Token Service (AWS STS) le ayuda a solicitar credenciales temporales con privilegios limitados para los usuarios.
- AWS Transit Gatewayes un centro central que conecta las nubes privadas virtuales (VPCs) y las redes locales.
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Epics

Descubrimiento y evaluación

Tarea	Descripción	Habilidades requeridas
Evalúe el rendimiento de F5 BIG-IP.	Recopile y registre las métricas de rendimiento de las aplicaciones del servidor virtual, así como las métricas de los sistemas que se migrarán. Esto le ayudará a dimensionar correctam ente la AWS infraestructura de destino para una mejor optimización de los costos.	Arquitecto de F5, ingeniero y arquitecto de redes, ingeniero
Evalúe el sistema operativo y la configuración de F5 BIG-IP.	Evalúe qué objetos se migrarán y si es necesario mantener una estructura de red, por ejemplo VLANs.	Arquitecto de F5, ingeniero
Evalúe las opciones de licencia de F5.	Evalúe qué licencia y modelo de consumo necesitará. Esta valoración debe basarse en su evaluación del sistema operativo y la configuración de F5 BIG-IP.	Arquitecto de F5, ingeniero
Evalúe las aplicaciones públicas.	Determine qué aplicacio nes requerirán direcciones IP públicas. Alinee dichas aplicaciones con las instancia s y los clústeres necesario s para cumplir con sus necesidades de rendimiento y acuerdo de nivel de servicio (SLA).	Arquitecto de F5, arquitect o de la nube, arquitecto de redes, ingeniero, equipos de aplicación

Tarea	Descripción	Habilidades requeridas
Evalúe las aplicaciones internas.	Evalúe qué aplicaciones necesitarán los usuarios internos. Asegúrese de saber dónde se encuentra n esos usuarios internos en la organización y cómo se conectan esos entornos a la Nube de AWS. También debe garantizar que esas aplicaciones puedan usar el sistema de nombres de dominio (DNS) como parte del dominio predeterminado.	Arquitecto de F5, arquitect o de la nube, arquitecto de redes, ingeniero, equipos de aplicación
Finalice la AMI.	No todas las versiones de F5 BIG-IP se crean como Amazon Machine Images (). AMIs Puede usar la herramien ta generadora de imágenes de F5 BIG-IP si necesita versiones específicas de ingeniería de reparación rápida (QFE). Para obtener más información sobre esta herramienta, consulte la sección «Recursos relaciona dos».	Arquitecto de F5, arquitecto de la nube, ingeniero
Finalice los tipos de instancia y la arquitectura.	Decida los tipos de instancia s, la arquitectura de VPC y la arquitectura interconectada.	Arquitecto de F5, arquitecto de la nube, arquitecto de redes, ingeniero

Complete las actividades de seguridad y cumplimiento

Tarea	Descripción	Habilidades requeridas
Documente las políticas de seguridad de F5 existentes.	Recopile y documente las políticas de seguridad existentes de F5. Asegúrese de crear una copia de las mismas en un repositorio de código seguro.	Arquitecto de F5, ingeniero
Cifre la AMI.	(Opcional) Es posible que su organización requiera el cifrado de los datos en reposo. Para obtener más informaci ón acerca de cómo crear una imagen personalizada de tipo traiga su propia licencia (BYOL), consulte la sección “Recursos relacionados”.	Arquitecto de F5, ingeniero y arquitecto de redes, ingeniero
Refuerce los dispositivos.	Esto ayudará a protegerlos contra posibles vulnerabi lidades.	Arquitecto de F5, ingeniero

Configure su nuevo entorno AWS

Tarea	Descripción	Habilidades requeridas
Cree cuentas periféricas y de seguridad.	Inicie sesión en Consola de administración de AWS y cree el Cuentas de AWS que proporcionará y operará los servicios perimetrales y de seguridad. Estas cuentas pueden ser diferentes de las cuentas que funcionan VPCs	Arquitecto de la nube, ingeniero

Tarea	Descripción	Habilidades requeridas
	para aplicaciones y servicios compartidos. Este paso se puede completar como parte de una zona de aterrizaje.	
Implemente la periferia y la seguridad VPCs.	Instale y configure lo VPCs necesario para ofrecer servicios perimetrales y de seguridad.	Arquitecto de la nube, ingeniero
Conectar al centro de datos de origen.	Conéctese al centro de datos de origen que aloja su carga de trabajo de F5 BIG-IP.	Arquitecto de la nube, arquitecto de redes, ingeniero
Implemente las conexiones de VPC.	Conecte el servicio perimetral y de seguridad VPCs a la aplicación VPCs.	Arquitecto de redes, ingeniero
Implemente las instancias.	Implemente las instancias mediante las CloudFormation plantillas de la sección «Recursos relacionados».	Arquitecto de F5, ingeniero
Pruebe y configure la conmutación por error de la instancia.	Asegúrese de que la plantilla AWS avanzada de alta disponibilidad para iApp o la extensión F5 Cloud Failover estén configuradas y funcionen correctamente.	Arquitecto de F5, ingeniero

Configurar redes

Tarea	Descripción	Habilidades requeridas
Prepare la topología de la VPC.	Abra la consola de Amazon VPC y asegúrese de que su VPC cuenta con todas las subredes y protecciones necesarias para la implement ación de F5 BIG-IP VE.	Arquitecto de redes, arquitect o de F5, arquitecto de la nube, ingeniero
Prepare sus puntos de conexión de VPC.	Prepare los puntos de enlace de la VPC para Amazon EC2, Amazon S3 AWS STS y si una carga de trabajo de BIG-IP de F5 no tiene acceso a una puerta de enlace NAT o a una dirección IP elástica en una interfaz TMM.	Arquitecto de la nube, ingeniero

Migración de datos

Tarea	Descripción	Habilidades requeridas
Migre la configuración.	Migre la configuración de F5 BIG-IP a F5 BIG-IP VE en la Nube de AWS.	Arquitecto de F5, ingeniero
Asocie el secundario. IPs	Las direcciones IP de los servidores virtuales tienen relación con las direcciones IP secundarias asignadas a las instancias. Asigne direcciones IP secundarias y asegúrese de seleccionar la opción	Arquitecto de F5, ingeniero

Tarea	Descripción	Habilidades requeridas
	“Permitir remapeo/reasignación”.	

Probar la configuración

Tarea	Descripción	Habilidades requeridas
Valide las configuraciones del servidor virtual.	Pruebe los servidores virtuales.	Arquitecto de F5, equipos de aplicación

Finalice las operaciones

Tarea	Descripción	Habilidades requeridas
Cree la estrategia de copia de seguridad.	Los sistemas deben estar apagados para crear una instantánea completa. Para obtener más información, consulte “Actualizar una máquina virtual F5 BIG-IP” en la sección “Recursos relacionados”.	Arquitecto de F5, arquitecto de la nube, ingeniero
Cree el manual de procedimientos de conmutación por error del clúster.	Asegúrese de que el proceso del manual de procedimientos de conmutación por error esté completo.	Arquitecto de F5, ingeniero
Configure y valide el registro.	Configure la transmisión por telemetría de F5 para enviar los registros a los destinos requeridos.	Arquitecto de F5, ingeniero

Complete la transición

Tarea	Descripción	Habilidades requeridas
Transicione a la nueva implementación.		Arquitecto de F5, arquitecto de nube, arquitecto de redes, ingeniero, AppTeams

Recursos relacionados

Guía de migración

- Migración de F5 BIG-IP a F5 BIG-IP VE en Nube de AWS

Recursos de F5

- CloudFormation plantillas en el GitHub repositorio de F5
- F5 en AWS Marketplace
- Descripción general de F5 BIG-IP VE
- Ejemplo de inicio rápido: BIG-IP Virtual Edition con WAF (LTM + ASM)
- Información general sobre AWS los servicios de aplicaciones de F5 (vídeo)
- Guía del usuario para la extensión Application Services 3 de F5
- Documentación de F5 Cloud
- iControl REST de F5 wiki
- Descripción general de los archivos de configuración individuales (11.x - 15.x) de F5
- Documentos técnicos de F5
- Herramienta generadora de imágenes de F5 BIG-IP
- Actualizar una máquina virtual F5 BIG-IP VE
- Descripción general de la opción de «migración de plataforma» de UCS archive

Migración de una aplicación web Go en las instalaciones a AWS Elastic Beanstalk mediante el método binario

Suhas Basavaraj y Shumaz Mukhtar Kazi, Amazon Web Services

Resumen

En este patrón se describe cómo migrar una aplicación web Go en las instalaciones a AWS Elastic Beanstalk. Tras migrar la aplicación, Elastic Beanstalk crea el binario para el paquete de código fuente y lo despliega en una instancia de Amazon Elastic Compute Cloud (Amazon). EC2

Como estrategia de migración para volver a alojar, el enfoque de este patrón es rápido y no requiere cambios de código, lo que se traduce en menos tiempo de pruebas y migración.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una aplicación web Go en las instalaciones.
- Un GitHub repositorio que contiene el código fuente de la aplicación Go. Si no lo usa GitHub, hay otras formas de crear un paquete de código fuente de aplicación para Elastic Beanstalk.

Versiones de producto

- La versión de Go más reciente compatible con Elastic Beanstalk. Para obtener más información, consulte la documentación de Elastic Beanstalk.

Arquitectura

Pila de tecnología de origen

- Una aplicación web Go en las instalaciones

Pila de tecnología de destino

- AWS Elastic Beanstalk
- Amazon CloudWatch

Arquitectura de destino

Tools (Herramientas)

- AWS Elastic Beanstalk permite implementar y administrar aplicaciones rápidamente en la nube de AWS sin tener que los usuarios tengan que preocuparse por la infraestructura que las ejecuta. Elastic Beanstalk reduce la complejidad de la administración sin restringir la libertad de elección ni el control.
- GitHubes un sistema de control de versiones distribuido de código abierto.

Epics

Crear el archivo .zip de la agrupación de código fuente de la aplicación web Go

Tarea	Descripción	Habilidades requeridas
Cree la agrupación de código fuente de la aplicación web Go.	Abre el GitHub repositorio que contiene el código fuente de tu aplicación Go y prepara el paquete fuente. La agrupació n de código fuente contiene un archivo `application.go` de origen en el directorio raíz, que aloja el paquete principal de la aplicación Go. Si no lo utilizas GitHub, consulta la sección de requisitos previos que aparece anteriormente en este patrón para ver otras formas de crear el paquete fuente de la aplicación.	Administrador del sistema, desarrollador de aplicaciones
Cree un archivo de configura ción.	Cree una carpeta `.ebextens ions` en la agrupació n de código fuente y, a continuación, cree un archivo `options.config` dentro	Administrador del sistema, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	de esta carpeta. Para obtener más información, consulte la documentación de Elastic Beanstalk.	
Cree el archivo .zip de la agrupación de código fuente.	Ejecute el comando siguiente. `git archive -o ../godemoapp.zip HEAD` Esto crea el archivo .zip de la agrupación de código fuente. Descargue y guarde el archivo .zip como un archivo local. **Important** El archivo .zip no puede superar los 512 MB y no puede incluir una carpeta principal ni un directorio de nivel superior.	Administrador del sistema, desarrollador de aplicaciones

Migración de la aplicación web Go a Elastic Beanstalk

Tarea	Descripción	Habilidades requeridas
Seleccione la aplicación de Elastic Beanstalk.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Elastic Beanstalk.	Administrador del sistema, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	2. En la lista Regions, seleccione su región de AWS. 3. En el panel de navegación, seleccione Applications y, a continuación, seleccione una aplicación de Elastic Beanstalk existente o cree una. Para obtener instrucciones sobre cómo crear una aplicación de Elastic Beanstalk, consulte la documentación de Elastic Beanstalk.	
Inicie el entorno del servidor web de Elastic Beanstalk.	1. En la página de descripción general de la aplicación, seleccione Create a new environment (Crear un nuevo entorno) y, a continuación, Web server environment (Entorno de servidor web). 2. Complete los campos Environment name (Nombre del entorno) y Domain name (Nombre de dominio). 3. Seleccione Platform version (Versión de la plataforma) y seleccione Go como plataforma.	Administrador del sistema, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Cargue el archivo .zip de la agrupación de código fuente en Elastic Beanstalk.	1. En Application code (Código de la aplicación), seleccione Upload your code (Cargar el código) y, a continuación, Upload. 2. Seleccione el archivo .zip que contiene la agrupación de código fuente. 3. En Version label, asigne un nombre exclusivo al archivo y, a continuación, seleccione Create environment (Crear entorno).	Administrador del sistema, desarrollador de aplicaciones
Pruebe la aplicación web Go implementada.	Se le redirigirá a la página de información general de la aplicación Elastic Beanstalk. En la parte superior de la descripción general, junto a Environment ID, seleccione la URL que termina en `elasticbeanstalk.com` para navegar hasta la aplicación. La aplicación debe usar este nombre en su archivo de configuración como variable de entorno y mostrarlo en la página web.	Administrador del sistema, desarrollador de aplicaciones

Resolución de problemas

Problema	Solución
No se puede acceder a la aplicación a través de un equilibrador de carga de aplicación.	Compruebe el grupo de destino que contiene su aplicación de Elastic Beanstalk. Si no está en buen estado, inicie sesión en la instancia de Elastic Beanstalk y compruebe la configuración del archivo `nginx.conf` para asegurar que se dirija a la URL de estado correcta. Es posible que tenga que cambiar la URL de la comprobación de estado del grupo objetivo.

Recursos relacionados

- Go platform versions supported by Elastic Beanstalk (Versiones de la plataforma Go compatibles con Elastic Beanstalk)
- Using configuration files with Elastic Beanstalk (Usar archivos de configuración con Elastic Beanstalk)
- Creating an example application in Elastic Beanstalk (Crear una aplicación de ejemplo en Elastic Beanstalk)

Migre un servidor SFTP local para utilizar AWS AWS Transfer for SFTP

Akash Kumar, Amazon Web Services

Resumen

Este patrón describe cómo migrar una solución de transferencia de archivos local que utiliza el Protocolo de transferencia de archivos (SFTP) de Secure Shell (SSH) a través del Nube de AWS servicio. AWS Transfer for SFTP Por lo general, los usuarios se conectan a un servidor SFTP a través de su nombre de dominio o mediante una IP fija. Este patrón cubre ambos casos.

AWS Transfer for SFTP es miembro de. AWS Transfer Family Es un servicio de transferencia segura que puede utilizar para transferir archivos dentro y fuera de los servicios de AWS almacenamiento a través de SFTP. Puede usarlo AWS Transfer for SFTP con Amazon Simple Storage Service (Amazon S3) o Amazon Elastic File System (Amazon EFS). Este patrón utiliza Amazon S3 para el almacenamiento.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.
- Un nombre de dominio SFTP existente o una IP SFTP fija.

Limitaciones

- El objeto más grande que se puede transferir en una solicitud es de 5 GiB actualmente. Para archivos de más de 100 MiB, considere la posibilidad de utilizar la carga multiparte de Amazon S3.

Arquitectura

Pila de tecnología de origen

- Archivos planos en las instalaciones o archivos de volcado de bases de datos.

Pila de tecnología de destino

- AWS Transfer for SFTP
- Amazon S3

- Amazon Virtual Private Cloud (Amazon VPC)
- AWS Identity and Access Management Funciones y políticas (IAM)
- Direcciones IP elásticas
- Grupos de seguridad
- Amazon CloudWatch Logs (opcional)

Arquitectura de destino

Automatización y escala

Para automatizar la arquitectura de destino de este patrón, utilice las CloudFormation plantillas adjuntas:

- `amazon-vpc-subnets.yml` aprovisiona una nube privada virtual (VPC) con dos subredes públicas y dos privadas.
- `amazon-sftp-server.yml` aprovisiona el servidor SFTP.
- `amazon-sftp-customer.yml` añade usuarios.

Tools (Herramientas)

Servicios de AWS

- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas y aplicaciones Servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos. Este patrón utiliza Amazon S3 como sistema de almacenamiento para las transferencias de archivos.
- AWS Transfer for SFTPle ayuda a transferir archivos dentro y fuera de los servicios de AWS almacenamiento a través del protocolo SFTP.
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Epics

Creación de una VPC

Tarea	Descripción	Habilidades requeridas
Cree una VPC con dos subredes.	Abra la Consola de Amazon VPC. Cree una nube privada virtual (VPC) con dos subredes públicas. (La segunda subred proporciona alta disponibilidad). —o— Puede implementar la CloudFormation plantilla adjunta en la CloudFormation consola para automatizar las tareas de esta epopeya. `amazon-vpc-subnets.yml`	Desarrollador, administrador de sistemas
Añada una puerta de enlace de Internet.	Cree una puerta de enlace de Internet y vincúlela a la VPC.	Desarrollador, administrador de sistemas
Migre una IP existente.	Adjunte una IP existente a la dirección IP elástica. Puede crear una dirección IP elástica a partir de su grupo de direcciones y utilizarla.	Desarrollador, administrador de sistemas

Aprovisionar un servidor SFTP

Tarea	Descripción	Habilidades requeridas
Cree un servidor SFTP.	Abra la consola de AWS Transfer Family. Siga las	Desarrollador, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	instrucciones de la AWS Transfer Family documentación sobre cómo crear un terminal con conexión a Internet para su servidor a fin de crear un servidor SFTP con un punto final con conexión a Internet. En Tipo de punto de enlace, seleccione Alojado en la VPC. En Acceso, seleccione Acceso a Internet. En VPC, seleccione la VPC que acaba de crear en los pasos anteriores. —o— Puedes implementar la CloudFormation plantilla adjunta en la CloudFormation consola para automatizar las tareas de esta epopeya. `amazon-sftp-server.yml`	

Tarea	Descripción	Habilidades requeridas
Migre el nombre del dominio.	Adjunte el nombre de dominio existente al nombre de host personalizado. Si utiliza un nombre de dominio nuevo, utilice el alias DNS de Amazon Route 53. Para un nombre de dominio existente, seleccione Otros DNS. Para obtener más información, consulte Trabajar con nombres de host personalizados en la AWS Transfer Family documentación.	Desarrollador, administrador de sistemas
Añada una función de CloudWatch registro.	(Opcional) Si quieres habilitar el CloudWatch registro, crea un `Transfer` rol con las operaciones de la API de CloudWatch registros `logs:CreateLogGroup logs:CreateLogStream` , `logs:DescribeLogStreams` , `ylogs:PutLogEvents` . Para obtener más información, consulte Registrar la actividad CloudWatch en la AWS Transfer Family documentación.	Desarrollador, administrador de sistemas
Guarde y envíe.	Seleccione Save. En Acciones, seleccione Iniciar y espere a que se cree el servidor SFTP con el estado En línea.	Desarrollador, administrador de sistemas

Asignar direcciones IP elásticas al servidor SFTP

Tarea	Descripción	Habilidades requeridas
Detenga el servidor para poder modificar la configuración.	En la consola de AWS Transfer Family, elija Servidores y, a continuación, seleccione el servidor SFTP que creó. En Acciones, seleccione Detener. Cuando el servidor esté desconectado, seleccione Editar para modificar su configuración.	Desarrollador, administrador de sistemas
Seleccione zonas de disponibilidad y subredes.	En la sección Zonas de disponibilidad, seleccione las zonas de disponibilidad y subredes para su VPC.	Desarrollador, administrador de sistemas
Agregue direcciones IP elásticas.	En el IPv4 caso de las direcciones, elija una dirección IP elástica para cada subred y, a continuación, seleccione Guardar.	Desarrollador, administrador de sistemas

Adición de usuarios

Tarea	Descripción	Habilidades requeridas
Cree un rol de IAM para que los usuarios accedan al bucket de S3.	Cree un rol de IAM para `Transfer` y añada `s3:ListBucket`, `s3:GetBucketLocation` y `s3:PutObject` con el nombre del bucket de S3 como recurso. Para obtener más información, consulte	Desarrollador, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	Crear una función y una política de IAM en la AWS Transfer Family documentación. —o— Puedes implementar la CloudFormation plantilla adjunta en la CloudFormation consola para automatizar las tareas de esta epopeya. `amazon-sftp-customer.yml`	
Cree un bucket de S3.	Cree un bucket de S3 para la aplicación.	Desarrollador, administrador de sistemas
Cree una carpeta opcional.	(Opcional) Si desea almacenar los archivos de los usuarios por separado, en carpetas específicas de Amazon S3, añada carpetas según corresponda.	Desarrollador, administrador de sistemas
Cree una clave pública SSH.	Para crear un par de claves SSH, consulta Generar claves SSH en la AWS Transfer Family documentación.	Desarrollador, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Agregue usuarios.	En la consola de AWS Transfer Family, seleccione Servidores, seleccione el servidor SFTP que creó y, a continuación, Agregar usuario. En el Directorio principal, seleccione el bucket de S3 que creó. En Clave pública SSH, escriba el componente de clave pública del par de claves de SSH. Añada usuarios al servidor SFTP y, a continuación, seleccione Añadir.	Desarrollador, administrador de sistemas

Probar el servidor SFTP

Tarea	Descripción	Habilidades requeridas
Actualice el grupo de seguridad.	En la sección Grupos de seguridad de su servidor SFTP, añada la IP de su máquina de prueba para obtener acceso a SFTP.	Desarrollador
Utilice una utilidad de cliente SFTP para probar el servidor.	Pruebe las transferencias de archivos mediante cualquier utilidad de cliente SFTP. Para obtener una lista de clientes e instrucciones, consulte Transferencia de archivos mediante un cliente en la AWS Transfer Family documentación.	Desarrollador

Recursos relacionados

- AWS Transfer Family Guía del usuario
- Guía del usuario de Amazon S3
- Direcciones IP elásticas en la EC2 documentación de Amazon

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migre una máquina virtual local a Amazon EC2 mediante AWS Application Migration Service

Thanh Nguyen, Amazon Web Services

Resumen

En lo que respecta a la migración de aplicaciones, las organizaciones pueden adoptar diferentes enfoques para volver a alojar (migrar mediante lift-and-shift) los servidores de las aplicaciones del entorno local a la nube de Amazon Web Services (AWS). Una forma consiste en aprovisionar nuevas instancias de Amazon Elastic Compute Cloud (Amazon EC2) y, a continuación, instalar y configurar la aplicación desde cero. Otro enfoque consiste en utilizar servicios de migración nativos de AWS o de terceros para migrar varios servidores al mismo tiempo.

Este patrón describe los pasos para migrar una máquina virtual (VM) compatible a una EC2 instancia de Amazon en la nube de AWS mediante AWS Application Migration Service. Puede utilizar el enfoque de este patrón para migrar una o varias máquinas virtuales de forma manual, una por una o automáticamente mediante la creación de los scripts de automatización adecuados en función de los pasos descritos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa en una de las regiones de AWS que admiten el Servicio de migración de aplicaciones
- Conectividad de red entre el servidor de origen y el EC2 servidor de destino a través de una red privada mediante AWS Direct Connect o una red privada virtual (VPN), o a través de Internet

Limitaciones

- Para obtener la lista más reciente de regiones admitidas, consulte las regiones de AWS admitidas.
- Para obtener una lista de los sistemas operativos compatibles, consulta la sección Sistemas operativos compatibles y la sección General de Amazon EC2 FAQs.

Arquitectura

Pila de tecnología de origen

- Un servidor físico, virtual o alojado en la nube que ejecute un sistema operativo compatible con Amazon EC2

Pila de tecnología de destino

- Una EC2 instancia de Amazon que ejecute el mismo sistema operativo que la máquina virtual de origen
- Amazon Elastic Block Store (Amazon EBS)

Arquitectura de origen y destino

El siguiente diagrama muestra la arquitectura de alto nivel y los componentes principales de la solución. En el centro de datos en las instalaciones, hay máquinas virtuales con discos locales. En AWS, hay un área de ensayo con servidores de replicación y un área de recursos migrados con EC2 instancias para realizar pruebas y transferencias. Ambas subredes contienen volúmenes de EBS.

1. Inicie el Servicio de migración de aplicaciones de AWS.
2. Configure la configuración y los informes del servidor del área de ensayo, incluidos los recursos del área de ensayo.
3. Instale los agentes en los servidores de origen y utilice la replicación continua de datos a nivel de bloques (comprimidos y cifrados).
4. Automatice la orquestación y la conversión del sistema para acortar el período de transición.

Arquitectura de redes

El siguiente diagrama muestra la arquitectura de alto nivel y los componentes principales de la solución desde la perspectiva de las redes, incluidos los protocolos y puertos necesarios para la comunicación entre los componentes principales del centro de datos en las instalaciones y de AWS.

Tools (Herramientas)

- El Servicio de migración de aplicaciones de AWS le ayuda a volver a alojar (migrar mediante lift-and-shift) aplicaciones a la nube de AWS sin cambios y con un tiempo de inactividad mínimo.

Prácticas recomendadas

- No desconecte el servidor de origen ni lo reinicie hasta que se complete la transición a la EC2 instancia de destino.
- Ofrezca a los usuarios amplias oportunidades de realizar pruebas de aceptación del usuario (UAT) en el servidor de destino para identificar y resolver cualquier problema. Lo ideal es que estas pruebas comiencen al menos dos semanas antes de la transición.
- Supervise con frecuencia el estado de replicación del servidor en la consola del Servicio de migración de aplicaciones para identificar los problemas desde el principio.
- Utilice las credenciales de AWS Identity and Access Management (IAM) temporales para instalar el agente en lugar de las credenciales de usuario de IAM permanentes.

Epics

Generar credenciales de AWS

Tarea	Descripción	Habilidades requeridas
Cree el rol de IAM de AWS Replication Agent.	Inicie sesión en la cuenta de AWS con permisos administrativos. Cree un rol de IAM en la consola de AWS Identity and Access Management (IAM): 1. En la consola de IAM, seleccione Roles. 2. Elija Create role (Crear rol). 3. En la página Seleccionar una entidad de confianza, en la sección Tipo de entidad de confianza, seleccione Cuenta de AWS. 4. En la sección Una cuenta de AWS, seleccione Esta cuenta (< account-id>).	Administrador de AWS, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	5. Elija Siguiente. 6. En la página Add permissions (Añadir permisos), busque la política `AWSApplicationMigrationAgentInstallationPolicy`, seleccione la casilla de verificación situada junto al nombre de la política. 7. Elija Siguiente. 8. En la página de Role details (Detalles del rol), introduzca MGN_Agent_Installation_Role como nombre del rol. 9. Compruebe que los campos son correctos y, a continuación, seleccione Create rol (Crear rol).	

Tarea	Descripción	Habilidades requeridas
Genere credenciales de seguridad temporales.	En una máquina con la Interfaz de la línea de comandos de AWS (AWS CLI) instalada, inicie sesión con permisos de administrador. O bien (dentro de una región de AWS compatible), en la consola de administración de AWS, inicie sesión con permisos administrativos en la cuenta de AWS y abra AWS CloudShell. Genere credenciales temporales con el siguiente comando y sustitúyalas por `<account-id>` con el ID de la cuenta de AWS. `aws sts assume-role --role-arn arn:aws:iam::<account-id>:role/MGN_Agent_Installation_Role --role-session-name mgn_installation_session_role` En el resultado del comando, copie los valores de `AccessKeyId`, `SecretAccessKey`, y `SessionToken`. Guárdelos en un lugar seguro para usarlos más adelante.	Administrador de AWS, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	Important Estas credenciales temporales caducarán después de una hora. Si necesita las credenciales después de una hora, repita los pasos anteriores.	

Inicie el Servicio de migración de aplicaciones y cree la plantilla de configuración de replicación

Tarea	Descripción	Habilidades requeridas
Inicie el servicio.	Inicie sesión en la consola con permisos administrativos para la cuenta de AWS. Elija Application Migration Service (Servicio de migración de aplicaciones) y, a continuación, elija Get started (Introducción).	Administrador de AWS, ingeniero de migraciones
Cree y configure la plantilla de ajustes de replicación.	1. Proporcione los siguientes detalles de configuración: a. Seleccione la subred del área de ensayo. b. Seleccione el tipo de instancia del servidor de replicación (`t3.small` por defecto).	Administrador de AWS, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	c. Seleccione el tipo de volumen de EBS (gp3 por defecto). d. Seleccione la opción de cifrado de EBS. e. Asegúrese de que la casilla Usar siempre el grupo de seguridad del Servicio de migración de aplicaciones esté seleccionada. f. Seleccione la casilla Usar IP privada para la replicación de datos (VPN DirectConnect, interconexión de VPC) si utiliza una conectividad de red privada entre el entorno local y AWS. g. Seleccione la casilla Reducir el ancho de banda de la red (por servidor, en Mbps) si desea limitar el ancho de banda de la red para el Servicio de migración de aplicaciones. 2. Seleccione Crear plantilla. El Servicio de aplicación de migraciones creará automáticamente todos los roles de IAM necesarios para facilitar	

Tarea	Descripción	Habilidades requeridas
	la replicación de datos y el lanzamiento de los servidores migrados.	

Instale los agentes de replicación de AWS en las máquinas de origen

Tarea	Descripción	Habilidades requeridas
Tenga preparadas las credenciales de AWS necesarias.	Cuando ejecute el archivo de instalación en un servidor de origen, tendrá que introducir las credenciales temporales que generó anteriormente, incluidas `AccessKeyId` , `SecretAccessKey` , y `SessionToken` .	Ingeniero de migraciones; administrador de AWS
Para los servidores de Linux, instale el agente.	Copie el comando del instalador, inicie sesión en los servidores de origen y ejecute el instalador. Para obtener instrucciones detalladas, consulte la documentación de AWS.	Administrador de AWS, ingeniero de migraciones
Para los servidores de Windows, instale el agente.	Descargue el archivo del instalador en cada servidor y, a continuación, ejecute el comando del instalador. Para obtener instrucciones detalladas, consulte la documentación de AWS.	Administrador de AWS, ingeniero de migraciones
Espere a que se complete la replicación inicial de los datos.	Cuando se haya instalado el agente, el servidor de origen	Administrador de AWS, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	aparecerá en la consola del Servidor de migración de aplciaciones, en la sección Servidores de origen. Espere a que el servidor realice la replicación inicial de los datos.	

Configure los ajustes de lanzamiento

Tarea	Descripción	Habilidades requeridas
Especifique los detalles del servidor.	En la consola del Servicio de migración de aplicaciones, elija la sección Servidores de origen y, a continuación, elija un nombre de servidor de la lista para acceder a los detalles del servidor.	Administrador de AWS, ingeniero de migraciones
Configure los ajustes de lanzamiento.	Seleccione la pestaña ajustes de lanzamiento. Puede configurar una variedad de ajustes, incluidos los ajustes generales de lanzamiento y los ajustes de la plantilla de EC2 lanzamien to. Para obtener instrucci ones detalladas, consulte la documentación de AWS.	Administrador de AWS, ingeniero de migraciones

Realice una prueba

Tarea	Descripción	Habilidades requeridas
Pruebe los servidores de origen.	1. En la consola del Servicio de migración de aplicaciones, en la sección Servidores de origen, asegúrese de que el ciclo de vida de migración de los servidores de origen esté preparado para las pruebas y de que el estado de la replicación de los datos sea correcto. 2. Marque la casilla situada a la izquierda de cada servidor de origen. 3. Elija Test and Cutover (Prueba y transición) y, a continuación, elija Launch Test Instance (Lanzar instancia de prueba). 4. Cuando se le pregunte, elija Launch (Lanzar). Se lanzarán los servidores.	Administrador de AWS, ingeniero de migraciones
Compruebe que la prueba se haya completado correctamente.	Una vez que el servidor de prueba se haya iniciado por completo, el estado de las alertas de la página mostrará Lanzado para cada servidor.	Administrador de AWS, ingeniero de migraciones
Pruebe el servidor.	Realice pruebas con el servidor de prueba para	Administrador de AWS, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	asegurarse de que funciona según lo esperado.	

Programe y realice una transición

Tarea	Descripción	Habilidades requeridas
Programe una transición temporal.	Programe un período de transición adecuado con los equipos pertinentes.	Administrador de AWS, ingeniero de migraciones
Lleve a cabo la transición.	1. En la consola de migración de aplicaciones, en la página Servidores de origen, active la casilla de verificación situada a la izquierda de cada servidor de origen. 2. Elija Test and Cutover (Prueba y transición) y seleccione Mark as “Ready for cutover” (Marcar como “Listo para la transición”). 3. Compruebe que el ciclo de vida de migración de cada servidor de origen esté preparado para la transició n. 4. Elija Test and Cutover (Prueba y transición) y, a continuación, elija Launch cutover instances (Lanzar instancias de transición).	Administrador de AWS, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	5. Cuando se le pregunte, elija Launch (Lanzar). Se lanzarán los servidores. El ciclo de vida de la migración del servidor de origen pasará a transición en curso.	
Compruebe que la transición se haya completado correctamente.	Una vez que los servidores de transición se hayan iniciado por completo, el estado de las Alertas en los Servidores de origen de la página mostrarán Lanzado para cada servidor.	Administrador de AWS, ingeniero de migraciones
Pruebe el servidor.	Realice pruebas con el servidor de transición para asegurarse de que funciona según lo esperado.	Administrador de AWS, ingeniero de migraciones
Finalice la transición.	Elija Test and Cutover (Prueba y transición) y, a continuación, seleccione Finalize cutover (Finalizar la transición) para finalizar el proceso de migración.	Administrador de AWS, ingeniero de migraciones

Recursos relacionados

- AWS Application Migration Service
- Guía de usuario del servicio de migración de aplicaciones de AWS

Migre pequeños conjuntos de datos del entorno local a Amazon S3 mediante AWS SFTP

Charles Gibson y Sergiy Shevchenko, Amazon Web Services

Resumen

Este patrón describe cómo migrar pequeños conjuntos de datos (5 TB o menos) de centros de datos locales a Amazon Simple Storage Service (Amazon S3) mediante AWS Transfer for SFTP ().AWS SFTP Los datos pueden ser volcados de bases de datos o archivos planos.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Un AWS Direct Connect enlace establecido entre su centro de datos y AWS

Limitaciones

- Los archivos de datos deben tener menos de 5 TB. Para archivos de más de 5 TB, puede realizar una carga multiparte a Amazon S3 o elegir otro método de transferencia de datos.

Arquitectura

Pila de tecnología de origen

- Archivos planos en las instalaciones o volcados de bases de datos locales

Pila de tecnología de destino

- Amazon S3

Arquitectura de origen y destino

Tools (Herramientas)

- AWS SFTP— Permite la transferencia de archivos directamente desde y hacia Amazon S3 mediante el Protocolo seguro de transferencia de archivos (SFTP).

- AWS Direct Connect— Establece una conexión de red dedicada desde sus centros de datos locales a. AWS
- Puntos de enlace de VPC: le permiten conectar de forma privada una VPC a servicios de punto final de VPC compatibles y alimentados por Servicios de AWS ellos AWS PrivateLink sin una puerta de enlace de Internet, un dispositivo de traducción de direcciones de red (NAT), una conexión VPN o una conexión. Direct Connect Las instancias en una VPC no necesitan direcciones IP públicas para comunicarse con los recursos del servicio.

Epics

Preparación para la migración

Tarea	Descripción	Habilidades requeridas
Documente los requisitos actuales de SFTP.		Propietario de la aplicación, SA
Identifique los requisitos de autenticación.	Los requisitos pueden incluir la autenticación basada en claves, el nombre de usuario o la contraseña o el proveedor de identidades (IdP).	Propietario de la aplicación, SA
Identifique los requisitos de integración de la aplicación.		Propietario de la aplicación
Identifique a los usuarios que requieren el servicio.		Propietario de la aplicación
Determine el nombre DNS del punto de conexión del servidor SFTP.		Red
Determinar la estrategia de copia de seguridad.		SA, Administrador de base de datos (si se transfieren datos)

Tarea	Descripción	Habilidades requeridas
Identifique la estrategia de migración o transición de la aplicación.		Propietario de la aplicación, SA, Administrador de base de datos

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una o más nubes privadas virtuales (VPCs) y subredes en su. Cuenta de AWS		Propietario de la aplicación, AMS
Crear grupos de seguridad y listas de control de acceso a la red (ACL).		Seguridad, redes, AMS
Cree el bucket de Amazon S3.		Propietario de la aplicación, AMS
Cree el rol AWS Identity and Access Management (IAM).	Cree una política de IAM que incluya los permisos que le permitirán acceder AWS SFTP a su bucket de Amazon S3. Esta política de IAM determina el nivel de acceso que otorga a los usuarios de SFTP. Cree otra política de IAM con la que establecer una relación de confianza. AWS SFTP	Seguridad, AMS
Asocia un dominio registrado (opcional).	Si tiene su propio dominio registrado, puede asociarlo al servidor SFTP. Puede enrutar el tráfico SFTP al punto de	Redes, AMS

Tarea	Descripción	Habilidades requeridas
	conexión de su servidor SFTP desde un dominio o desde un subdominio.	
Cree un servidor SFTP.	Especifique el tipo del proveedor de identidad que el servicio debe usar para autenticar a los usuarios.	Propietario de la aplicación, AMS
Abrir un cliente SFTP.	Abra un cliente SFTP y configure la conexión para usar el host del punto final SFTP. AWS SFTP es compatible con cualquier cliente SFTP estándar. Los clientes SFTP más utilizados incluyen OpenSSH, WinSCP, Cyberduck y. FileZilla Puede obtener el nombre de host del servidor SFTP desde la consola. AWS SFTP	Propietario de la aplicación, AMS

Planificar y probar

Tarea	Descripción	Habilidades requeridas
Planifique la migración de la aplicación.	Planifique los cambios necesarios en la configuración de la aplicación, establezc a la fecha de migración y determine el programa de pruebas.	Propietario de la aplicación, AMS
Pruebe la infraestructura.	Realice pruebas en un entorno que no sea de producción.	Propietario de la aplicación, AMS

Recursos relacionados

Referencias

- AWS Transfer for SFTP Guía del usuario
- AWS Direct Connect resources
- Puntos de enlace de la VPC

Tutoriales y videos

- AWS Transfer for SFTP (vídeo)
- AWS Transfer for SFTP guía de usuario
- AWS SA Whiteboarding - Direct Connect (vídeo)

Migre una base de datos Oracle local a Oracle on Amazon EC2

Baji Shaik y Pankaj Choudhary, Amazon Web Services

Resumen

Este patrón le guía por los pasos para migrar una base de datos Oracle local a Oracle en una instancia de Amazon Elastic Compute Cloud EC2 (Amazon). Describe dos opciones de migración: usar AWS Data Migration Service (AWS DMS) o usar herramientas nativas de Oracle, como RMAN, importación/exportación de Data Pump, espacios de tabla transportables y Oracle. GoldenGate

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de origen de Oracle en un centro de datos en las instalaciones

Limitaciones

- El sistema operativo (SO) de destino debe ser compatible con Amazon EC2. Para obtener una lista completa de los sistemas compatibles, consulta Amazon EC2 FAQs.

Versiones de producto

- Versiones de Oracle 10.2 y posteriores (para las versiones 10.x), 11g y hasta 12.2 y 18c para las ediciones Enterprise, Standard, Standard One y Standard Two. Para ver la lista más reciente de versiones compatibles con AWS DMS, consulte «Bases de datos locales y de EC2 instancias de Amazon» en Fuentes para la migración de datos en la documentación de AWS DMS.

Arquitectura

Pila de tecnología de origen

- Una base de datos de Oracle en las instalaciones

Pila de tecnología de destino

- Una instancia de base de datos Oracle en Amazon EC2

Arquitectura de destino

Arquitectura de migración de datos

Uso de AWS DMS:

Uso de herramientas nativas de Oracle:

Tools (Herramientas)

- AWS DMS: AWS Database Migration Service (AWS DMS) admite varios tipos de bases de datos de origen y destino. Para obtener información sobre las versiones y ediciones de bases de datos compatibles, consulte Uso de una base de datos de Oracle como origen para AWS DMS. Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características.
- Herramientas nativas de Oracle: RMAN, importación/exportación de Data Pump, tablespaces transportables, Oracle GoldenGate

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.		Administrador de base de datos
Identifique la versión del sistema operativo de destino.		DBA, SysAdmin
Identifique los requisitos de hardware de la instancia del servidor de destino en función de la lista de compatibilidad		DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
de Oracle y los requisitos de capacidad.		
Identifique los requisitos de almacenamiento (como el tipo y la capacidad de almacenamiento).		DBA, SysAdmin
Identifique los requisitos de la red, como la latencia y el ancho de banda.		DBA, SysAdmin
Elija el tipo de instancia adecuado en función de la capacidad, las características de almacenamiento y las características de red.		DBA, SysAdmin
Identifique los requisitos de seguridad de network/host acceso para las bases de datos de origen y destino.		DBA, SysAdmin
Identifique una lista de los usuarios del sistema operativo necesarios para la instalación del software Oracle.		DBA, SysAdmin
Descargue e instale la herramienta de conversión de esquemas de AWS (AWS SCT)		Administrador de base de datos
Cree un proyecto de AWS SCT para la carga de trabajo y conéctese a la base de datos de origen.		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Genere archivos SQL para la creación de objetos (tablas, índices, secuencias, etc.).		Administrador de base de datos
Determine una estrategia de copia de seguridad.		DBA, SysAdmin
Determine los requisitos de disponibilidad.		Administrador de base de datos
Identifique la estrategia de migración/cambio de aplicaciones.		DBA, propietario de la SysAdmin aplicación

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC) y subredes en su cuenta de AWS.		SysAdmin
Cree grupos de seguridad y listas de control de acceso a la red (ACLs).		SysAdmin
Configure e inicie la EC2 instancia.		SysAdmin

Instalación del software Oracle

Tarea	Descripción	Habilidades requeridas
Cree los usuarios y grupos del sistema operativo necesarios		DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
para que funcione el software Oracle.		
Descargue la versión requerida del software Oracle.		
Instale el software de Oracle en la EC2 instancia.		DBA, SysAdmin
Cree objetos como tablas, claves principales, vistas y secuencias mediante los scripts generados por AWS SCT.		Administrador de base de datos

Migración de datos: opción 1

Tarea	Descripción	Habilidades requeridas
Utilice las herramientas nativas de Oracle o herramientas de terceros para migrar los objetos y datos de la base de datos.	Las herramientas de Oracle incluyen la importación/exportación de Data Pump, RMAN, espacios de tablas transportables y. GoldenGate	Administrador de base de datos

Migración de datos: opción 2

Tarea	Descripción	Habilidades requeridas
Determine el método de migración.		Administrador de base de datos
Cree una instancia de replicación con la consola de AWS DMS.		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree puntos de conexión de origen y destino.		Administrador de base de datos
Cree una tarea de replicación.		Administrador de base de datos
Habilite la captura de datos de cambios (CDC) para capturar los cambios para una replicación continua.		Administrador de base de datos
Ejecute la tarea de replicación y supervise los registros.		Administrador de base de datos
Cree objetos secundarios como índices y claves externas cuando se complete la carga.		Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de migración de aplicaciones.		SysAdminDBA, propietario de la aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Siga la estrategia de transición o cambio de la aplicación.		DBA, propietario de la SysAdmin aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cierre los recursos temporales de AWS Secrets Manager.		DBA, SysAdmin
Revise y valide los documento s del proyecto.		DBA, propietario de la SysAdmin aplicación
Recopile métricas sobre el tiempo de migración, el porcentaje de migraciones manuales en comparación con las realizadas con herramien tas, el ahorro de costos, etc.		DBA, propietario de la SysAdmin aplicación
Cerrar el proyecto y enviar comentarios.		

Recursos relacionados

Referencias

- Estrategias para migrar bases de datos de Oracle a AWS
- Migración de bases de datos de Oracle a la nube de AWS
- EC2 Sitio web de Amazon
- Sitio web de AWS DMS
- Publicaciones del blog de AWS DMS
- EC2 Precios de Amazon
- Concesión de licencias de software de Oracle en el entorno de computación en la nube

Tutoriales y videos

- Cómo empezar con Amazon EC2
- Introducción a AWS DMS

- Introducción a Amazon EC2 : Elastic Cloud Server & Hosting con AWS (vídeo)

Migre una base de datos Oracle local a Amazon EC2 mediante Oracle Data Pump

Navakanth Talluri, Amazon Web Services

Resumen

Al migrar las bases de datos, debe tener en cuenta factores como los motores y las versiones de las bases de datos de origen y destino, las herramientas y servicios de migración y los períodos de inactividad aceptables. Si va a migrar una base de datos Oracle local a Amazon Elastic Compute Cloud EC2 (Amazon), puede utilizar herramientas de Oracle, como Oracle Data Pump y Oracle Recovery Manager (RMAN). Para obtener más información sobre estrategias, consulte la guía Migración de bases de datos de Oracle a la nube de AWS.

Oracle Data Pump le ayuda a extraer la copia de seguridad lógica y coherente de la base de datos y a restaurarla en la instancia de destino. EC2 Este patrón describe cómo migrar una base de datos Oracle local a una EC2 instancia mediante Oracle Data Pump y el `NETWORK_LINK` parámetro, con un tiempo de inactividad mínimo. El parámetro `NETWORK_LINK` inicia una importación a través de un enlace de base de datos. El cliente Oracle Data Pump Import (impdp) de la EC2 instancia de destino se conecta a la base de datos de origen, recupera los datos de la misma y los escribe directamente en la base de datos de la instancia de destino. En esta solución no se utilizan archivos de copia de seguridad ni de volcado.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una base de datos de Oracle en las instalaciones:
  - No es una base de datos de Oracle Real Application Clusters (RAC)
  - No es una base de datos de Oracle Automatic Storage Management (Oracle ASM)
  - Está en modo de lectura-escritura.
- Ha creado un enlace de AWS Direct Connect entre su centro de datos en las instalaciones y AWS. Para obtener más información, consulte Crear una conexión (documentación de Direct Connect).

Versiones de producto

- Oracle Database 10g versión 1 (10.1) y posteriores

Arquitectura

Pila de tecnología de origen

- Un servidor de base de datos de Oracle independiente (sin RAC ni ASM) en un centro de datos en las instalaciones

Pila de tecnología de destino

- Una base de datos Oracle que se ejecuta en Amazon EC2

Arquitectura de destino

El pilar de fiabilidad del Marco de AWS Well-Architected recomienda crear copias de seguridad de datos para ayudar a proporcionar alta disponibilidad y resiliencia. Para obtener más información, consulte Diseño de arquitectura para alta disponibilidad en Prácticas recomendadas para ejecutar bases de datos de Oracle en AWS. Este patrón configura las bases de datos principales y en espera en EC2 las instancias mediante Oracle Active Data Guard. Para una alta disponibilidad, las EC2 instancias deben estar en diferentes zonas de disponibilidad. Sin embargo, las zonas de disponibilidad pueden estar en la misma región de AWS o en regiones de AWS diferentes.

Active Data Guard proporciona acceso de solo lectura a una base de datos física en espera al tiempo que rehace los cambios de forma continua desde la base de datos principal. En función de su objetivo de punto de recuperación (RPO) y el objetivo de tiempo de recuperación (RTO), puede elegir entre las opciones de transporte de rehacer síncrono y asíncrono.

La siguiente imagen muestra la arquitectura de destino si las EC2 instancias principal y en espera se encuentran en distintas regiones de AWS.

Arquitectura de migración de datos

Una vez que haya terminado de configurar la arquitectura de destino, utilice Oracle Data Pump para migrar los datos y esquemas locales a la instancia principal EC2 . Durante la transición, las aplicaciones no pueden acceder a la base de datos en las instalaciones ni a la base de datos de destino. Cierre estas aplicaciones hasta que se puedan conectar a la nueva base de datos de destino de la instancia principal EC2 .

En la imagen siguiente, se muestra la arquitectura durante la migración de datos. En este ejemplo de arquitectura, las EC2 instancias principal y en espera se encuentran en distintas regiones de AWS.

Tools (Herramientas)

Servicios de AWS

- AWS Direct Connect vincula su red interna con una ubicación de Direct Connect a través de un cable estándar Ethernet de fibra óptica. Con esta conexión, puede crear interfaces virtuales directamente en servicios públicos de AWS omitiendo a los proveedores de servicios de Internet en su ruta de acceso a la red.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.

Otras herramientas y servicios

- Oracle Active Data Guard le ayuda a crear, mantener, gestionar y supervisar bases de datos en espera.
- Oracle Data Pump le ayuda a trasladar datos y metadatos de una base de datos a otra a altas velocidades.

Prácticas recomendadas

- Best Practices for Running Oracle Database on AWS
- Importación de datos mediante NETWORK_LINK

Epics

Configure las EC2 instancias en AWS

Tarea	Descripción	Habilidades requeridas
Identifique la configuración de hardware de origen para el host en las instalaciones y los parámetros del núcleo.	Valide la configuración local, incluidos el tamaño del almacenamiento, input/output las operaciones por segundo (IOPS) y la CPU. Esto es	DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
	importante para las licencias de Oracle, que se basan en los núcleos de la CPU.	
Cree la infraestructura en AWS.	Cree las nubes privadas virtuales (VPCs), las subredes privadas, los grupos de seguridad, las listas de control de acceso a la red (ACLs), las tablas de enrutamiento y la puerta de enlace a Internet. Para obtener más información, consulte los siguientes temas: • VPCs y subredes • Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Configure las EC2 instancias mediante Active Data Guard.	Configure las EC2 instancias de AWS mediante una configuración de Active Data Guard, tal y como se describe en el AWS Well-Architected Framework. La versión de Oracle Database de la EC2 instancia puede ser diferente de la versión local porque este patrón utiliza copias de seguridad lógicas. Tenga en cuenta lo siguiente: • Coloque la base de datos de destino en modo de lectura-escritura. • En la base de datos de destino, proporcione los detalles del sustrato de red transparente (TNS) de la base de datos de origen. Para obtener más información, consulte lo siguiente: • Puesta en marcha de una base de datos (documentación de Oracle) • Creación y configuración de una base de datos de Oracle (documentación de Oracle)	Administrador de base de datos, administrador de sistemas

Migre la base de datos a Amazon EC2

Tarea	Descripción	Habilidades requeridas
Cree un dblink a la base de datos local desde la instancia. EC2	Cree un enlace de base de datos (dblink) entre la base de datos Oracle de la EC2 instancia y la base de datos Oracle local. Para obtener más información, consulte Uso de la importación de enlaces de red para mover datos (documentación de Oracle).	Administrador de base de datos
Compruebe la conexión entre la EC2 instancia y el host local.	Usa el dblink para confirmar que la conexión entre la EC2 instancia y la base de datos local funciona. Para obtener instrucciones, consulte CREATE DATABASE LINK (documentación de Oracle).	Administrador de base de datos
Detenga todas las aplicacio nes conectadas a la base de datos en las instalaciones.	Una vez aprobado el tiempo de inactividad de la base de datos, cierre todas las aplicaciones y trabajos dependientes que se conecten a la base de datos en las instalaciones. Puede hacerlo directamente desde la aplicación o desde la base de datos mediante cron. Para obtener más información, consulte Uso de la utilidad Crontab para programar tareas en Oracle Linux.	Administrador de base de datos, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Programe el trabajo de migración de datos.	En el host de destino, utilice el comando `impdb` para programar la importación de Data Pump. Esto conecta la base de datos de destino con el host en las instalaciones e inicia la migración de datos. Para obtener más información, consulte Importación de Data Pump y NETWORK_LINK (documentación de Oracle).	Administrador de base de datos
Validar la migración de datos.	La validación de los datos es un paso crucial. Para la validación de datos, puede utilizar herramientas personalizadas o herramientas de Oracle, como una combinación de consultas dblink y SQL.	Administrador de base de datos

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Coloque la base de datos de origen en un modo de solo lectura.	Confirme que la aplicación esté cerrada y que no se estén realizando cambios en la base de datos de origen. Abra la base de datos de origen en modo de solo lectura. Esto le permite evitar cualquier transacción abierta. Para obtener más información, consulte `ALTER`	Administrador de bases de datos, DevOps ingeniero y desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`DATABASE` en SQL Statements (documentación de Oracle).	
Valide el recuento de objetos y los datos.	Para validar los datos y objetos, puede utilizar herramientas personalizadas o herramientas de Oracle, como una combinación de consultas dblink y SQL.	Administrador de base de datos, desarrollador de aplicaciones
Conecte las aplicaciones a la base de datos de la EC2 instancia principal.	Cambie el atributo de conexión de la aplicación para que apunte a la nueva base de datos que creó en la EC2 instancia principal.	Administrador de base de datos, desarrollador de aplicaciones
Valide el rendimiento de la aplicación.	Inicie la aplicación. Valide la funcionalidad y el rendimiento de la aplicación mediante el Repositorio automatizado de cargas de trabajo (documentación de Oracle).	Desarrollador de aplicaciones, DevOps ingeniero y administrador de bases de datos

Recursos relacionados

Referencias de AWS

- Migración de bases de datos de Oracle a la Nube de AWS
- Amazon EC2 para Oracle
- Migración de bases de datos voluminosas de Oracle a AWS para entornos multiplataforma
- VPCs y subredes
- Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos

Referencias de Oracle

- Configuraciones de Oracle Data Guard
- Importación de Data Pump

Migración de los sistemas BYOL de RHEL a instancias con licencia incluida de AWS mediante AWS MGN

Mike Kuznetsov, Amazon Web Services

Resumen

Al migrar sus cargas de trabajo a AWS mediante el AWS Application Migration Service (AWS MGN), es posible que tenga que migrar mediante lift-and-shift (volver a alojar) sus instancias de Red Hat Enterprise Linux (RHEL) y cambiar la licencia del modelo traiga su propia licencia (BYOL) predeterminado a un modelo AWS License Included (LI) durante la migración. AWS MGN admite un enfoque escalable que utiliza los Identificadores de imagen de máquina de Amazon (AMI). Este patrón describe cómo realizar el cambio de licencia en los servidores de RHEL durante la migración de volver a alojar a escala. También explica cómo cambiar la licencia de un sistema RHEL que ya se ejecuta en Amazon Elastic Compute Cloud (Amazon EC2).

Requisitos previos y limitaciones

Requisitos previos

- Acceso a la cuenta de AWS de destino
- AWS MGN se inicializó en la cuenta y región de AWS de destino para la migración (no es obligatorio si ya ha migrado de su sistema en las instalaciones a AWS)
- Un servidor RHEL de origen con una licencia RHEL válida

Arquitectura

Este patrón cubre dos escenarios:

- Migración de un sistema en las instalaciones directamente a una instancia de AWS LI mediante AWS MGN. Para este escenario, siga las instrucciones de la primera epopeya (Migración a una instancia de LI: opción 1) y de la tercera epopeya.
- Cambie el modelo de licencias de BYOL a LI para un sistema RHEL migrado anteriormente que ya se ejecuta en Amazon EC2. Para este escenario, siga las instrucciones de la segunda epopeya (migrar a una instancia de LI: opción 2) y de la tercera epopeya.

> **Note**
>
> La tercera epopeya implica la reconfiguración de la nueva instancia de RHEL para utilizar los servidores de Red Hat Update Infrastructure (RHUI) proporcionados por AWS. Este proceso es el mismo en ambos escenarios.

Tools (Herramientas)

Servicios de AWS

- El AWS Application Migration Service (AWS MGN) le ayuda a volver a alojar (migrar mediante lift-and-shift) las aplicaciones a la nube de AWS sin cambios y con un tiempo de inactividad mínimo.

Epics

Migración a una instancia LI: opción 1 (para un sistema RHEL en las instalaciones)

Tarea	Descripción	Habilidades requeridas
Busque el Identificador de AMI de la instancia de RHEL AWS LI en la región de destino.	Visite AWS Marketplace o utilice la consola Amazon EC2 para buscar el Identificador de AMI de RHEL que coincida con la versión del sistema fuente de RHEL (por ejemplo, RHEL-7.7) y anote el ID de AMI. En la consola Amazon EC2, puede filtrarlos AMIs mediante uno de los siguiente s términos de búsqueda: • Descripción = Proporcio nada por Red Hat, Inc. • Nombre de la AMI = RHEL-7.7	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Configure los ajustes de lanzamiento de AWS MGN.	1. En la consola de AWS MGN, añada el sistema RHEL de origen: instale el agente de replicación de AWS y añada el servidor de origen siguiendo las instrucciones de la documentación de AWS MGN. 2. En la página Servidores de origen, elija el sistema RHEL de origen y, a continuación, elija la pestaña Configuración de lanzamiento. 3. En la sección Configuración de las opciones generales de lanzamiento, seleccione Editar. Para deshabilitar la selección automática y especificar manualmente el tipo de instancia de destino, cambie el Tamaño correcto del tipo de instancia a Ninguno y, a continuación, seleccione Guardar configuración. Esto le permite usar el tipo de instancia que haya configurado en su plantilla de lanzamiento de Amazon EC2. Para obtener más información, consulte la	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	documentación de AWS MGN. 4. En la sección Plantilla de lanzamiento de EC2, elija Modificar. En el cuadro de diálogo Acerca de la modificación de las plantillas de lanzamiento de EC2, vuelva a seleccion ar Modificar. Esto abre la consola Amazon EC2 para que pueda cambiar la plantilla de esta instancia. 5. Consulte las considera ciones clave en la documentación de AWS MGN. **Note** Puede hacer caso omiso de la advertencia de no elegir su propia AMI. 6. En la consola Amazon EC2, en la nueva plantilla de lanzamiento, modifique lo siguiente: • Para AMI, especifiq ue el Identificador de AMI que identificó anteriormente o busque RHEL-x y especifique la	

Tarea	Descripción	Habilidades requeridas
	versión que necesita (por ejemplo, RHEL-7.7). • En Tipo de instancia, defina el tipo de instancia de destino deseado. • No modifique las siguientes secciones: Par de claves (inicio de sesión), Configuración de red (a menos que desee especificar una subred y grupos de seguridad de destino), Almacenamiento y Etiquetas de recursos (a menos que desee agregar o modificar alguna etiqueta). • (Opcional) En la sección Detalles avanzados, especifique el rol del perfil de instancia de IAM, si es necesario para que AWS Systems Manager lo administre en el futuro. 7. Seleccione Crear versión de plantilla y, a continuación, elija el enlace que aparece en el mensaje de confirmación para ver la plantilla de lanzamiento. 8. Seleccione Acciones y Cómo establecer la versión predeterminada.	

Tarea	Descripción	Habilidades requeridas
	En la Versión de plantilla, seleccione la versión más reciente (versión 2 para un sistema nuevo) y, a continuación, elija Cómo establecer como versión predeterminada. AWS MGN utilizará ahora esta versión de la plantilla de lanzamiento para lanzar instancias de prueba o de transición. Para obtener más información, consulte la documentación de AWS MGN.	

Tarea	Descripción	Habilidades requeridas
Valide la configuración.	1. En la consola MGN de AWS, en la página Servidores de origen, elija su servidor de origen y, a continuación, elija la pestaña Configuración de lanzamiento. 2. En la sección Plantilla de lanzamiento de EC2, compruebe que los parámetros del Tipo de instancia, la Subred y los Grupos de seguridad estén configurados correctam ente. **Note** En esta sección no se muestra el ID de AMI que ha seleccion ado. Para ver el Identificador, puede abrir la consola Amazon EC2 en la vista Plantillas de lanzamiento y buscar el Identific ador de plantilla que se muestra en esta sección.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Lance la nueva instancia de LI.	1. Cuando se complete la sincronización inicial, la columna Ciclo de vida de la migración del servidor en la página Servidores de origen de la consola AWS MGN cambia a Listo para la prueba. Para lanzar la nueva instancia de prueba, elija su servidor de origen, abra el menú Prueba y transición y, a continuac ión, elija Lanzar instancia s de prueba. Seleccione Ver detalles del trabajo para supervisar el estado del trabajo de lanzamiento. Para obtener más informaci ón, consulte la documenta ción de AWS MGN. 2. Espere a que se complete el trabajo de lanzamien to y, a continuación, abra la página de detalles de la instancia EC2 lanzada. Seleccione la pestaña Detalles y compruebe que la sección de Detalles de la instancia contiene lo siguiente: • Detalles de la plataform a: “Red Hat Enterprise Linux”	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	• Nombre de la AMI: el nombre de la AMI que especificó en la plantilla de lanzamiento de EC2 3. Realizar la transición a la nueva instancia de LI siguiendo las instrucciones de la documentación de AWS MGN. 4. Vuelva a configurar la nueva instancia para usar los servidores RHUI proporcionados por AWS siguiendo los pasos de la última epopeya.	

Migración a una instancia LI: opción 2 (para una instancia RHEL BYOL EC2)

Tarea	Descripción	Habilidades requeridas
Migre una instancia de RHEL BYOL EC2 a una instancia de AWS LI.	Puede cambiar los sistemas RHEL que anteriormente migró a AWS como BYOL a instancias de AWS LI moviendo sus discos (volúmenes de Amazon Elastic Block Store) y adjuntándolos a una nueva instancia de LI. Para realizar este cambio, siga estos pasos: 1. Lance una nueva instancia de RHEL de destino desde una AMI de RHEL LI.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	Asegúrese de que la AMI que ha seleccionado: • Utilice la misma versión de RHEL que tiene la instancia de RHEL actual. • Tiene el mismo proceso de arranque (BIOS o UEFI) que la instancia de RHEL actual. Por ejemplo, si el servidor de origen está basado en BIOS, utilice la AMI de RHEL de AWS Marketplace que también esté basada en BIOS. Para los sistemas basados en UEFI, elija la AMI basada en UEFI. 2. Detenga ambas instancias: la nueva instancia de LI y la instancia de origen original. 3. Separe todos los volúmenes de EBS (incluido el disco raíz) de la nueva instancia de LI y elimínelos. 4. Separe todos los volúmenes de EBS (incluido el disco raíz) de la antigua instancia de origen y adjúntelos a la nueva instancia de LI. Mantenga la misma asignación de volúmenes a los dispositivos. (Por ejemplo, el	

Tarea	Descripción	Habilidades requeridas
	volumen de EBS que estaba conectado anteriormente a la unidad de `/dev/sda` debe estar conectado como `/dev/sda` a la nueva instancia). 5. Elimine la instancia de origen (ahora sin disco). 6. Inicie la nueva instancia de LI. Inicie sesión en la instancia y vuelva a configurarla para usar los servidores RHUI proporcionados por AWS siguiendo los pasos de la siguiente epopeya.	

Reconfigurar el sistema operativo RHEL para usar la RHUI proporcionada por AWS (ambas opciones)

Tarea	Descripción	Habilidades requeridas
Anule el registro del sistema operativo de la suscripción y la licencia de Red Hat.	Tras la migración y la transición exitosa, es necesario eliminar el sistema RHEL de la suscripción a Red Hat para dejar de consumir la licencia de Red Hat y evitar la doble facturación. Para eliminar el sistema operativo RHEL de la suscripción a Red Hat, siga el proceso descrito en la documentación	Administrador de sistemas o Linux

Tarea	Descripción	Habilidades requeridas
	sobre Red Hat Subscription Management (RHSM). Utilice el comando CLI: `subscription-manager unregister` También puede deshabilitar el complemento del administrador de suscripciones para dejar de comprobar el estado de la suscripción en cada llamada de yum. Para ello, edite el archivo de configuración `/etc/yum/pluginconf.d/subscription-manager.conf` y cambie el parámetro `enabled=1` a `enabled=0` .	

Tarea	Descripción	Habilidades requeridas
Sustituya la configuración de actualización anterior (RHUI, red Red Hat Satellite, repositorios yum) por la RHUI proporcionada por AWS.	Debe volver a configurar el sistema RHEL migrado para utilizar los servidores RHUI proporcionados por AWS. Esto le da acceso a los servidores RHUI dentro de las regiones de AWS sin necesidad de una infraestr uctura de actualización externa. El proceso consta de los pasos siguientes: 1. Realice una copia de seguridad de la configura ción actual de yum. 2. Elimine la configuración y los paquetes antiguos de RHUI (repositorios yum). 3. Añada los nuevos paquetes de certificados y configura ción de RHUI proporcio nados por AWS. Debe recuperarlos de otra instancia de RHEL en AWS, ya que estos paquetes de configuración solo están disponibles en los servidore s RHUI proporcionados por AWS. Estos son los pasos y comandos detallados:	Administrador de sistemas o Linux

Tarea	Descripción	Habilidades requeridas

	1. Haga una copia de seguridad de la configuración y los certificados de yum existentes copiando todas las carpetas `/etc/yum*` y `/etc/pki/*` en una ubicación de copia de seguridad. Por ejemplo:
	`mkdir yum-backup`
	`cp -ra /etc/yum* /etc/pki ./yum-backup`
	`tar czf yum-backup.tgz ./yum-backup`
	2. Elimine la configuración y los paquetes de RHUI anteriores:
	a. Encuentre todos los paquetes RHUI instalados:
	`sudo rpm -qa | grep rhui`
	b. Elimine estos paquetes:
	`sudo yum remove $(rpm -qa | grep rhui)`
	c. Elimine el archivo `/etc/yum/vars/releasever`, si existe.
	3. Añada los nuevos paquetes de certificados y RHUI proporcionados por AWS.	

Tarea	Descripción	Habilidades requeridas

	Debe recuperarlos de otra instancia de RHEL en AWS. Puede hacer esto de varias formas. Por ejemplo, puede seguir las instrucciones que se proporcionan en el artículo de la base de conocimiento de Red Hat:
	a. Lance otra instancia de RHEL (RHEL-EC2) desde AWS Marketplace.
	b. Descargue dos paquetes de esta instancia: el paquete de configuración del cliente RHUI más reciente y los certifica dos de la autoridad de certificación (CA). Por ejemplo, ejecute este comando desde el escritorio:
	`ssh RHEL-EC2 "sudo yumdownloader ca-certificates rh-amazon-rhui-cli ent"`
	c. Copie los paquetes de la instancia RHEL-EC2 al nuevo sistema migrado. Por ejemplo:
	`scp RHEL-EC2:rh-amazon-rhui-cli`	

Tarea	Descripción	Habilidades requeridas
	ent* RHEL-EC2:ca-certificates* . ssh <migrated-instance> "mkdir /tmp/amazon" scp rh-amazon-rhui-client* ca-certificates* <migrated-instance>:/tmp/amazon d. Instale los nuevos paquetes de configuración de RHUI y CA en la instancia migrada: ssh <migrated-instance> "sudo rpm -Uhv /tmp/amazon/*"	
Valide la configuración.	En la instancia migrada de destino, compruebe que la nueva configuración es correcta: sudo yum clean all sudo yum repolist	Administrador de sistemas o Linux

Recursos relacionados

- Guía del usuario de AWS Application Migration Service (AWS MGN)
- Obtenga soporte para un paquete de cliente RHUI de AWS IMDSv2 (artículo de la base de conocimiento de Red Hat)
- Plantillas de lanzamiento de Amazon EC2 (documentación de Amazon EC2)

Migre una base de datos local de Microsoft SQL Server a Amazon EC2

Senthil Ramasamy, Amazon Web Services

Resumen

Este patrón describe cómo migrar una base de datos de Microsoft SQL Server local a Microsoft SQL Server en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Incluye dos opciones de migración: usar AWS Database Migration Service (AWS DMS) o usar herramientas nativas de Microsoft SQL Server, como la copia de seguridad y la restauración, el asistente para copiar bases de datos o copiar y adjuntar bases de datos.

Requisitos previos y limitaciones

Requisitos previos

- Una AWS cuenta activa
- Un sistema operativo compatible con Amazon EC2 (para obtener una lista completa de las versiones de sistemas operativos compatibles, consulte Amazon EC2 FAQs)
- Una base de datos de origen de Microsoft SQL Server en un centro de datos en las instalaciones

Versiones de producto

- Para las bases de datos locales y de EC2 instancias de Amazon, AWS DMS admite:
  - Versiones de SQL Server 2005, 2008, 2008R2, 2012, 2014, 2016, 2017 y 2019
  - Ediciones Enterprise, Standard, Workgroup, Developer y Web
- Para ver la lista actualizada de versiones compatibles, consulte Using a Microsoft SQL Server Database as a Target for AWS DMS.

Arquitectura

Pila de tecnología de origen

- Base de datos de Microsoft SQL Server en las instalaciones

Pila de tecnología de destino

- Base de datos de Microsoft SQL Server en una EC2 instancia

Arquitectura de destino

Arquitectura de migración de datos

- Usando AWS DMS

- Uso de herramientas nativas de SQL Server

Tools (Herramientas)

- AWS Database Migration Service (AWS DMS) le ayuda a migrar sus datos hacia y desde bases de datos comerciales y de código abierto muy utilizadas, como Oracle, SQL Server, MySQL y PostgreSQL. Puede utilizarlos AWS DMS para migrar sus datos a Nube de AWS, entre instancias locales (mediante una Nube de AWS configuración) o entre combinaciones de configuraciones locales y en la nube.
- AWS Schema Conversion Tool (AWS SCT) admite migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayoría del código personalizado a un formato compatible con la base de datos de destino.
- Las herramientas nativas de Microsoft SQL Server incluyen la copia de seguridad y restauración, el asistente para copiar bases de datos y la función de copiar y adjuntar bases de datos.

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Identificar la versión del sistema operativo de destino.		Administrador de base de datos, administrador de sistemas
Identifique los requisitos de hardware para la instancia del servidor de destino en función de la lista de compatibilidad de Microsoft SQL Server y los requisitos de capacidad.		Administrador de base de datos, administrador de sistemas
Identificar los requisitos de almacenamiento relativos al tipo y la capacidad.		Administrador de base de datos, administrador de sistemas
Identificar los requisitos de la red, como la latencia y el ancho de banda.		Administrador de base de datos, administrador de sistemas
Elija el tipo de EC2 instancia en función de la capacidad , las características de almacenamiento y las características de la red.		Administrador de base de datos, administrador de sistemas
Identificar los requisitos de seguridad para acceder a la red y al host de las bases de datos de origen y destino.		Administrador de base de datos, administrador de sistemas
Identificar la lista de usuarios necesarios para la instalaci ón del software Microsoft SQL Server.		Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Determinar la estrategia de copia de seguridad.		Administrador de base de datos
Determinar los requisitos de disponibilidad.		Administrador de base de datos
Identificar la estrategia de migración y transición de aplicaciones.		Administrador de base de datos, administrador de sistemas

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC) y subredes.		Administrador de sistemas
Cree grupos de seguridad y listas de control de acceso a la red (ACL).		Administrador de sistemas
Configura e inicia una EC2 instancia.		Administrador de sistemas

Instalar el software

Tarea	Descripción	Habilidades requeridas
Crear los usuarios y grupos necesarios para el software Microsoft SQL Server.		Administrador de base de datos, administrador de sistemas
Descargar el software Microsoft SQL Server.		Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Instale el software Microsoft SQL Server en la EC2 instancia y configure el servidor.		Administrador de base de datos, administrador de sistemas

Migración de datos: opción 1

Tarea	Descripción	Habilidades requeridas
Utilizar herramientas nativas de MySQL Server o herramientas de terceros para migrar los objetos y datos de la base de datos.	Las herramientas incluyen la copia de seguridad y la restauración, el asistente para copiar bases de datos y la función de copiar y adjuntar bases de datos. Para obtener más información, consulte la guía Migrating Microsoft SQL Server databases to the Nube de AWS.	Administrador de base de datos

Migración de datos: opción 2

Tarea	Descripción	Habilidades requeridas
Migre los datos mediante AWS DMS.	Para obtener más información sobre su uso AWS DMS, consulte los enlaces de la sección Recursos relacionados.	Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de migración de aplicaciones.	Utilice AWS Schema Conversion Tool (AWS SCT) para analizar y modificar el código SQL que está incrustado en el código fuente de la aplicación.	Administrador de base de datos, propietario de la aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de cambio de aplicaciones.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cierre todos los AWS recursos temporales.	Los recursos temporales incluyen la instancia de AWS DMS replicación y la EC2 instancia para AWS SCT.	Administrador de base de datos, administrador de sistemas
Revise y valide los documentos del proyecto.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Recopile métricas sobre el tiempo de migración		Administrador de base de datos, propietario de la

Tarea	Descripción	Habilidades requeridas
, el porcentaje de ahorro de costos manuales en comparación con los de herramientas, etc.		aplicación, administrador de sistemas
Cerrar el proyecto y enviar comentarios.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Recursos relacionados

Referencias

- Migración de bases de datos de Microsoft SQL Server a Nube de AWS
- Amazon EC2
- Amazon EC2 FAQs
- EC2 Precios de Amazon
- AWS Database Migration Service
- Productos de Microsoft en AWS
- Licencias de Microsoft en AWS
- Microsoft SQL Server en AWS

Tutoriales y videos

- Cómo empezar con Amazon EC2
- Introducción a AWS Database Migration Service
- Unir una EC2 instancia de Amazon a su Active Directory de Simple AD
- Unir una EC2 instancia de Amazon a su AWS Managed Microsoft AD Active Directory
- AWS Database Migration Service (video)
- Introducción a Amazon EC2 : Elastic Cloud Server & Hosting con AWS (vídeo)

Vuelva a alojar las cargas de trabajo en las instalaciones en la nube de AWS: lista de verificación de migración

Srikanth Rangavajhala, Amazon Web Services

Resumen

Volver a alojar las cargas de trabajo en las instalaciones en la nube de Amazon Web Services (AWS) implica las siguientes fases de migración: planificación, predetección, detección, creación, prueba y transición. Este patrón describe las fases y sus tareas relacionadas. Las tareas se describen de forma detallada y soportan aproximadamente el 75 % de todas las cargas de trabajo de las aplicaciones. Puede implementar estas tareas en un plazo de dos o tres semanas en un ciclo de iteraciones ágil.

Debería revisar y examinar estas tareas con su equipo de migración y sus consultores. Tras la revisión, puede recopilar los datos, eliminar o volver a evaluar las tareas según sea necesario para cumplir con sus requisitos y modificar otras tareas para que admitan al menos el 75 % de las cargas de trabajo de las aplicaciones de su cartera. A continuación, puede utilizar una herramienta de gestión de proyectos ágil, como Atlassian Jira o Rally Software, para importar las tareas, asignarlas a los recursos y realizar un seguimiento de las actividades de migración.

El patrón supone que utiliza AWS Cloud Migration Factory para volver a alojar sus cargas de trabajo, pero puede utilizar la herramienta de migración que prefiera.

Amazon Macie puede ser útil para identificar información confidencial en sus bases de conocimiento, que se almacenan como orígenes de datos, registros de invocación de modelos y almacenes de peticiones en buckets de Amazon Simple Storage Service (Amazon S3). Para obtener más información, consulte la documentación de Macie.

Requisitos previos y limitaciones

Requisitos previos

- Herramienta de gestión de proyectos para realizar un seguimiento de las tareas de migración (por ejemplo, Atlassian Jira o Rally Software)
- Herramienta de migración para volver a alojar sus cargas de trabajo en AWS (por ejemplo, Cloud Migration Factory)

Arquitectura

Plataforma de origen

- Pila de origen en las instalaciones (incluidas tecnologías, aplicaciones, bases de datos e infraestructura)

Plataforma de destino

- Pila de destino en la nube de AWS (incluidas tecnologías, aplicaciones, bases de datos e infraestructura)

Arquitectura

En el siguiente diagrama, se muestra el realojamiento (detección y migración de servidores desde un entorno de origen en las instalaciones a AWS) mediante Cloud Migration Factory y AWS Application Migration Service.

Tools (Herramientas)

- Puede utilizar la herramienta de migración y gestión de proyectos que elija.

Epics

Fase de planificación

Tarea	Descripción	Habilidades requeridas
Prepare el volumen de trabajo pendiente previo a la detección.	Lleve a cabo la sesión de trabajo previa a la detección de los volúmenes de trabajo pendientes con los jefes de departamento y los propietar ios de las aplicaciones.	Director de proyectos, líder de Agile Scrum
Dirija la sesión de trabajo de planificación de la iteración.	Como ejercicio de análisis, distribuya las aplicaciones que	Director de proyectos, líder de Agile Scrum

Tarea	Descripción	Habilidades requeridas
	desee migrar entre iteraciones y oleadas.	

Fase previa a la detección

Tarea	Descripción	Habilidades requeridas
Confirmar los conocimientos de la aplicación.	Confirme y documente al propietario de la aplicació n y su conocimiento de la aplicación. Determinar si hay otra persona de contacto para las cuestiones técnicas.	Especialista en migración (entrevistador)
Determine los requisitos de conformidad de las aplicacio nes.	Confirme con el propietario de la aplicación que la aplicació n no tiene por qué cumplir los requisitos del estándar de seguridad de datos del sector de las tarjetas de pago (PCI DSS), la Ley Sarbanes-Oxley (SOX), la información de identificación personal (PII) u otras normas. Si existen requisitos de conformidad, los equipos deben finalizar las comprobaciones de conformid ad en los servidores que se van a migrar.	Especialista en migración (entrevistador)
Confirme los requisitos de lanzamiento de producción.	Confirme los requisitos para lanzar la aplicación migrada a producción (como la fecha de lanzamiento y la duración del tiempo de inactividad) con el	Especialista en migración (entrevistador)

Tarea	Descripción	Habilidades requeridas
	propietario de la aplicación o el contacto técnico.	
Obtener la lista de servidores.	Obtenga la lista de servidores asociados a la aplicación de destino.	Especialista en migración (entrevistador)
Obtener el diagrama lógico que muestra el estado actual.	Obtenga el diagrama de estado actual de la aplicación del arquitecto empresarial o del propietario de la aplicación.	Especialista en migración (entrevistador)
Crear un diagrama lógico que muestre el estado objetivo.	Cree un diagrama lógico de la aplicación que muestre la arquitectura de destino en AWS. Este diagrama debe ilustrar los servidores, la conectividad y los factores de asignación.	Arquitecto empresarial, propietario de una empresa
Obtener información sobre el servidor.	Recopile información sobre los servidores asociados a la aplicación, incluidos sus detalles de configuración.	Especialista en migración (entrevistador)

Tarea	Descripción	Habilidades requeridas
Añada la información del servidor a la plantilla de detección.	Añada información detallada del servidor a la plantilla de detección de aplicaciones (consulte `mobilize-application-questionnaire.xlsx` en el anexo de este patrón). Esta plantilla incluye todos los detalles de seguridad, infraestructura, sistema operativo y redes relacionados con las aplicaciones.	Especialista en migración (entrevistador)
Publicar la plantilla de detección de aplicaciones.	Comparta la plantilla de detección de aplicaciones con el propietario de la aplicación y el equipo de migración para un acceso y un uso comunes.	Especialista en migración (entrevistador)

Fase de detección

Tarea	Descripción	Habilidades requeridas
Confirmar la lista de servidores.	Confirme la lista de servidores y el propósito de cada servidor con el propietario de la aplicación o el responsable técnico.	Especialista de migración
Identificar y añadir grupos de servidores.	Identifique grupos de servidores, como servidores web o servidores de aplicaciones, y añada esta información a la plantilla de detección	Especialista de migración

Tarea	Descripción	Habilidades requeridas
	de aplicaciones. Seleccione el nivel de la aplicación (web, aplicación, base de datos) al que debe pertenecer cada servidor.	
Publicar la plantilla de detección de aplicaciones.	Complete los detalles de la plantilla de detección de aplicaciones con la ayuda del equipo de migración, el equipo de aplicaciones y AWS.	Especialista de migración
Añada los detalles del servidor que faltan (equipos de middleware y sistema operativo).	Pida a los equipos de middleware y sistema operativo (SO) que revisen la plantilla de detección de aplicaciones y añadan los detalles del servidor que falten, incluida la información de la base de datos.	Especialista de migración
Obtenga las normas de inbound/outbound tráfico (equipo de red).	Pida al equipo de red que obtenga las reglas de inbound/outbound tráfico para los servidores de origen y destino. El equipo de red también debe añadir las reglas de firewall existentes, exportarlas a un formato de grupo de seguridad y añadir los equilibradores de carga existentes a la plantilla de detección de aplicaciones.	Especialista de migración
Identificar el etiquetado necesario.	Determine los requisitos de etiquetado de la aplicación.	Especialista de migración

Tarea	Descripción	Habilidades requeridas
Crear detalles de solicitud de firewall.	Capture y filtre las reglas de firewall necesarias para comunicarse con la aplicación.	Especialista en migración, arquitecto de soluciones y líder de redes
Actualiza el tipo de EC2 instancia.	Actualice el tipo de instancia de Amazon Elastic Compute Cloud (Amazon EC2) para que se utilice en el entorno de destino, en función de los requisitos de infraestructura y servidor.	Especialista en migración, arquitecto de soluciones y líder de redes
Identifique el diagrama de estado actual.	Identifique o cree el diagrama que muestra el estado actual de la aplicación. Este diagrama se utilizará en la solicitud de seguridad de la información (InfoSec).	Especialista en migración, arquitecto de soluciones
Finalice el diagrama de estado futuro.	Finalice el diagrama que muestra el estado futuro (destino) de la aplicación. Este diagrama también se utilizará en la InfoSec solicitud.	Especialista en migración, arquitecto de soluciones
Cree solicitudes de servicio de firewall o grupo de seguridad.	Cree solicitudes de servicios de firewall o grupos de seguridad (para desarrollo, control de calidad, preproducción y producción). Si utiliza Cloud Migration Factory, incluya puertos específicos para la replicación si aún no están abiertos.	Especialista en migración, arquitecto de soluciones y líder de redes

Tarea	Descripción	Habilidades requeridas
Revise las solicitudes de firewall o grupos de seguridad (InfoSec equipo).	En este paso, el InfoSec equipo revisa y aprueba las solicitudes de firewall o grupo de seguridad que se crearon en el paso anterior.	InfoSec ingeniero, especialista en migración
Implemente las solicitudes de grupos de seguridad de firewall (equipo de red).	Una vez que el InfoSec equipo aprueba las solicitudes de firewall, el equipo de red implementa las reglas de inbound/outbound firewall requeridas.	Especialista en migración, arquitecto de soluciones y líder de redes

Fase de construcción (repita para los entornos de desarrollo/control de calidad, preproducción y producción)

Tarea	Descripción	Habilidades requeridas
Importe los datos de la aplicación y del servidor.	1. Compruebe que ha iniciado sesión en el servidor de ejecución de la migración como usuario del dominio con permisos de administrador local en los servidores de origen incluidos en el ámbito de aplicación. 2. Utilice el formulario de admisión de la migración para importar los atributos de los servidores de origen incluidos en el ámbito de aplicación. Para obtener información adicional , consulte la Guía de	Especialista en migración, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	implementación de Cloud Migration Factory. Si no utiliza Cloud Migration Factory, siga las instrucciones para configurar su herramienta de migración.	
Compruebe los requisitos previos de los servidores de origen.	Conéctese con los servidores de origen incluidos en el ámbito para comprobar los requisitos previos, como el puerto TCP 1500, el puerto TCP 443, el espacio libre del volumen raíz, la versión de .NET Framework y otros parámetros. Estos son necesarios para la replicación. Para obtener información adicional, consulte la Guía de implementación de Cloud Migration Factory.	Especialista en migración, administrador de la nube
Cree una solicitud de servicio para instalar agentes de replicación.	Cree una solicitud de servicio para instalar los agentes de replicación en los servidores incluidos para fines de desarrollo, control de calidad, preproducción o producción.	Especialista en migración, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Instale los agentes de replicación.	Instale los agentes de replicación en los servidores de origen incluidos en los equipos de desarrollo, control de calidad, preproducción o producción. Para obtener información adicional, consulte la Guía de implementación de Cloud Migration Factory.	Especialista en migración, administrador de la nube
Inserte los scripts posteriores al lanzamiento.	Application Migration Service admite scripts posteriores al lanzamiento para ayudarlo a automatizar las actividades a nivel del sistema operativo, como la instalación o desinstalación del software después de lanzar las instancias de destino. Este paso envía los scripts posteriores al lanzamiento a equipos Windows o Linux, en función de los servidores identificados para la migración. Para obtener instrucciones, consulte la Guía de implementación de Cloud Migration Factory.	Especialista en migración, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Verificar el estado de la replicación.	Confirme automáticamente el estado de la replicación de los servidores de origen incluidos en el ámbito de aplicación mediante el script proporcio nado. El script se repite cada cinco minutos hasta que el estado de todos los servidore s de origen de la oleada en cuestión cambie a Correcto. Para obtener instrucciones, consulte la Guía de implement ación de Cloud Migration Factory.	Especialista en migración, administrador de la nube
Cree el usuario administrador.	Es posible que se necesite un administrador local o un usuario de sudo en los equipos de origen para solucionar cualquier problema tras la transición de la migración de los servidore s de origen incluidos en el ámbito a AWS. El equipo de migración utiliza este usuario para iniciar sesión en el servidor de destino cuando no se puede acceder al servidor de autenticación (por ejemplo, el servidor DC o LDAP). Para obtener instrucciones para este paso, consulte la Guía de implementación de Cloud Migration Factory.	Especialista en migración, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Valide la plantilla de lanzamiento.	Valide los metadatos del servidor para asegurarse de que funcionan correctamente y que no contienen datos no válidos. Este paso valida los metadatos de prueba y de transición. Para obtener instrucciones, consulte la Guía de implementación de Cloud Migration Factory.	Especialista en migración, administrador de la nube

Fase de prueba (repita para los entornos de desarrollo/control de calidad, preproducción y producción)

Tarea	Descripción	Habilidades requeridas
Cree una solicitud de servicio.	Cree una solicitud de servicio para que el equipo de infraestructura y otros equipos realicen la transición de las aplicaciones a las instancias de desarrollo, control de calidad, preproducción o producción.	Especialista en migración, administrador de la nube
Configure un equilibrador de carga (opcional).	Configure los equilibradores de carga necesarios, como un Equilibrador de carga de aplicación o un equilibrador de cargas F5 con iRules.	Especialista en migración, administrador de la nube
Inicie instancias para realizar pruebas.	Inicie todos los equipos de destino de una oleada determinada en Application Migration Service en modo de prueba. Para obtener	Especialista en migración, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	información adicional, consulte la Guía de implementación de Cloud Migration Factory.	
Verifique el estado de la instancia de destino.	Verifique el estado de la instancia de destino comprobando el proceso de arranque de todos los servidores de origen incluidos en la misma oleada. Las instancias de destino pueden tardar hasta 30 minutos en iniciarse. Para comprobar el estado manualmente, inicia sesión en la EC2 consola de Amazon, busca el nombre del servidor de origen y revisa la columna Comprobación de estado. Las dos comprobaciones de estado aprobadas indican que la instancia está en buen estado desde el punto de vista de la infraestructura.	Especialista en migración, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Modifique las entradas de DNS.	Modifique las entradas del sistema de nombres de dominio (DNS). (Utilice `resolv.conf` o `host.conf` para un entorno Microsoft Windows). Configura cada EC2 instancia para que apunte a la nueva dirección IP de este host. **Note** Asegúrese de que no haya conflictos de DNS entre los servidores en las instalaciones y los de la nube de AWS. Este paso y los siguiente s son opcionales, según el entorno en el que esté alojado el servidor.	Especialista en migración, administrador de la nube
Pruebe la conectividad con los hosts de back-end desde EC2 las instancias.	Compruebe los inicios de sesión con las credenciales de dominio de los servidores migrados.	Especialista en migración, administrador de la nube
Actualice el registro A de DNS.	Actualiza el registro A de DNS de cada host para que apunte a la nueva dirección IP EC2 privada de Amazon.	Especialista en migración, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Actualice el registro CNAME de DNS.	Actualice el registro CNAME del DNS virtual IPs (nombres de los balanceadores de carga) para que apunte al clúster de los servidores web y de aplicaciones.	Especialista en migración, administrador de la nube
Pruebe la aplicación en los entornos aplicables.	Inicie sesión en la nueva EC2 instancia y pruebe la aplicación en los entornos de desarrollo, control de calidad, preproducción y producción.	Especialista en migración, administrador de la nube
Marque como listo para la transición.	Cuando se hayan completado las pruebas, cambie el estado del servidor de origen para indicar que está listo para la transición, de modo que los usuarios puedan iniciar una instancia de transición. Para obtener instrucciones, consulte la Guía de implementación de Cloud Migration Factory.	Especialista en migración, administrador de la nube

Fase de transición

Tarea	Descripción	Habilidades requeridas
Cree un plan de implementación de producción.	Cree un plan de implementación de producción (que incluya un plan de respaldo).	Especialista en migración, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Notifique al equipo de operaciones sobre el tiempo de inactividad.	Notifique al equipo de operaciones el programa de inactividad de los servidores. Es posible que algunos equipos necesiten un ticket de solicitud de cambio o de solicitud de servicio (CR/SR) para esta notificación.	Especialista en migración, administrador de la nube
Replique los equipos de producción.	Replique los equipos de producción mediante Application Migration Service u otra herramienta de migración.	Especialista en migración, administrador de la nube
Cierre los servidores de origen incluidos en el ámbito de aplicación.	Tras comprobar el estado de replicación de los servidores de origen, puede cerrar los servidores de origen para detener las transacciones de las aplicaciones cliente a los servidores. Puede cerrar los servidores de origen en la ventana de transición. Para obtener más información, consulte la Guía de implementación de Cloud Migration Factory.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Inicie instancias para la transición.	Inicie todos los equipos de destino de una oleada determinada en Application Migration Service en modo de transición. Para obtener más información, consulte la Guía de implementación de Cloud Migration Factory.	Especialista en migración, administrador de la nube
Recupere la instancia de destino. IPs	Recupera IPs las cuatro instancias de destino. Si la actualización del DNS es un proceso manual en su entorno, necesitará obtener las nuevas direcciones IP de todas las instancias de destino. Para obtener más información, consulte la Guía de implementación de Cloud Migration Factory.	Especialista en migración, administrador de la nube
Verifique las conexiones del servidor de destino.	Tras actualizar los registros DNS, puede conectarse a las instancias de destino con el nombre de host para comprobar las conexiones. Para obtener más información, consulte la Guía de implementación de Cloud Migration Factory.	Especialista en migración, administrador de la nube

Recursos relacionados

- ¿Cómo migrar?

- Guía de implementación de AWS Cloud Migration Factory
- Automatizar las migraciones de servidores a gran escala con Cloud Migration Factory
- Guía de usuario del servicio de migración de aplicaciones de AWS
- Programa de aceleración de la migración AWS

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Configure una infraestructura Multi-AZ para una FCI Always On de SQL Server mediante Amazon FSx

Manish Garg, T.V.R.L. Phani Kumar Dadi, Nishad Mankar y RAJNEESH TYAGI, Amazon Web Services

Resumen

Si necesita migrar rápidamente un gran número de instancias de clúster de conmutación por error Always On de Microsoft SQL Server (FCIs), este patrón puede ayudarle a minimizar el tiempo de aprovisionamiento. Al utilizar la automatización y Amazon FSx for Windows File Server, se reducen los esfuerzos manuales, los errores cometidos por el hombre y el tiempo necesario para implementar una gran cantidad de clústeres.

Este patrón configura la infraestructura de SQL Server FCIs en una implementación de zona de disponibilidad múltiple (Multi-AZ) en Amazon Web Services (AWS). El aprovisionamiento de los servicios de AWS necesarios para esta infraestructura se automatiza mediante CloudFormation plantillas de AWS. La instalación de SQL Server y la creación de nodos de clúster en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) se realizan mediante PowerShell comandos.

Esta solución utiliza un sistema de archivos Amazon FSx para Windows Multi-AZ de alta disponibilidad como testigo compartido para almacenar los archivos de la base de datos de SQL Server. El sistema de FSx archivos de Amazon y las instancias de EC2 Windows que alojan SQL Server se unen al mismo dominio de AWS Directory Service para Microsoft Active Directory (AWS Managed Microsoft AD).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un usuario de AWS con permisos suficientes para aprovisionar recursos mediante CloudFormation plantillas de AWS
- AWS Directory Service para Microsoft Active Directory
- Credenciales en AWS Secrets Manager para autenticarse en AWS Managed Microsoft AD en un par clave-valor:
  - `ADDomainName`: <Nombre del dominio>
  - `ADDomainJoinUserName`: <Nombre-de-usuario>

- `ADDomainJoinPassword`: <Domain User Password>
- `TargetOU`: <Target OU Value>

> **Note**
>
> Utilizará el mismo nombre clave en la automatización de AWS Systems Manager para la actividad de unión a AWS Managed Microsoft AD.

- Archivos multimedia de SQL Server para la instalación de SQL Server y la creación de cuentas de servicio o dominio de Windows, que se utilizarán durante la creación del clúster
- Una nube privada virtual (VPC), con dos subredes públicas en zonas de disponibilidad independientes, dos subredes privadas en las zonas de disponibilidad, una puerta de enlace de Internet, puertas de enlace NAT, asociaciones de tablas de enrutamiento y un servidor Jump

Versiones de producto

- Microsoft Windows Server 2012 R2 y Microsoft SQL Server 2016

Arquitectura

Pila de tecnología de origen

- SQL Server local con el FCIs uso de una unidad compartida

Pila de tecnología de destino

- EC2 Instancias de AWS
- Servidor FSx de archivos Amazon para Windows
- Manual de procedimiento de Automatización de AWS Systems Manager
- Configuraciones de red (VPC, subredes, puerta de enlace de Internet, puertas de enlace NAT, servidor de salto, grupos de seguridad)
- AWS Secrets Manager
- AWS Managed Microsoft AD
- Amazon EventBridge
- AWS Identity y Access Management (IAM)

Arquitectura de destino

El siguiente diagrama muestra una cuenta de AWS en una sola región de AWS, con una VPC que incluye dos zonas de disponibilidad, dos subredes públicas con puertas de enlace NAT, un servidor de salto en la primera subred pública, dos subredes privadas, cada una con una EC2 instancia para un nodo de SQL Server en un grupo de seguridad de nodos, y un sistema de FSx archivos de Amazon que se conecta a cada uno de los nodos de SQL Server. También se incluyen AWS Directory Service EventBridge, Amazon, AWS Secrets Manager y AWS Systems Manager.

Automatización y escala

- Puede usar AWS Systems Manager para unirse a AWS Managed Microsoft AD y realizar la instalación de SQL Server.

Tools (Herramientas)

Servicios de AWS

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS Directory Service ofrece varias formas de utilizar Microsoft Active Directory (AD) con otros servicios de AWS, como Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS) para SQL Server y FSx Amazon para Windows File Server.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, las funciones de AWS Lambda, los puntos de conexión de invocación HTTP que utilizan destinos de API o los buses de eventos de otras cuentas de AWS.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Secrets Manager le permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.

- AWS Systems Manager le permite administrar las aplicaciones y la infraestructura que se ejecutan en la nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo requerido para detectar y resolver problemas operativos y ayuda a utilizar y administrar los recursos de AWS a escala de manera segura.

Otras herramientas

- PowerShelles un programa de administración de automatización y configuración de Microsoft que se ejecuta en Windows, Linux y macOS. Este patrón utiliza PowerShell scripts.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub aws-windows-failover-cluster-automation.

Prácticas recomendadas

- Las funciones de IAM que se utilizan para implementar esta solución deben cumplir con el principio de privilegios mínimos. Para obtener más información, consulte la documentación de IAM.
- Siga las prácticas CloudFormation recomendadas de AWS.

Epics

Implementación de la infraestructura

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation pila Systems Manager.	1. Inicie sesión en su cuenta de AWS y abra la consola de administración de AWS. 2. Navegue hasta la CloudFormation consola y cargue la `ssm.yaml` plantilla para crear la CloudFormation pila de Systems Manager.	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Proporcione valores para los siguientes parámetros: • StateUnJoinAssociationLoggingBucketName— Proporcione un nombre para el depósito de S3 que la plantilla creará con fines de registro. • SSMAssociationADUnjoinNombre: proporcione un nombre para el `AWS::SSM::Association` recurso. • SSMAutomationDocumentName— Proporcione un nombre para el manual de automatización de Systems Manager. • EventBridgeName— Proporcione un nombre para el bus de EventBridge eventos. 3. Implemente la CloudFormation pila de Systems Manager lanzando la `ssm.yaml` CloudFormation plantilla. La plantilla creará el manual de ejecución de Systems Manager Automation que se iniciará cuando se lance una nueva EC2 instancia con	

Tarea	Descripción	Habilidades requeridas
	la etiqueta. `ADJoined: FSXADD` El manual de procedimiento de Automation añadirá la instancia al directorio de AWS Managed Microsoft AD.	

Tarea	Descripción	Habilidades requeridas
Implemente la pila de infraestructuras.	Tras implementar correctamente la pila de Systems Manager, cree la `infra` pila, que incluye los nodos de EC2 instancia, los grupos de seguridad, el sistema de archivos Amazon FSx for Windows File Server y la función de IAM. 1. Navegue hasta la CloudFormation consola e inicie la `infra-cf.yaml` plantilla. Para implementar esta pila, se requieren los siguientes parámetros: • `ActiveDirectoryId` : Identificador de AWS Managed Microsoft AD • `ADDnsIpAddresses1` : Dirección IP DNS principal de AWS Managed Microsoft AD • `ADDnsIpAddresses2` : Dirección IP DNS secundaria de Microsoft AD gestionado por AWS • `FSxSecurityGroupName` — Nombre del grupo de FSx seguridad de Amazon • `FSxWindowsFileSystemName` — Nombre de la FSx unidad Amazon	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• `ImageID`: Identificador de la imagen base de Windows 2012 R2 o Imagen de máquina de Amazon (AMI) utilizada para crear el nodo de instancia de SQL Server • `KeyPairName` — Par clave-valor para adjuntar a los nodos de la EC2 instancia para su acceso • `Node1SecurityGroupName` : Nombre del grupo de seguridad del primer nodo • `Node2SecurityGroupName` : Nombre del grupo de seguridad del segundo nodo • `OUSecretName` : Nombre del secreto que contiene la informaci ón de AWS Managed Microsoft AD • `PrivateSubnet1` : Identificador de la primera subred privada • `PrivateSubnet2` : Identificador de la segunda subred privada • `SqlFSxFCIName` — Nombre de la etiqueta aplicada a los nodos	

Tarea	Descripción	Habilidades requeridas
	principal y secundario y a Amazon FSx. • `SqlFSxServerNetBIOSName1` — Nombre del nodo de la EC2 instancia principal (15 caracteres como máximo) • `SqlFSxServerNetBIOSName2` — Nombre del nodo de EC2 instancia secundario (15 caracteres como máximo) • `VPC`: ID de VPC • `WorkloadInstanceType` — Tipo de EC2 instancia Implemente la pila de `infra`. La pila creará todos los componentes de infraestructura necesarios para configurar la FCI de Windows SQL Server. 2. Una vez lanzados los nodos de la EC2 instancia, se invocará el documento de automatización de Systems Manager para unir estas instancias a AWS Managed Microsoft AD. Puede realizar un seguimiento del progreso en la página Automatiz	

Tarea	Descripción	Habilidades requeridas
	ación de la consola de Systems Manager.	

Configure el Windows SQL Server Always On FCI

Tarea	Descripción	Habilidades requeridas

Instale las herramientas de Windows.	1. Inicie sesión en la EC2 instancia principal, que es el nodo 1. Para instalar las funciones de Windows (Active Directory y FCI Tools), ejecute el siguiente PowerShell script.
	`Install-WindowsFeature -Name RSAT-AD-Powershell,Failover-Clustering -IncludeManagementTools`
	`Install-WindowsFeature -Name RSAT-Clustering,RSAT-ADDS-Tools,RSAT-AD-Powershell,RSAT-DHCP,RSAT-DNS-Server`
	2. Inicie sesión en la EC2 instancia secundaria, que es el nodo 2, y ejecute el mismo script para habilitar las funciones en el nodo 2.
		AWS DevOps, DevOps ingeniero, administrador de bases de datos

Preconfigure los objetos informáticos del clúster en los servicios de dominio de Active Directory.	Para preconfigurar el objeto de nombre de clúster (CNO) en los Servicios de dominio de Active Directory (AD DS)	AWS DevOps, administrador de bases de datos, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	y preconfigurar un objeto de equipo virtual (VCO) para una función agrupada, siga las instrucciones de Documentación de Windows Server.	

Tarea	Descripción	Habilidades requeridas
Cree el WSFC.	Para crear el Clúster de Conmutación por error de Windows Server (WSFC), haga lo siguiente: 1. Inicie sesión en la EC2 instancia principal, que es el nodo 1. Para crear el recurso compartido de FSx archivos de Amazon y conceder acceso total a la cuenta de servicio de AD que aparece en la lista, ejecuta el siguiente código. `Invoke-Command -ComputerName "<FSx Windows Remote PowerShell Endpoint>" -ConfigurationName FSxRemoteAdmin -scriptblock { New-FSxSmbShare -Name "SQLDB" -Path "D:\share" -Description "SQL Databases Share" -ContinuouslyAvailable $true -FolderEnumerationMode AccessBased -EncryptData $true grant-fsxsmbshareaccess -name SQLDB -AccountName "<domain\user>" -accessRight Full }`	AWS DevOps, administrador de bases de datos, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	Este comando también creará el recurso compartido de archivos disponible de forma continua (CA), que está optimizado para su uso en Microsoft SQL Server. 2. Para crear el clúster de conmutación por error en la instancia principal (nodo 1), ejecute el siguiente comando. `New-Cluster -Name <CNO Name> -Node <Node1 Name>, <Node2 Name> -StaticAddress <Node1 Secondary Private IP>, <Node2 Secondary Private IP>` El comando requiere los siguientes parámetros: • `Name`: el nombre del clúster (CNO) • `Node`: los nombres de los nodos principal y secundario, respectivamente • `StaticAddress` : las direcciones IP secundarias de los nodos principal y secundario, respectivamente	

Tarea	Descripción	Habilidades requeridas
	Important Un administrador de dominio o un usuario normal debe tener permiso de administrador en ambos nodos para crear el clúster de conmutación por error de Windows Server (WSFC). De lo contrario, el comando anterior fallará y devolverá el mensaje, `You do not have administrator privilege on servers`. 3. Una vez creado el clúster, ejecute el comando siguiente para adjuntar el testigo del recurso compartido de archivos. `Set-ClusterQuorum -FileShareWitness \ \<FSx Windows Remote PowerShell Endpoint> \share\witness`	

Tarea	Descripción	Habilidades requeridas
Instale el clúster de conmutación por error de SQL Server.	Una vez configurado el clúster de WSFC, instale el clúster de SQL Server en la instancia principal (node1). 1. En la unidad T de ambos nodos, cree carpetas `tempdb` y `log` Las carpetas se utilizan en los PowerShell comandos. 2. Después de copiar los archivos multimedia de SQL Server para la instalación de SQL Server en ambos nodos, ejecute el siguiente PowerShell comando en el nodo 1 para instalar SQL Server en el nodo 1. `D:\setup.exe /Q ` `/ACTION=InstallFailoverCluster ` `/IACCEPTSQLSERVERLICENSETERMS ` `/FEATURES="SQL,IS,BC,Conn" ` `/INSTALLSHAREDDIR="C:\Program Files\Microsoft SQL Server" ` `/INSTALLSHAREDWOWDIR="C:\Program Files (x86)\Microsoft SQL Server" ` `/RSINSTALLMODE="FilesOnlyMode" ` `/INSTANCEID="MSSQLSERVER" `	AWS DevOps, administrador de bases de datos, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	`/INSTANCENAME="MSSQLSERVER" ` `/FAILOVERCLUSTERGROUP="SQL Server (MSSQLSERVER)" ` `/FAILOVERCLUSTERIPADDRESSES="IPv4;<2nd Sec Private Ip node1>;Cluster Network 1;<subnet mask>" ` `/FAILOVERCLUSTERNETWORKNAME="<Fail over cluster Network Name>" ` `/INSTANCEDIR="C:\Program Files\Microsoft SQL Server" ` `/ENU="True" ` `/ERRORREPORTING=0 ` `/SQMREPORTING=0 ` `/SAPWD="<Domain User password>" ` `/SQLCOLLATION="SQL_Latin1_General_CP1_CI_AS" ` `/SQLSYSADMINACCOUNTS="<domain\username>" ` `/SQLSVCACCOUNT="<domain\username>" /SQLSVCPASSWORD="<Domain User password>" ` `/AGTSVCACCOUNT="<domain\username>" /AGTSVCPASSWORD="<Domain User password>" ` `/ISSVCACCOUNT="<domain\username>" /ISSVCPASSWORD="<Domain User password>" `	

Tarea	Descripción	Habilidades requeridas
	`/FTSVCACCOUNT="NT Service\MSSQLFDLauncher" ` `/INSTALLSQLDATADIR="\\<FSX DNS name>\share\Program Files\Microsoft SQL Server" ` `/SQLUSERDBDIR="\\<FSX DNS name>\share\data" ` `/SQLUSERDBLOGDIR="\\<FSX DNS name>\share\log" ` `/SQLTEMPDBDIR="T:\tempdb" ` `/SQLTEMPDBLOGDIR="T:\log" ` `/SQLBACKUPDIR="\\<FSX DNS name>\share\SQLBackup" ` `/SkipRules=Cluster_VerifyForErrors ` `/INDICATEPROGRESS`	

Tarea	Descripción	Habilidades requeridas
Agregue un nodo secundario al clúster.	Para añadir SQL Server al nodo secundario (nodo 2), ejecute el siguiente PowerShell comando. `D:\setup.exe /Q  ` `/ACTION=AddNode ` `/IACCEPTSQLSERVERLICENSETERMS ` `/INSTANCENAME="MSSQLSERVER"  ` `/FAILOVERCLUSTERGROUP="SQL Server (MSSQLSERVER)" ` `/FAILOVERCLUSTERIPADDRESSES="IPv4;<2nd Sec Private Ip node2>;Cluster Network 2;<subnet mask>" ` `/FAILOVERCLUSTERNETWORKNAME="<Fail over cluster Network Name>" ` `/CONFIRMIPDEPENDENCYCHANGE=1 ` `/SQLSVCACCOUNT="<domain\username>"  /SQLSVCPASSWORD="<Domain User password>" ` `/AGTSVCACCOUNT="domain\username>"  /AGTSVCPASSWORD="<Domain User password>" ` `/FTSVCACCOUNT="NT Service\MSSQLFDLauncher" ` `/SkipRules=Cluster_VerifyForErrors `	AWS DevOps, administrador de bases de datos, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	`/INDICATEPROGRESS`	
Pruebe la FCI de SQL Server.	1. En la instancia de Windows de uno de los nodos, en Herramientas administrativas, inicie el administrador de Clúster de conmutación por error. 2. Navegue hasta Nodos y confirme que el estado del nodo es Estado en ejecución. 3. Seleccione Roles, abra el menú contextual (haga clic con el botón derecho) de SQL Server (MSSQLSERVER) y seleccione Mover y seleccionar nodo. 4. Tras la selección del nodo, SQL Server debería estar ejecutándose en el otro nodo.	DBA, ingeniero DevOps

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Eliminación de recursos.	Para limpiar los recursos, utilice el proceso de eliminación de CloudFormation pilas de AWS: 1. Abra la CloudFormation consola de AWS.	AWS DevOps, administrador de bases de datos, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	2. En la página Pilas, seleccione la pila `infra`. La pila se debe estar ejecutando en este momento. 3. En el panel de detalles de la pila, seleccione Eliminar. 4. Seleccione Eliminar pila cuando se le indique. 5. Repita los pasos 2 a 4 para la pila de `ssm`. Una vez que se haya completado la eliminación de la pila, la pila estará en el estado `DELETE_COMPLETE` . De forma predeterminada, las pilas en ese `DELETE_COMPLETE` estado no se muestran en la CloudFormation consola. Para mostrar las pilas eliminadas, debe cambiar el filtro de vista de pilas tal y como se describe en Visualización de las pilas eliminadas en la consola de AWS CloudFormation . Si la eliminación ha fallado, la pila tendrá el estado `DELETE_FAILED` . Para obtener información sobre las soluciones, consulte los errores al eliminar una pila en	

Tarea	Descripción	Habilidades requeridas
	la CloudFormation documentación.	

Resolución de problemas

Problema	Solución
Fallo en CloudFormation la plantilla de AWS	Si la CloudFormation plantilla falla durante la implementación, haga lo siguiente: 1. Abra la CloudFormation consola de AWS. 2. En la página Stacks de la CloudFormation consola, selecciona la pila. 3. Elija Eventos y compruebe el estado de la pila.
Error de conexión de AWS Managed Microsoft AD	Para solucionar los problemas de unión, siga estos pasos: 1. Abra la consola de Systems Manager. 2. Seleccione la región de implementación. 3. En el panel izquierdo, elija Automatización y localice el manual de procedimientos de automatización fallida. 4. Abra el manual de automatización y compruebe Estado de la ejecución y Pasos de ejecución. 5. Investigue los detalles del paso fallido para ver el error o el fallo exactos.

Recursos relacionados

- Simplifique las implementaciones de alta disponibilidad de Microsoft SQL Server con Amazon FSx for Windows File Server

- Uso FSx para Windows File Server con Microsoft SQL Server

Utilice las consultas de BMC Discovery para extraer datos de migración para planificar la migración

Ben Tailor-Hamblin, Emma Baldry, Simon Cunningham y Shabnam Khan, Amazon Web Services

Resumen

Esta guía proporciona ejemplos de consultas y pasos que le ayudarán a extraer datos de su infraestructura y aplicaciones en las instalaciones mediante BMC Discovery. El patrón le muestra cómo utilizar las consultas de BMC Discovery para analizar su infraestructura y extraer información sobre el software, los servicios y las dependencias. Los datos extraídos son necesarios para las fases de evaluación y movilización de una migración a gran escala a la nube de Amazon Web Services (AWS). Puede utilizar estos datos para tomar decisiones críticas sobre qué aplicaciones migrar juntas como parte de su plan de migración.

Requisitos previos y limitaciones

Requisitos previos

- Una licencia para BMC Discovery (anteriormente BMC ADDM) o la versión de software como servicio (SaaS) de BMC Helix Discovery
- La versión de BMC Discovery en las instalaciones o SaaS instalada

> **Note**
>
> En el caso de las versiones en las instalaciones de BMC Discovery, debe instalar la aplicación en una red cliente con acceso a todos los dispositivos de red y servidor que puedan migrarse a varios centros de datos. El acceso a la red del cliente debe proporcionarse de acuerdo con las instrucciones de instalación de la aplicación. Si es necesario escanear la información de Windows Server, debe configurar un dispositivo administrador de proxy de Windows en la red.

- Acceso a la red para permitir que la aplicación escanee dispositivos en todos los centros de datos, si utiliza BMC Helix Discovery

Versiones de producto

- BMC Discovery 22.2 (12.5)

- BMC Discovery 22.1 (12.4)
- BMC Discovery 21.3 (12.3)
- BMC Discovery 21.05 (12.2)
- BMC Discovery 20.08 (12.1)
- BMC Discovery 20.02 (12.0)
- BMC Discovery 11.3
- BMC Discovery 11.2
- BMC Discovery 11.1
- BMC Discovery 11.0
- BMC Atrium Discovery 10.2
- BMC Atrium Discovery 10.1
- BMC Atrium Discovery 10.0

Arquitectura

El siguiente diagrama muestra cómo los administradores de activos pueden utilizar las consultas de BMC Discovery para escanear aplicaciones modeladas por BMC en entornos SaaS y en las instalaciones.

El diagrama muestra el siguiente flujo de trabajo: un administrador de activos utiliza BMC Discovery o BMC Helix Discovery para escanear las instancias de bases de datos y software que se ejecutan en servidores virtuales alojados en varios servidores físicos. La herramienta puede modelar aplicaciones con componentes que abarquen varios servidores físicos y virtuales.

Pila de tecnología

- BMC Discovery
- BMC Helix Discovery

Tools (Herramientas)

- BMC Discovery es una herramienta de detección de centros de datos que le ayuda a descubrir automáticamente su centro de datos.

- BMC Helix Discovery es un sistema de descubrimiento y modelado de dependencias basado en SaaS que le ayuda a modelar dinámicamente sus activos de datos y sus dependencias.

Prácticas recomendadas

Se recomienda mapear los datos de las aplicaciones, las dependencias y la infraestructura al migrar a la nube. El mapeo le ayuda a comprender la complejidad de su entorno actual y las dependencias entre los distintos componentes.

La información sobre los activos que proporcionan estas consultas es importante por varios motivos:

1. Planificación: comprender las dependencias entre los componentes le ayuda a planificar el proceso de migración de forma más eficaz. Por ejemplo, es posible que primero deba migrar algunos componentes para asegurarse de que otros se puedan migrar correctamente.
2. Evaluación de riesgos: mapear las dependencias entre los componentes puede ayudarle a identificar cualquier riesgo o problema potencial que pueda surgir durante el proceso de migración. Por ejemplo, es posible que descubra que algunos componentes se basan en tecnologías anticuadas o no compatibles, lo que podría provocar problemas en la nube.
3. Arquitectura de nube: mapear los datos de sus aplicaciones e infraestructura también puede ayudarlo a diseñar una arquitectura de nube adecuada que satisfaga las necesidades de su organización. Por ejemplo, es posible que necesite diseñar una arquitectura de varios niveles para cumplir con los requisitos de alta disponibilidad o escalabilidad.

En general, el mapeo de los datos de las aplicaciones, las dependencias y la infraestructura es un paso crucial en el proceso de migración a la nube. El ejercicio de mapeo puede ayudarlo a comprender mejor su entorno actual, identificar cualquier problema o riesgo potencial y diseñar una arquitectura de nube adecuada.

Epics

Identifique y evalúe las herramientas de descubrimiento

Tarea	Descripción	Habilidades requeridas
Identifique a los propietarios de ITSM.	Identifique a los propietarios de la administración de servicios de TI (ITSM) (por lo	Líder de migración

Tarea	Descripción	Habilidades requeridas
	general, contactando con los equipos de soporte operativo).	
Visitar CMDB.	Identifique la cantidad de bases de datos de administración de la configuración (CMDBs) que contienen información de activos y, a continuación, identifique las fuentes de esa información.	Líder de migración
Identifique las herramientas de descubrimiento y compruebe el uso de BMC Discovery.	Si su organización utiliza BMC Discovery para enviar datos sobre su entorno a la herramienta CMDB, compruebe el alcance y la cobertura de sus escaneos. Por ejemplo, compruebe si BMC Discovery escanea todos los centros de datos y si los servidores de acceso están ubicados en zonas perimetrales.	Líder de migración
Compruebe el nivel de modelado de la aplicación.	Compruebe si las aplicaciones están modeladas en BMC Discovery. Si no es así, recomiende utilizar la herramienta BMC Discovery para modelar qué instancias de software en ejecución proporcionan una aplicación y un servicio empresarial.	Ingeniero de migraciones, líder de migración

Extracción de datos de infraestructura

Tarea	Descripción	Habilidades requeridas
Extraiga datos en servidores físicos y virtuales.	Para extraer datos de los servidores físicos y virtuales escaneados por BMC Discovery, utilice Generador de consultas para ejecutar la siguiente consulta: `search Host show key as 'Serverid', virtual, name as 'HOSTNAME', os_type as 'osName', os_version as 'OS Version', num_logical_processors as 'Logical Processor Counts', cores_per_processor as 'Cores per Processor', logical_ram as 'Logical RAM', #Consumer:StorageUse:Provider:DiskDrive.size as 'Size'` **Note** Puede utilizar los datos extraídos para determinar los tamaños de instancia adecuados para la migración.	Ingeniero de migraciones, líder de migración
Extraiga datos de aplicaciones modeladas.	Si sus aplicaciones están modeladas en BMC Discovery	Propietario de la aplicación BMC Discovery

Tarea	Descripción	Habilidades requeridas
	, puede extraer datos sobre los servidores que ejecutan el software de la aplicación. Para obtener los nombres de los servidores, utilice Generador de consultas para ejecutar la siguiente consulta: `search SoftwareInstance show key as 'ApplicationID', #RunningSoftware:HostedSoftware:Host:Host.key as 'ReferenceID', type, name` **Note** Las aplicaciones se modelan en BMC Discovery mediante un conjunto de instancias de software en ejecución. La aplicación depende de todos los servidores que ejecutan el software de la aplicación.	

Tarea	Descripción	Habilidades requeridas
Extraiga datos de bases de datos.	Para obtener una lista de todas las bases de datos escaneadas y los servidores en los que se ejecutan estas bases de datos, utilice Generador de consultas para ejecutar la siguiente consulta: `search Database show key as 'Key', name, type as 'Source Engine Type', #Detail:Detail:ElementWithDetail:SoftwareInstance.name as 'Software Instance', #Detail:Detail:ElementWithDetail:SoftwareInstance.product_version as 'Product Version', #Detail:Detail:ElementWithDetail:SoftwareInstance.edition as 'Edition', #Detail:Detail:ElementWithDetail:SoftwareInstance.#RunningSoftware:HostedSoftware:Host:Host.key as 'ServerID'`	Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Extraiga datos de la comunicación con el servidor.	Para obtener información sobre todas las comunicaciones de red entre servidores recopilada por BMC Discovery a partir de los registros históricos de comunicaciones de red, utilice Generador de consultas para ejecutar la siguiente consulta: `search Host TRAVERSE InferredElement:Inference:Associate:DiscoveryAccess TRAVERSE DiscoveryAccess:DiscoveryAccessResult:DiscoveryResult:NetworkConnectionList TRAVERSE List:List:Member:DiscoveredNetworkConnection PROCESS WITH networkConnectionInfo`	Propietario de la aplicación BMC Discovery

Tarea	Descripción	Habilidades requeridas
Extraiga datos sobre el descubrimiento de aplicaciones.	Para obtener información sobre las dependencias de las aplicaciones, utilice Generador de consultas para ejecutar la siguiente consulta: `search SoftwareInstance show key as 'SRC App ID', #Dependant:Dependency:DependedUpon:SoftwareInstance.key as 'DEST App ID'`	Propietario de la aplicación BMC Discovery
Extraiga datos sobre servicios empresariales.	Para extraer datos sobre los servicios empresariales proporcionados por los hosts, utilice Generador de consultas para ejecutar la siguiente consulta: `search Host show name, #Host:HostedSoftware:AggregateSoftware:BusinessService.name as 'Name'`	Propietario de la aplicación BMC Discovery

Resolución de problemas

Problema	Solución
No se puede ejecutar una consulta o contiene columnas sin rellenar.	Revise los registros de activos de BMC Discovery y determine qué campos necesita. A continuación, sustituya estos campos en la consulta mediante Generador de consultas.

Problema	Solución
Los detalles de un activo dependiente no se rellenan.	Es probable que esto se deba a los permisos de acceso o a la conectividad de la red. Es posible que la herramienta de detección no tenga los permisos necesarios para acceder a determinados activos, especialmente si se encuentran en redes o entornos diferentes. Le recomendamos que colabore estrecham ente con expertos en la materia de descubrim iento para garantizar que se identifiquen todos los activos relevantes.

Recursos relacionados

Referencias

- Derechos de BMC Discovery Licensing (documentación de BMC)
- Características y componentes de BMC Discovery (documentación de BMC)
- Guía del usuario de BMC Discovery (documentación de BMC)
- Búsqueda de datos (en BMC Discovery) (documentación de BMC)
- Descubrimiento y análisis de carteras para la migración (Recomendaciones de AWS)

Tutoriales y videos

- BMC Discovery: seminario web sobre las mejores prácticas en materia de consultas de informes (primera parte) (YouTube)

Reubicar

Temas

- Migre una base de datos de Amazon RDS for Oracle a Cuenta de AWS otra Región de AWS y AWS DMS utilícela para la replicación continua
- Migración de una instancia de base de datos de Amazon RDS a otra VPC o cuenta
- Migración de un clúster de Amazon Redshift a una región de AWS en China
- Transportar bases de datos PostgreSQL entre dos instancias de base de datos de Amazon RDS utilizando pg_transport

Migre una base de datos de Amazon RDS for Oracle a Cuenta de AWS otra Región de AWS y AWS DMS utilícela para la replicación continua

Durga Prasad Cheepuri y Eduardo Valentim, Amazon Web Services

Resumen

Advertencia: Los usuarios de IAM tienen credenciales de larga duración, lo que supone un riesgo de seguridad. Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten.

Este patrón le guía por los pasos para migrar una base de datos fuente de Amazon Relational Database Service (Amazon RDS) para Oracle a una y diferente. Cuenta de AWS Región de AWS El patrón utiliza una instantánea de base de datos para una carga completa de datos única y habilita AWS Database Migration Service (AWS DMS) para una replicación continua.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS que contiene la base de datos Amazon RDS for Oracle de origen, que se ha cifrado con una clave AWS Key Management Service distinta de la predeterminada AWS KMS()
- Un activo Cuenta de AWS en una base de datos Región de AWS diferente a la de origen, para usarlo en la base de datos Amazon RDS for Oracle de destino
- Emparejamiento de nube privada virtual (VPC) entre el origen y el destino VPCs
- Familiaridad con el uso de una base de datos Oracle como fuente de AWS DMS
- Familiaridad con el uso de una base de datos Oracle como destino para AWS DMS

Versiones de producto

- Versiones de Oracle 11g (versiones 11.2.0.3.v1 y posteriores) hasta 12.2, y 18c. Para ver la lista más reciente de versiones y ediciones compatibles, consulte la AWS documentación sobre el uso de una base de datos Oracle como fuente AWS DMS y con el uso de una base de AWS DMS datos Oracle como destino. Para ver las versiones de Oracle compatibles con Amazon RDS, consulte Oracle en Amazon RDS.

Arquitectura

Pilas de tecnología de origen y destino

- Instancia de base de datos de Amazon RDS para Oracle

Arquitectura de replicación continua

Tools (Herramientas)

Herramientas utilizadas para la carga completa de datos de una sola vez

- Amazon Relational Database Service (Amazon RDS) crea una instantánea del volumen de almacenamiento de la instancia de base de datos; para ello, hace una copia de seguridad de toda la instancia de base de datos y no solo de las bases de datos individuales. Cuando se crea una instantánea de base de datos, se debe identificar la instancia de base de datos cuya copia de seguridad se va a realizar y, a continuación, se debe asignar un nombre a la instantánea de base de datos para poder restaurarla posteriormente. El tiempo que tarda en crearse una instantánea varía en función del tamaño de sus bases de datos. Debido a que la instantánea incluye todo el volumen de almacenamiento, el tamaño de los archivos (por ejemplo, archivos temporales) también afecta la cantidad de tiempo que tarda en crearse la instantánea. Para obtener más información acerca de la instantáneas de base de datos, consulte crear una instantánea de base de datos en la documentación de Amazon RDS.
- AWS Key Management Service (AWS KMS) crea una clave para el cifrado de Amazon RDS. Al crear una instancia de base de datos cifrada, también puede proporcionar el identificador de AWS KMSclave de su clave de cifrado. Si no especifica un identificador de clave de AWS KMS, Amazon RDS utiliza la clave de cifrado predeterminada para la nueva instancia de base de datos. AWS KMS crea la clave de cifrado predeterminada para su Cuenta de AWS. Cuenta de AWS Tiene una clave de cifrado predeterminada diferente para cada una de ellas Región de AWS. En este patrón, la instancia de base de datos de Amazon RDS debe cifrarse con la clave de AWS KMS no predeterminada. Para obtener más información sobre el uso de claves de AWS KMS para el cifrado de Amazon RDS, consulte Cifrado de recursos de Amazon RDS en la documentación de Amazon RDS.

Herramientas utilizadas para la replicación continua

- AWS Database Migration Service (AWS DMS) se utiliza para replicar los cambios en curso y para mantener sincronizadas las bases de datos de origen y destino. Para obtener más información sobre AWS DMS su uso para la replicación continua, consulte Trabajar con una instancia de AWS DMS replicación en la AWS DMS documentación.

Epics

Configure su fuente Cuenta de AWS

Tarea	Descripción	Habilidades requeridas
Prepare la instancia de base de datos de origen.	Ejecute la instancia de base de datos Amazon RDS para Oracle en modo ARCHIVELOG y defina el período de retención. Para obtener más información, consulte Trabajar con una base de datos Oracle AWS gestionada como fuente de AWS DMS.	Administrador de base de datos
Configure el registro complementario para la instancia de base de datos de Oracle de origen.	Configure el registro complementario a nivel de base de datos y de tabla para la instancia de base de datos de Amazon RDS para Oracle. Para obtener más información, consulte Trabajar con una base de datos Oracle AWS gestionada como fuente de AWS DMS.	Administrador de base de datos
Actualice la política AWS KMS clave de la cuenta de origen.	Actualice la política de AWS KMS claves en el origen Cuenta de AWS para permitir que el destino Cuenta de AWS utilice la AWS KMS clave	SysAdmin

Tarea	Descripción	Habilidades requeridas
	cifrada de Amazon RDS. Para obtener más información, consulte la documentación de AWS KMS.	
Cree una instantánea manual de Amazon RDS de la instancia de base de datos de origen.		AWS IAM user
Compartir la instantánea manual cifrada de Amazon RDS con la Cuenta de AWS de destino.	Para obtener más información, consulte Uso compartido de una instantánea de base de datos.	Usuario de AWS IAM

Configure su objetivo Cuenta de AWS

Tarea	Descripción	Habilidades requeridas
Adjunte una política.	En el destino Cuenta de AWS, adjunte una política AWS Identity and Access Management (IAM) al usuario raíz de IAM para que este pueda copiar una instantán ea de base de datos cifrada con la clave compartida. AWS KMS	SysAdmin
Cambiar a la Región de AWS de origen.		Usuario de AWS IAM
Copie la instantánea compartida.	En la consola de Amazon RDS, en el panel Instantán eas, elija Compartido conmigo	Usuario de AWS IAM

Tarea	Descripción	Habilidades requeridas
	y, a continuación, seleccione la instantánea compartida. Copie la instantánea en la Región de AWS misma base de datos de origen utilizando el Amazon Resource Name (ARN) como AWS KMS clave utilizada por la base de datos de origen. Para obtener más información, consulte Copia de una instantánea de base de datos.	
Cambie al destino Región de AWS y cree una AWS KMS clave nueva.		Usuario de AWS IAM
Copie la instantánea.	Cambiar a la Región de AWS de origen. En la consola de Amazon RDS, en el panel Instantáneas, elija De mi propiedad y, a continuación, seleccione la instantánea copiada. Copie la instantánea en el objetivo Región de AWS mediante la AWS KMS clave del nuevo objetivo Región de AWS.	Usuario de AWS IAM

Tarea	Descripción	Habilidades requeridas
Restaurare la instantánea.	Cambia al objetivo Región de AWS. En la consola de Amazon RDS, en el panel Instantáneas, elija De mi propiedad. Seleccione la instantánea copiada y restáurela en una instancia de base de datos de Amazon RDS para Oracle. Para obtener más información, consulte Restauración a una instancia de base de datos.	Usuario de AWS IAM

Prepare la base de datos de origen para la replicación continua

Tarea	Descripción	Habilidades requeridas
Cree un usuario de Oracle con los permisos adecuados.	Crear un usuario de Oracle con los privilegios obligatorios para Oracle como origen para AWS DMS. Para obtener más información, consulte la documentación de AWS DMS.	Administrador de base de datos
Configure la base de datos de origen para Oracle LogMiner u Oracle Binary Reader.		Administrador de base de datos

Prepare la base de datos de destino para la replicación continua

Tarea	Descripción	Habilidades requeridas
Cree un usuario de Oracle con los permisos adecuados.	Cree un usuario de Oracle con los privilegios obligator	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	ios para Oracle como destino de AWS DMS. Para obtener más información, consulte la documentación de AWS DMS.	

Cree AWS DMS componentes

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación en el destino Región de AWS.	Cree una instancia de replicación en la VPC del destino. Región de AWS Para obtener más información, consulte la documentación de AWS DMS.	Usuario de AWS IAM
Cree puntos de conexión de origen y destino con el cifrado necesario y pruebe las conexiones.	Para obtener más información, consulte la documentación de AWS DMS.	Administrador de base de datos
Cree tareas de replicación.	1. En tipo de migración, seleccione replicación continua. 2. Como punto de partida de captura de datos de cambios (CDC), use el número de cambio del sistema Oracle (SCN) cuando se tomó la instantánea de Amazon RDS para la carga completa, o bien la marca temporal en la que se realizó la carga completa.	Usuario de IAM

Tarea	Descripción	Habilidades requeridas
	3. Para `TargetTab lePrepMode` , elija DO_NOTHING. Si la tarea tiene tablas de datos de objetos binarios grandes (LOB), elija Modo de LOB limitado y establezca el tamaño máximo de LOB en el tamaño máximo de datos de LOB de la tabla. 4. Habilitar el registro. 5. Agrupe las tablas relaciona das mediante claves en una sola tarea. Si hay tablas con una gran cantidad de datos LOB y sin relación con otras tablas, cree una tarea independiente para ellas con la configuración de LOB descrita anteriorm ente. Para obtener más información, consulte la documentación de AWS DMS.	
Inicie las tareas y monitoríc elas.	Para obtener más información, consulte la documentación de AWS DMS.	Usuario de AWS IAM

Tarea	Descripción	Habilidades requeridas
Habilite la validación de la tarea si es necesario.	Tenga en cuenta que habilitar la validación afectará al rendimiento de la replicación. Para obtener más información, consulte la documentación de AWS DMS.	Usuario de AWS IAM

Recursos relacionados

- Cambiar una política clave
- Crear una instantánea manual de base de datos de Amazon RDS
- Crear una instantánea manual de base de datos de Amazon RDS
- Copia de una instantánea
- Restauración desde una instantánea de base de datos de Amazon RDS
- Empezando con AWS DMS
- Uso de una base de datos Oracle como fuente para AWS DMS
- Utilizar una base de datos Oracle como destino para AWS DMS
- AWS DMS configuración mediante interconexión de VPC
- ¿Cómo comparto instantáneas de bases de datos manuales de Amazon RDS o instantáneas de clústeres de bases de datos con otra Cuenta de AWS? (Artículo del centro de conocimientos de AWS)

Migración de una instancia de base de datos de Amazon RDS a otra VPC o cuenta

Dhrubajyoti Mukherjee, Amazon Web Services

Resumen

Este patrón proporciona una guía para migrar una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) de una nube privada virtual (VPC) a otra en la misma cuenta de AWS, o bien de una cuenta de AWS a otra cuenta de AWS.

Este patrón resulta útil si quiere migrar sus instancias de base de datos de Amazon RDS a otra VPC o cuenta por motivos de seguridad o de separación (por ejemplo, cuando quiere colocar la pila de aplicaciones y la base de datos en VPCs un lugar diferente).

La migración de una instancia de base de datos a otra cuenta de AWS conlleva ciertos pasos, como tomar una instantánea manual, compartirla y restaurar la instantánea en la cuenta de destino. En función de los cambios en la base de datos y de las tasas de transacción, este proceso puede llevar mucho tiempo. También provoca un tiempo de inactividad en la base de datos, por lo que debe planificar la migración con antelación. Considere una estrategia de blue/green implementación para minimizar el tiempo de inactividad. Como alternativa, puede evaluar AWS Data Migration Service (AWS DMS) para minimizar el tiempo de inactividad provocado por el cambio. Sin embargo, este patrón no aborda dicha opción. Para obtener más información, consulte la documentación de AWS DMS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Permisos de AWS Identity and Access Management (IAM) para la VPC, las subredes y la consola de Amazon RDS

Limitaciones

- Los cambios en una VPC provocan el reinicio de la base de datos, lo que, a su vez, provoca interrupciones en las aplicaciones. Se recomienda que realice la migración durante las horas de menor actividad.
- Limitaciones al migrar Amazon RDS a otra VPC:

  - La instancia de base de datos a migrar debe ser una instancia única y no estar en espera. No puede formar parte de un clúster.
  - Amazon RDS no debe estar en varias zonas de disponibilidad.
  - Amazon RDS no debe tener réplicas de lectura.
  - El grupo de subredes creado en la VPC de destino debe tener subredes en la zona de disponibilidad en la que se ejecuta la base de datos de origen.
- Limitaciones al migrar Amazon RDS a otra cuenta de AWS:
  - Actualmente no es posible compartir instantáneas cifradas con la clave de servicio predeterminada de Amazon RDS.

Arquitectura

Migración a una VPC en la misma cuenta de AWS

El siguiente diagrama muestra el flujo de trabajo para migrar una instancia de base de datos de Amazon RDS a una VPC diferente en la misma cuenta de AWS.

Los pasos son los siguientes. Consulte la sección Epics para obtener instrucciones detalladas.

1. Cree un grupo de subredes de base de datos en la VPC de destino. Un grupo de subredes de base de datos es una colección de subredes que se permiten especificar una VPC concreta al crear instancias de base de datos.
2. Configure la instancia de base de datos de Amazon RDS en la VPC de origen para usar el nuevo grupo de subredes de base de datos.
3. Aplique los cambios para migrar la base de datos de Amazon RDS a la VPC de destino.

Migración a otra cuenta de AWS

El siguiente diagrama muestra el flujo de trabajo para migrar una instancia de base de datos de Amazon RDS a una cuenta diferente de AWS.

Los pasos son los siguientes. Consulte la sección Epics para obtener instrucciones detalladas.

1. Acceda a la instancia de base de datos de Amazon RDS en la cuenta de AWS de origen.

2. Cree una instantánea de Amazon RDS en la cuenta de AWS de origen.
3. Comparta la instantánea de Amazon RDS con la cuenta de AWS de destino.
4. Acceda a la instantánea de Amazon RDS en la cuenta de AWS de destino.
5. Cree una instancia de base de datos de Amazon RDS en la cuenta de AWS de destino.

Tools (Herramientas)

Servicios de AWS

- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Prácticas recomendadas

- Si el tiempo de inactividad de la base de datos al migrar una instancia de base de datos de Amazon RDS a otra cuenta le resulta un problema, le recomendamos que use AWS DMS. La replicación de datos proporcionada por este servicio le permite reducir la interrupción a menos de cinco minutos.

Epics

Migración a una VPC diferente en la misma cuenta de AWS

Tarea	Descripción	Habilidades requeridas
Cree una nueva VPC.	En la consola de Amazon VPC, cree una nueva VPC y subredes con las propiedad es y los rangos de direccion es IP deseados. Para obtener instrucciones detalladas, consulte la documentación de Amazon VPC.	Administrador

Tarea	Descripción	Habilidades requeridas
Creación de un grupo de subredes de base de datos.	Abra la consola de Amazon RDS: 1. Seleccione Grupos de subredes y, a continuación, Crear grupo de subredes de base de datos. 2. Introduzca el nombre, la descripción y la ID de VPC del grupo de subredes. 3. Agregue las subredes que pertenecen al grupo de subredes. Agregue subredes para cubrir, al menos, dos zonas de disponibilidad. 4. Seleccione Crear. Para obtener más información, consulte la documentación de Amazon RDS.	Administrador

Tarea	Descripción	Habilidades requeridas
Modifique la instancia de base de datos de Amazon RDS para usar el nuevo grupo de subredes.	Abra la consola de Amazon RDS: 1. En el panel de navegación, seleccione Bases de datos y, a continuación, el nombre de la instancia de base de datos de Amazon RDS que va a migrar. 2. En la sección Conectividad, elija el grupo de subredes asociado a la VPC de destino. 3. En la sección Programación de modificaciones, seleccione Aplicar inmediatamente. Cuando se completa la migración a la VPC de destino, el grupo de seguridad predeterminado de la VPC de destino se asigna a la instancia de base de datos de Amazon RDS. Puede configurar un nuevo grupo de seguridad para esa VPC con las reglas de entrada y salida necesarias para su instancia de base de datos. También puede usar la interfaz de la línea de comandos de AWS (AWS CLI)	Administrador

Tarea	Descripción	Habilidades requeridas
	para realizar la migración a la VPC de destino proporcionando explícitamente la ID del nuevo grupo de seguridad de la VPC. Por ejemplo: `aws rds modify-db-instance \ --db-instance-identifier testrds \ --db-subnet-group-name new-vpc-subnet-group \ --vpc-security-group-ids sg-idxxxx \ --apply-immediately`	

Migración a una cuenta de AWS diferente

Tarea	Descripción	Habilidades requeridas
Cree una nueva VPC y un grupo de subredes en la cuenta de AWS de destino.	1. En la consola de Amazon VPC, cree una nueva VPC y subredes con las propiedades y los rangos de direcciones IP deseados. Para obtener instrucciones detalladas, consulte la documentación de Amazon VPC. 2. Cree subredes para la nueva VPC siguiendo las instrucciones de la	Administrador

Tarea	Descripción	Habilidades requeridas
	documentación de Amazon VPC. 3. En la consola de Amazon RDS, cree grupos de subredes de base de datos. Para obtener instrucciones, consulte la documentación de Amazon RDS.	
Cree una instantánea manual de la base de datos y compártala con la cuenta de destino.	1. Realice una instantánea manual de la base de datos de origen siguiendo las instrucciones de la documentación de Amazon RDS. 2. Comparta la instantánea con la cuenta de AWS de destino proporcionando la ID de la cuenta de destino. Para obtener más instrucciones, consulte el artículo de Re:post sobre cómo compartir instantáneas de bases de datos con otras cuentas.	Administrador
Lance una nueva instancia de base de datos en Amazon RDS.	Lance una nueva instancia de base de datos de Amazon RDS a partir de la instantánea compartida en la cuenta de AWS de destino. Para obtener instrucciones, consulte la documentación de Amazon RDS.	Administrador

Recursos relacionados

- Documentación de Amazon RDS
- Documentación de Amazon RDS
- ¿Cómo cambio la VPC de una instancia de base de datos de Amazon RDS? (artículo de AWS Re:post)
- ¿Cómo transfiero la propiedad de los recursos de Amazon RDS a otra cuenta de AWS? (artículo de AWS Re:post)
- ¿Cómo comparto las instantáneas manuales de bases de datos de Amazon RDS o las instantáneas del clúster de base de datos Aurora con otra cuenta de AWS? (artículo de AWS Re:post)
- Documentación de AWS DMS

Migración de un clúster de Amazon Redshift a una región de AWS en China

Jing Yan, Amazon Web Services

Resumen

Este patrón proporciona un step-by-step enfoque para migrar un clúster de Amazon Redshift a una región de AWS en China desde otra región de AWS.

Este patrón emplea comandos SQL para recrear todos los objetos de base de datos, y usa el comando UNLOAD para mover estos datos de Amazon Redshift a un bucket de Amazon Simple Storage Service (Amazon S3) en la región de origen. A continuación, los datos se migran a un bucket de S3 en la región de AWS en China. El comando COPY carga datos del bucket de S3 y los transfiere al clúster de Amazon Redshift de destino.

Actualmente, Amazon Redshift no admite características entre regiones, como la copia de instantáneas en regiones de AWS en China. Este patrón proporciona una forma de evitar esta limitación. También puede invertir los pasos de este patrón para migrar datos de una región de AWS en China a otra región de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Cuentas de AWS activas, tanto en una región de China como en una región de AWS fuera de China
- Clústeres de Amazon Redshift existentes, tanto en una región de China como en una región de AWS fuera de China

Limitaciones

- Esta es una migración sin conexión, por lo que el clúster de Amazon Redshift de origen no podrá realizar operaciones de escritura durante la migración.

Arquitectura

Pila de tecnología de origen

- Clúster de Amazon Redshift en una región de AWS fuera de China

Pila de tecnología de destino

- Clúster de Amazon Redshift en una región de AWS en China

Arquitectura de destino

Tools (Herramientas)

Herramientas

- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y resultados. Puede usar Amazon S3 para almacenar datos de Amazon Redshift y copiar datos de un bucket de S3 a Amazon Redshift.
- Amazon Redshift: Amazon Redshift es un servicio de almacenamiento de datos de varios petabytes totalmente administrado en la nube.
- psql: psql es un frontend de PostgreSQL basado en terminal.

Epics

Preparación para la migración en la región de origen

Tarea	Descripción	Habilidades requeridas
Lance y configure una EC2 instancia en la región de origen.	Inicie sesión en la consola de administración de AWS y abra la consola de Amazon Elastic Compute Cloud (Amazon EC2). En la barra de navegación de la parte superior de la pantalla, se muestra la región actual. Esta región no puede ser una región de AWS en China. En el panel de control de la EC2 consola de Amazon, seleccion	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	a «Lanzar instancia» y crea y configura una EC2 instancia. Importante: Asegúrese de que sus grupos de EC2 seguridad para las reglas de entrada permitan el acceso sin restricciones al puerto TCP 22 desde su máquina de origen. Para obtener instrucciones sobre cómo lanzar y configurar una EC2 instancia, consulta la sección «Recursos relacionados».	
Instale la herramienta psql.	Descargue e instale PostgreSQL. Amazon Redshift no proporciona la herramienta psql. Esta se instala con PostgreSQL. Para obtener más información sobre el uso de psql y la instalación de las herramientas de PostgreSQL, consulte la sección “Recursos relacionados”.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Registre los detalles del clúster de Amazon Redshift.	Abra la consola de Amazon Redshift y elija “Clústeres” en el panel de navegación. A continuación, seleccion e el nombre del clúster de Amazon Redshift de la lista. En la pestaña “Propiedades”, en la sección “Configuraciones de la base de datos”, registre los valores de “Nombre de la base de datos” y “Puerto”. Abra la sección “Detalles de la conexión” y registre el valor de “Punto de conexión”, en el formato “endpoint:<puerto> /<nombrebasedatos>”. Importante: Asegúrese de que sus grupos de seguridad de Amazon Redshift para las reglas de entrada permitan el acceso sin restricciones al puerto TCP 5439 desde su instancia. EC2	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Conecte psql al clúster de Amazon Redshift.	En una línea de comandos, especifique la información de conexión ejecutando el comando “psql -h <puntoconexión> -U <idusuario> -d <nombrebasedatos> -p <puerto>”. Cuando se le solicite la contraseña de psql, ingrese la contraseña del usuario “<idusuario>”. Estará entonces conectado al clúster de Amazon Redshift y puede ingresar comandos de forma interactiva.	Administrador de base de datos
Cree un bucket de S3.	Abra la consola de Amazon S3 y cree un bucket de S3 que contenga los archivos exportados desde Amazon Redshift. Para obtener instrucciones sobre cómo crear un bucket de S3, consulte la sección “Recursos relacionados”.	Administrador de base de datos, AWS general

Tarea	Descripción	Habilidades requeridas
Cree una política de IAM que permita descargar datos.	Abra la consola de AWS Identity and Access Management (IAM) y seleccione “Políticas”. Seleccione “Crear política” y, a continuación, la pestaña “JSON”. Copie y pegue la política de IAM para descargar datos de la sección “Informac ión adicional”. Importante: Sustituya “s3_bucket_name” por el nombre de su bucket de S3. Seleccione “Revisar política” e ingrese un nombre y una descripción para la política. Seleccione “Crear política”.	Administrador de base de datos
Cree un rol de IAM que permita la operación UNLOAD en Amazon Redshift.	Abra la consola de IAM y seleccione “Roles”. Seleccion e “Crear rol” y elija “Servicio de AWS” en “Seleccionar el tipo de entidad de confianza ”. Elija “Redshift” en el servicio, seleccione “Redshift - Personalizable” y, a continuac ión, elija “Siguiente”. Elija la política “Descargar” que creó anteriormente y seleccion e “Siguiente”. Ingrese un valor en “Nombre del rol” y seleccione “Crear rol”.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Asociar un rol de IAM al clúster de Amazon Redshift.	Abra la consola de Amazon Redshift y elija “Administrar roles de IAM”. Elija “Roles disponibles” en el menú desplegable y seleccione el rol que creó anteriorm ente. Seleccione “Aplicar cambios”. Cuando el valor de “Estado” del rol de IAM en la sección “Administrar roles de IAM” aparezca como “Sincronizado”, podrá ejecutar el comando UNLOAD.	Administrador de base de datos
Detenga las operaciones de escritura en el clúster de Amazon Redshift.	Recuerde detener todas las operaciones de escritura en el clúster de Amazon Redshift de origen hasta que se complete la migración.	Administrador de base de datos

Preparación para la migración en la región de destino

Tarea	Descripción	Habilidades requeridas
Lance y configure una EC2 instancia en la región de destino.	Inicie sesión en la consola de administración de AWS de una región de China, ya sea Pekín o Ningxia. En la EC2 consola de Amazon, seleccion a «Lanzar instancia» y crea y configura una EC2 instancia. Importante: Asegúrese de que sus grupos de EC2 seguridad de Amazon para las reglas de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	entrada permitan el acceso sin restricciones al puerto TCP 22 desde su máquina de origen. Para obtener más instrucciones sobre cómo lanzar y configurar una EC2 instancia, consulta la sección «Recursos relacionados».	
Registre los detalles del clúster de Amazon Redshift.	Abra la consola de Amazon Redshift y elija “Clústeres” en el panel de navegación. A continuación, seleccione el nombre del clúster de Amazon Redshift de la lista. En la pestaña “Propiedades”, en la sección “Configuraciones de la base de datos”, registre los valores de “Nombre de la base de datos” y “Puerto”. Abra la sección “Detalles de la conexión” y registre el valor de “Punto de conexión”, en el formato “endpoint:<puerto>/<nombrebasedatos>”. Importante: Asegúrese de que sus grupos de seguridad de Amazon Redshift para las reglas de entrada permitan el acceso sin restricciones al puerto TCP 5439 desde su instancia. EC2	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Conecte psql al clúster de Amazon Redshift.	En una línea de comandos, especifique la información de conexión ejecutando el comando “psql -h <puntoconexión> -U <idusuario> -d <nombrebasedatos> -p <puerto>”. Cuando se le solicite la contraseña de psql, ingrese la contraseña del usuario “<idusuario>”. Estará entonces conectado al clúster de Amazon Redshift y puede ingresar comandos de forma interactiva.	Administrador de base de datos
Cree un bucket de S3.	Abra la consola de Amazon S3 y cree un bucket de S3 que contenga los archivos exportados desde Amazon Redshift. Para obtener ayuda con esta y otras historias, consulte la sección “Recursos relacionados”.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree una política de IAM que permita copiar datos.	Abra la consola de IAM y seleccione “Políticas”. Seleccione “Crear política” y, a continuación, la pestaña “JSON”. Copie y pegue la política de IAM para copiar datos de la sección “Informac ión adicional”. Importante: Sustituya “s3_bucket_name” por el nombre de su bucket de S3. Seleccione “Revisar política” e ingrese un nombre y una descripción para la política. Seleccione “Crear política”.	Administrador de base de datos
Cree un rol de IAM que permita la operación COPIAR en Amazon Redshift.	Abra la consola de IAM y seleccione “Roles”. Seleccion e “Crear rol” y elija “Servicio de AWS” en “Seleccionar el tipo de entidad de confianza ”. Elija “Redshift” en el servicio, seleccione “Redshift - Personalizable” y, a continuac ión, elija “Siguiente”. Elija la política “Copiar” que creó anteriormente y seleccion e “Siguiente”. Ingrese un valor en “Nombre del rol” y seleccione “Crear rol”.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Asociar un rol de IAM al clúster de Amazon Redshift.	Abra la consola de Amazon Redshift y elija “Administrar roles de IAM”. Elija “Roles disponibles” en el menú desplegable y seleccione el rol que creó anteriorm ente. Seleccione “Aplicar cambios”. Cuando el valor de “Estado” del rol de IAM en la sección “Administrar roles de IAM” aparezca como “Sincronizado”, podrá ejecutar el comando “COPY”.	Administrador de base de datos

Compruebe los datos de origen y la información de objeto antes de iniciar la migración

Tarea	Descripción	Habilidades requeridas
Compruebe las filas de las tablas de Amazon Redshift de origen.	Use los scripts de la sección “Información adicional” para verificar y registrar el número de filas de las tablas de Amazon Redshift de origen. Recuerde dividir los datos equitativamente para los scripts UNLOAD y COPY. Esto mejorará la eficiencia de la descarga y carga de datos, ya que la cantidad de datos incluida en cada script estará equilibrada.	Administrador de base de datos
Compruebe el número de objetos de base de datos en el	Utilice los scripts de la sección «Información adicional»	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
clúster de Amazon Redshift de origen.	para verificar y registrar el número de bases de datos, usuarios, esquemas, tablas, vistas y funciones definidas por el usuario (UDFs) en su clúster de Amazon Redshift de origen.	
Compruebe los resultados de las instrucciones SQL antes de la migración.	Algunas instrucciones SQL de validación de datos deben clasificarse de acuerdo con las situaciones empresariales y de datos reales. Este paso verificará los datos importado s y garantizará que sean coherentes y se muestren correctamente.	Administrador de base de datos

Migración de datos y objetos a la región de destino

Tarea	Descripción	Habilidades requeridas
Genere scripts DDL de Amazon Redshift.	Genere scripts de lenguaje de definición de datos (DDL) mediante los enlaces de la sección “Instrucciones de SQL para consultas en Amazon Redshift” en la sección “Información adicional ”. Estos scripts de DDL deben incluir las consultas “crear usuario”, “crear esquema”, “privilegios del usuario sobre el esquema”, “crear tabla/vis ta”, “privilegios del usuario	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	sobre los objetos” y “crear función”.	
Cree objetos en el clúster de Amazon Redshift para la región de destino.	Ejecute los scripts de DDL usando la Interfaz de la línea de comandos de AWS (AWS CLI) en la región de AWS en China. Estos guiones crean objetos en el clúster de Amazon Redshift para la región de destino.	Administrador de base de datos
Descargue los datos de origen del clúster de Amazon Redshift en el bucket de S3.	Ejecute el comando UNLOAD para descargar los datos del clúster de Amazon Redshift de la región de origen al bucket de S3.	Administrador de base de datos, desarrollador
Transfiera los datos del bucket de la región S3 de origen al bucket de la región S3 de destino.	Transfiera los datos del bucket de la región S3 de origen al bucket de la región S3 de destino. Ya que no se puede usar el comando “$ aws s3 sync”, asegúrese de seguir el proceso descrito en el artículo “Transferir datos de Amazon S3 de regiones de AWS a regiones de AWS en China” de la sección “Recursos relacionados”.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Cargue los datos en el clúster de Amazon Redshift de destino.	En la herramienta psql de la región de destino, ejecute el comando COPY para cargar los datos del bucket de S3 al clúster de Amazon Redshift de destino.	Administrador de base de datos

Verifique los datos en las regiones de origen y destino tras la migración

Tarea	Descripción	Habilidades requeridas
Verifique y compare el número de filas en las tablas de origen y destino.	Verifique y compare el número de filas en las tablas de origen y destino de las regiones para asegurarse de que todas han migrado.	Administrador de base de datos
Verifique y compare el número de objetos en las bases de datos de origen y destino.	Verifique y compare todos los objetos de la base de datos en las regiones de origen y destino para asegurarse de que todos se hayan migrado.	Administrador de base de datos
Verifique y compare los resultados de los scripts SQL en las regiones de origen y destino.	Ejecute los scripts SQL preparados antes de la migración. Verifique y compare los datos para asegurarse de que los resultados de SQL sean correctos.	Administrador de base de datos
Restablezca las contraseñ as de todos los usuarios del clúster de Amazon Redshift de destino.	Una vez finalizada la migración y verificados todos los datos, debe restablec er todas las contraseñas de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	usuario del clúster de Amazon Redshift en la región de AWS en China.	

Recursos relacionados

- Transferir datos de Amazon S3 de regiones de AWS a regiones de AWS en China
- Creating an S3 bucket (Crear un bucket de S3)
- Restablecer una contraseña de usuario de Amazon Redshift
- Documentación de psql

Información adicional

Política de IAM para descargar datos

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::s3_bucket_name"]
    },
    {
      "Effect": "Allow",
      "Action": ["s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::s3_bucket_name/*"]
    }
  ]
}
```

Política de IAM para copiar datos

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::s3_bucket_name"]
    },
    {
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": ["arn:aws:s3:::s3_bucket_name/*"]
    }
  ]
}
```

Instrucciones de SQL para consultas en Amazon Redshift

```
##Database

select * from pg_database where datdba>1;

##User

select * from pg_user where usesysid>1;

##Schema

SELECT n.nspname AS "Name",

  pg_catalog.pg_get_userbyid(n.nspowner) AS "Owner"

FROM pg_catalog.pg_namespace n

WHERE n.nspname !~ '^pg_' AND n.nspname <> 'information_schema'

ORDER BY 1;

##Table

select count(*) from pg_tables where schemaname not in
 ('pg_catalog','information_schema');

select schemaname,count(*) from pg_tables where schemaname not in
 ('pg_catalog','information_schema') group by schemaname order by 1;

##View
```

```
SELECT

    n.nspname AS schemaname,c.relname AS
 viewname,pg_catalog.pg_get_userbyid(c.relowner) as "Owner"

FROM

    pg_catalog.pg_class AS c

INNER JOIN

    pg_catalog.pg_namespace AS n

    ON c.relnamespace = n.oid

WHERE relkind = 'v' and n.nspname not in ('information_schema','pg_catalog');

##UDF

SELECT

   n.nspname AS schemaname,

   p.proname AS proname,

   pg_catalog.pg_get_userbyid(p.proowner) as "Owner"

FROM pg_proc p

LEFT JOIN pg_namespace n on n.oid = p.pronamespace

WHERE p.proowner != 1;
```

Secuencias de comandos SQL para generar sentencias DDL

- Script Get_schema_priv_by_user
- Script Generate_tbl_ddl
- Generate_view_ddl
- Generate_user_grant_revoke_ddl
- Generate_udf_ddl

Transportar bases de datos PostgreSQL entre dos instancias de base de datos de Amazon RDS utilizando pg_transport

Raunak Rishabh y Jitender Kumar, Amazon Web Services

Resumen

Este patrón describe los pasos para migrar bases de datos extremadamente grandes entre dos instancias de base de datos de Amazon Relational Database Service (Amazon RDS) para PostgreSQL mediante la extensión pg_transport. Esta extensión proporciona un mecanismo físico de transporte para trasladar cada base de datos. Al transmitir por streaming los archivos de base de datos con un procesamiento mínimo, proporciona un método extremadamente rápido para migrar bases de datos de gran tamaño entre instancias de base de datos con un tiempo de inactividad mínimo. Esta extensión utiliza un modelo de extracción donde la instancia de base de datos de destino importa la base de datos de la instancia de base de datos de origen.

Requisitos previos y limitaciones

Requisitos previos

- Ambas instancias de base de datos deben ejecutar la misma versión principal de PostgreSQL.
- La base de datos no debe existir en el destino. De lo contrario, el transporte devuelve un error.
- No se debe habilitar ninguna extensión que no sea pg_transport en la base de datos de origen.
- Todos los objetos de base de datos deben estar en el espacio de tablas predeterminado pg_default.
- El grupo de seguridad de la instancia de base de datos de origen debe permitir el tráfico desde la instancia de base de datos de destino.
- Instale un cliente de PostgreSQL, como psql, PgAdmino para trabajar con la instancia de base de datos PostgreSQL de Amazon RDS. Puede instalar el cliente en su sistema local o utilizar una instancia de Amazon Elastic Compute Cloud (Amazon EC2). En este patrón, utilizamos psql en una EC2 instancia.

Limitaciones

- No puede transportar bases de datos entre distintas versiones principales de Amazon RDS para PostgreSQL.
- Los privilegios de acceso y la propiedad de la base de datos de origen no se transfieren a la base de datos de destino.

- No puede transportar bases de datos en réplicas de lectura ni en instancias principales de réplicas de lectura.
- No puede utilizar tipos de datos de registro en ninguna tabla de base de datos que planee transportar con este método.
- Puede ejecutar hasta 32 transportes totales al mismo tiempo en una instancia de base de datos, (incluidas tanto importaciones como exportaciones).
- No puedes cambiar el nombre de nuestras tablas. include/exclude Todo se migra tal cual.

Precaución

- Realice copias de seguridad antes de eliminar la extensión, ya que al eliminar la extensión también se eliminan los objetos dependientes y algunos datos que son fundamentales para el funcionamiento de la base de datos.
- Tenga en cuenta la clase de instancia y los procesos que se ejecutan en otras bases de datos de la instancia de origen al determinar la cantidad de trabajadores y los `work_mem` valores de pg_transport.
- Cuando se inicia el transporte, finalizan todas las conexiones de la base de datos de origen y la base de datos pasa al modo de solo lectura.

> **Note**
>
> Cuando el transporte se ejecuta en una base de datos, no afecta a las demás bases de datos del mismo servidor.

Versiones de producto

- Amazon RDS para PostgreSQL 10.10 y posteriores y Amazon RDS para PostgreSQL 11.5 y posteriores. Para obtener información sobre la versión más reciente, consulte Transporte de bases de datos PostgreSQL entre instancias de base de datos en la documentación de Amazon RDS.

Arquitectura

Tools (Herramientas)

- pg_transport proporciona un mecanismo físico de transporte para trasladar cada base de datos. Al transmitir por streaming los archivos de la base de datos con un procesamiento mínimo, el transporte físico mueve los datos mucho más rápido que los procesos tradicionales de volcado y carga y requiere un tiempo de inactividad mínimo. Las bases de datos transportables de PostgreSQL utilizan un modelo de extracción donde la instancia de base de datos de destino importa la base de datos de la instancia de base de datos de origen. Esta extensión se instala en las instancias de base de datos al preparar los entornos de origen y destino, tal y como se explica en este patrón.
- psql le permite conectarse a sus instancias de base de datos de PostgreSQL y trabajar con ellas. Para instalar psql en su sistema, consulte la página de descargas de PostgreSQL.

Epics

Cree el grupo de parámetros de destino

Tarea	Descripción	Habilidades requeridas
Cree un grupo de parámetros para el sistema de destino.	Especifique un nombre de grupo que lo identifique como grupo de parámetros de destino; por ejemplo,v `pgtarget-param-group` . Para obtener instrucciones, consulte la Documentación de Amazon RDS.	Administrador de base de datos
Modifique los parámetros para el grupo de parámetros.	Establezca los siguientes parámetros: 1. Añada `pg_transport` al parámetro `shared_preload_libraries` . `shared_preload_libraries = pg_stat_s`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`tatements, pg_transp ort` 2. Establezca el parámetro `pg_transport.num_w orkers` . Seleccione el número de trabajadores con los que quiere gestionar el transporte. El valor que establezca determina la cantidad de `transport .send_file` trabajado res que se crearán en la fuente. 3. Aumente el valor de `max_worker_process es` a más de tres veces el valor de`pg_transp ort.num_workers` . Por ejemplo, si establece el valor de `pg_transp ort.num_workers` en 4, el `max_worke r_processes` valor debe ser al menos 13. Si esto no funciona, pg_transp ort recomienda un valor mínimo. 4. Establezca `pg_transp ort.timing` en 1. Esta configuración permite notificar la información de tiempo durante el transport e.	

Tarea	Descripción	Habilidades requeridas
	5. Establezca el parámetro `pg_transport.work_mem` . Este parámetro especifica la memoria máxima que se debe asignar a cada trabajador. El valor predeterminado es 128 MB. Para obtener más información acerca de estos parámetros, consulte la documentación de Amazon RDS.	

Crear el grupo de parámetros

Tarea	Descripción	Habilidades requeridas
Cree un grupo de parámetros para el sistema de origen.	Especifique un nombre de grupo que lo identifique como grupo de parámetros de origen; por ejemplo, `pgsource-param-group` . Para obtener instrucciones, consulte la Documentación de Amazon RDS.	Administrador de base de datos
Modifique los parámetros para el grupo de parámetros.	Establezca los siguientes parámetros: 1. Añada `pg_transport` al parámetro `shared_preload_libraries` .	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`shared_preload_libraries = pg_stat_statements, pg_transport` 2. Establezca el parámetro `pg_transport.num_workers` . El valor de este parámetro definido en el objetivo determina el número de `transport.send_file` trabajadores que se van a utilizar. Si tiene una importación en ejecución en esta instancia, aumente este valor, pero tenga en cuenta la cantidad de trabajadores que ya se están ejecutando. 3. Aumente el valor de `max_worker_processes` a más de tres veces el valor del `pg_transport.num_workers` objetivo. Por ejemplo, si establece el valor de `pg_transport.num_workers` 4 en el destino, el `max_worker_processes` valor del origen debe ser al menos 13. Si esto no funciona, pg_transport recomienda un valor mínimo.	

Tarea	Descripción	Habilidades requeridas
	4. Establezca el parámetro `pg_transport.work_mem` . Este parámetro especifica la memoria máxima que se debe asignar a cada trabajador. El valor predeterminado es 128 MB. Para obtener más información acerca de estos parámetros, consulte la documentación de Amazon RDS.	

Prepare el entorno de destino

Tarea	Descripción	Habilidades requeridas
Cree una nueva instancia de base de datos de Amazon RDS para PostgreSQL a la que transportar la base de datos de origen.	Determine la clase de instancia y la versión de PostgreSQL en función de los requisitos de su empresa.	Administrador de base de datos, administrador de sistemas, arquitecto de bases de datos
Modifique el grupo de seguridad del destino para permitir las conexiones en el puerto de la instancia de base de datos desde la EC2 instancia.	De forma predeterminada, el puerto para la instancia de PostgreSQL es 5432. Si utiliza otro puerto, las conexione s a ese puerto deben estar abiertas para la EC2 instancia.	Administrador de base de datos, administrador de sistemas
Modifique la instancia y asigne el nuevo grupo de parámetros de destino.	Por ejemplo, `pgtarget-param-group` .	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Reinicie la instancia de base de datos de Amazon RDS de destino.	Los parámetros `shared_preload_libraries` y `max_worker_processes` son parámetros estáticos y requieren el reinicio de la instancia.	Administrador de base de datos, administrador de sistemas
Conéctese a la base de datos desde la EC2 instancia mediante psql.	Utilice el comando: `psql -h <rds_end_point> -p PORT -U username -d database -W`	Administrador de base de datos
Cree la extensión pg_transport.	Ejecute la siguiente consulta como usuario con el rol `rds_superuser` : `create extension pg_transport;`	Administrador de base de datos

Preparación del entorno de origen

Tarea	Descripción	Habilidades requeridas
Modifique el grupo de seguridad de la fuente para permitir las conexiones en el puerto de la instancia de base de datos desde la instancia de Amazon y la EC2 instancia de base de datos de destino	De forma predeterminada, el puerto para la instancia de PostgreSQL es 5432. Si utiliza otro puerto, las conexiones a ese puerto deben estar abiertas para la EC2 instancia.	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Modifique la instancia y asigne el nuevo grupo de parámetros de origen.	Por ejemplo, `pgsource-param-group` .	Administrador de base de datos
Reinicie la instancia de base de datos de Amazon RDS de origen.	Los parámetros `shared_preload_libraries` y `max_worker_processes` son parámetros estáticos y requieren el reinicio de la instancia.	Administrador de base de datos
Conéctese a la base de datos desde la EC2 instancia mediante psql.	Utilice el comando: `psql -h <rds_end_point> -p PORT -U username -d database -W`	Administrador de base de datos
Cree la extensión pg_transport y elimine todas las demás extensiones de las bases de datos que se van a transportar.	El transporte fallará si hay alguna extensión que no sea pg_transport instalada en la base de datos de origen. Este comando debe ejecutarlo un usuario con el rol `rds_superuser` .	Administrador de base de datos

Realice el transporte

Tarea	Descripción	Habilidades requeridas
Ejecute una prueba.	Utilice la función `transport.import_from_server` para realizar primero un simulacro:	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`SELECT transport .import_from_serve r( 'source-db-instanc e-endpoint', source- db-instance-port, 'source-db-instance- user', 'source-user- password', 'source- database-name', 'destination-user- password', 'true');` El último parámetro de esta función (establecido en`true`) define el funcionamiento en seco. Esta función muestra los errores que aparecen al ejecutar el transporte principal. Resuelva los errores antes de ejecutar el transporte principal.	

Tarea	Descripción	Habilidades requeridas
Si el simulacro se realiza correctamente, inicie el transporte de la base de datos.	Ejecute la función `transport.import_from_server` para realizar el transporte. Se conecta a la fuente e importa los datos. `SELECT transport.import_from_server( 'source-db-instance-endpoint', source-db-instance-port, 'source-db-instance-user', 'source-user-password', 'source-database-name', 'destination-user-password', false);` El último parámetro de esta función (establecido en`false`) indica que no se trata de un simulacro.	Administrador de base de datos
Realice los pasos posteriores al transporte.	Una vez finalizado el transporte de la base de datos: • Valide los datos en el entorno de destino. • Añada todos los roles y permisos al objetivo. • Habilite todas las extensiones necesarias en el destino y el origen, si es necesario. • Revierta el valor del parámetro `max_worker_processes` .	Administrador de base de datos

Recursos relacionados

- Documentación de Amazon RDS
- Documentación de pg_transport
- Migración de bases de datos mediante bases de datos transportables PostgreSQL de RDS (entrada del blog)
- Descargas de PostgreSQL
- utilidad psql
- Creación de un grupo de parámetros de base de datos
- Cómo modificar parámetros en un grupo de parámetros de base de datos
- Descargas de PostgreSQL

Redefinir la plataforma

Temas

- Exportación de una base de datos de Microsoft SQL Server a Amazon S3 mediante AWS DMS
- Migración de valores CLOB de Oracle a filas individuales en PostgreSQL en AWS
- Migre Oracle PeopleSoft a Amazon RDS Custom
- Migración de la funcionalidad ROWIdentificador de Oracle a PostgreSQL en AWS
- Migración de códigos de error de Oracle Database a una base de datos Amazon Aurora compatible con PostgreSQL
- Migre SAP ASE de Amazon EC2 a Amazon Aurora compatible con PostgreSQL mediante AWS SCT y AWS DMS
- Migración de los certificados SSL de Windows a un equilibrador de carga de aplicación mediante ACM
- Migración de una cola de mensajes de Microsoft Azure Service Bus a Amazon SQS
- Migre una EnterpriseOne base de datos de Oracle JD Edwards a AWS mediante Oracle Data Pump y AWS DMS
- Migre una PeopleSoft base de datos de Oracle a AWS mediante AWS DMS
- Migración de una base de datos MySQL en las instalaciones a Amazon RDS para MySQL
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server
- Migración de datos de Microsoft Azure Blob a Amazon S3 mediante Rclone
- Migración de Couchbase Server a Couchbase Capella en AWS
- Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2
- Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2 con Auto Scaling
- Migración de una aplicación .NET de Microsoft Azure App Service a AWS Elastic Beanstalk
- Migre de Oracle WebLogic a Apache Tomcat (ToMEE) en Amazon ECS
- Migre una base de datos Oracle de Amazon EC2 a Amazon RDS for Oracle mediante AWS DMS
- Migre una base de datos Oracle local a Amazon OpenSearch Service mediante Logstash
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump
- Migre de PostgreSQL en EC2 Amazon a Amazon RDS para PostgreSQL mediante pglogical

- Migración de una base de datos PostgreSQL en las instalaciones a Aurora PostgreSQL
- Migre una base de datos local de Microsoft SQL Server a Microsoft SQL Server en Amazon EC2 con Linux
- Migración de bases de datos en las instalaciones de Microsoft SQL Server a Amazon RDS para SQL Server mediante servidores vinculados
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server mediante métodos nativos de copia de seguridad y restauración
- Migración de una base de datos de Microsoft SQL Server a Aurora MySQL mediante AWS DMS y AWS SCT
- Migración de una base de datos de MariaDB en las instalaciones hasta Amazon RDS para MariaDB mediante herramientas nativas
- Migración de una base de datos de MySQL en las instalaciones a Aurora MySQL
- Migre bases de datos MySQL locales a Aurora MySQL mediante Percona, XtraBackup Amazon EFS y Amazon S3
- Migración de aplicaciones Java locales en las instalaciones a AWS mediante AWS App2Container
- Migre sistemas de archivos compartidos en una migración AWS grande
- Migre una base de datos Oracle a Amazon RDS for Oracle mediante adaptadores de archivos planos de GoldenGate Oracle
- Cambie las aplicaciones de Python y Perl para que admitan la migración de bases de datos de Microsoft SQL Server a una edición compatible con PostgreSQL de Amazon Aurora

Exportación de una base de datos de Microsoft SQL Server a Amazon S3 mediante AWS DMS

Sweta Krishna, Amazon Web Services

Resumen

Con frecuencia, las organizaciones necesitan copiar bases de datos a Amazon Simple Storage Service (Amazon S3) para la migración de bases de datos, la copia de seguridad y la restauración, el archivado y el análisis de datos. Este patrón describe cómo puede exportar una base de datos de Microsoft SQL Server a Amazon S3. La base de datos de origen se puede alojar localmente o en Amazon Elastic Compute Cloud (Amazon EC2) o Amazon Relational Database Service (Amazon RDS) para Microsoft SQL Server en la nube de Amazon Web Services (AWS).

Los datos se exportan mediante AWS Database Migration Service (AWS DMS). De forma predeterminada, AWS DMS escribe los datos de captura de datos de carga completa y cambios (CDC) en formato de valores separados por comas (.csv). Para un almacenamiento más compacto y opciones de consulta más rápidas, este patrón utiliza la opción de formato Apache Parquet (.parquet).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un rol de AWS Identity and Access Management (IAM) para la cuenta con acceso de escritura, eliminación y etiquetado al bucket de S3 de destino, y se ha agregado AWS DMS (`dms.amazonaws.com`) como entidad de confianza a este rol de IAM
- Una base de datos Microsoft SQL Server local (o Microsoft SQL Server en una EC2 instancia o una base de datos Amazon RDS for SQL Server)
- Conectividad de red entre la nube privada virtual (VPC) de AWS y la red en las instalaciones proporcionada por AWS Direct Connect o una red privada virtual (VPN)

Limitaciones

- Actualmente, las versiones de AWS DMS anteriores a la 3.4.7 no admiten un bucket de S3 habilitado para VPC (VPC de puerta de enlace).
- No se admiten cambios en la estructura de la tabla de origen durante la carga completa.

- No se admite el modo de objetos binarios grandes (LOB) completo de AWS DMS.

Versiones de producto

- Versiones de Microsoft SQL Server 2005 o posterior, para las ediciones Enterprise, Standard, Workgroup y Developer.
- La compatibilidad con Microsoft SQL Server versión 2019 como origen está disponible en las versiones 3.3.2 y posteriores de AWS DMS.

Arquitectura

Pila de tecnología de origen

- Una base de datos Microsoft SQL Server local (o Microsoft SQL Server en una EC2 instancia o una base de datos Amazon RDS for SQL Server)

Pila de tecnología de destino

- AWS Direct Connect
- AWS DMS
- Amazon S3

Arquitectura de destino

Tools (Herramientas)

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- AWS Direct Connect vincula su red interna con una ubicación de Direct Connect a través de un cable estándar Ethernet de fibra óptica. Con esta conexión, puede crear interfaces virtuales directamente en servicios públicos de AWS omitiendo a los proveedores de servicios de Internet en su ruta de acceso a la red.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Epics

Preparación para la migración

Tarea	Descripción	Habilidades requeridas
Valide la versión de la base de datos.	Valide la versión de la base de datos de origen y asegúrese de que es compatible con AWS DMS. Para obtener información sobre las versiones de bases de datos de SQL Server compatibles, consulte Uso de una base de datos de Microsoft SQL Server como fuente de AWS DMS.	Administrador de base de datos
Crear una VPC y un grupo de seguridad.	En su cuenta de AWS, cree una VPC y un grupo de seguridad. Para obtener más información, consulte la documentación de Amazon VPC.	Administrador de sistemas
Cree un usuario para la tarea de AWS DMS.	Cree un usuario de AWS DMS en la base de datos de origen y concédale permisos de LECTURA. AWS DMS utilizará este usuario.	Administrador de base de datos
Pruebe la conectividad de la base de datos.	Pruebe la conectividad con la instancia de base de datos SQL Server desde el usuario de AWS DMS.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Crear el bucket de S3 objetivo. Este bucket contendrá los datos de la tabla migrados.	Administrador de sistemas
Crear una política y un rol de IAM.	1. Para crear una política de IAM con permisos de bucket, use el código de la sección Información adicional. 2. Cree un rol AWS DMS y asocie la política a dicho rol.	Administrador de sistemas

Migración de datos mediante AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación de AWS DMS.	Inicie sesión en la Consola de administración de AWS y abra la consola de AWS DMS. En el panel de navegación, seleccione Instancias de replicación y Crear instancia de replicación. Para obtener instrucciones, consulte el paso 1 de la documentación de AWS DMS.	Administrador de base de datos
Cree puntos de conexión de origen y destino.	Cree puntos de conexión de origen y destino. Pruebe la tarea desde la instancia de replicación a los puntos de conexión de origen y destino. Para obtener instrucciones,	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	consulte el paso 2 de la documentación de AWS DMS.	
Cree una tarea de replicación.	Cree una tarea de replicación y seleccione carga completa o carga completa con captura de datos de cambios (CDC) para migrar los datos de SQL Server al bucket de S3. Para obtener instrucciones, consulte el paso 3 de la documentación de AWS DMS.	Administrador de base de datos
Iniciar la tarea de replicación.	Inicie la tarea de replicación y supervise los registros para detectar cualquier error.	Administrador de base de datos

Valide los datos

Tarea	Descripción	Habilidades requeridas
Valide los datos migrados.	En la consola de Amazon S3, acceda a su bucket. Abra la subcarpeta que tiene el mismo nombre que la base de datos de origen. Confirme que la carpeta contiene todas las tablas que se migraron de la base de datos de origen.	Administrador de base de datos

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Cierre y elimine los recursos temporales de AWS.	Cierre los recursos temporales de AWS que haya creado para la migración de datos, como la instancia de replicación de AWS DMS, y elimínelos después de validar la exportación.	Administrador de base de datos

Recursos relacionados

- Guía de usuario del servicio de migración de bases de datos de AWS
- Uso de una base de datos de Microsoft SQL Server como origen para AWS DMS
- Uso de Amazon S3 como destino para el servicio de migración de bases de datos de AWS
- Uso de un bucket de S3 como destino de AWS DMS (AWS re:POST)

Información adicional

Utilice el siguiente código para añadir una política de IAM con permisos de bucket de S3 para la función DMS de AWS. Reemplace `bucketname` con el nombre de su bucket.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Effect": "Allow",
             "Action": [
                 "s3:PutObject",
                 "s3:DeleteObject"
             ],
             "Resource": [
                 "arn:aws:s3:::bucketname*"
             ]
         },
         {
```

```
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucketname*"
            ]
        }
    ]
}
```

Migración de valores CLOB de Oracle a filas individuales en PostgreSQL en AWS

Sai Krishna Namburu y Sindhusha Paturu, Amazon Web Services

Resumen

Este patrón describe cómo dividir valores de objetos grandes (CLOB) de Oracle en filas individuales en Amazon Aurora compatible con PostgreSQL y Amazon Relational Database Service (Amazon RDS) para PostgreSQL. PostgreSQL no admite el tipo de datos CLOB.

Las tablas con particiones de intervalos se identifican en la base de datos de Oracle de origen, y el nombre de la tabla, el tipo de partición, el intervalo de partición y otros metadatos se registran y cargan en la base de datos de destino. Puede cargar datos CLOB de tamaño inferior a 1 GB en tablas de destino como texto mediante AWS Database Migration Service (AWS DMS), o bien puede exportar los datos en formato CSV, cargarlos en un bucket de Amazon Simple Storage Service (Amazon S3) y migrarlos a su base de datos PostgreSQL de destino.

Tras la migración, puede usar el código de PostgreSQL personalizado proporcionado con este patrón para dividir los datos CLOB en filas individuales en función del nuevo identificador de caracteres de línea (`CHR(10)`) y rellenar la tabla de destino.

Requisitos previos y limitaciones

Requisitos previos

- Una tabla de base de datos de Oracle con particiones de intervalos y registros con tipo de datos CLOB.
- Una base de datos de Aurora compatible con PostgreSQL o Amazon RDS para PostgreSQL con una estructura de tabla similar a la tabla de origen (las mismas columnas y tipos de datos).

Limitaciones

- El valor de CLOB no puede superar 1 GB.
- Cada fila de la tabla de destino debe tener un nuevo identificador de caracteres de línea.

Versiones de producto

- Oracle 12c
- Aurora PostgreSQL 11.6

Arquitectura

El siguiente diagrama muestra una tabla de origen de Oracle con datos CLOB, y la tabla PostgreSQL equivalente en Aurora compatible con PostgreSQL versión 11.6.

Tools (Herramientas)

Servicios de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.
- Amazon Relational Database Service (Amazon RDS) para PostgreSQL le ayuda a configurar, utilizar y escalar una base de datos relacional de PostgreSQL en la nube de AWS.
- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

Puede usar las siguientes herramientas de cliente para conectarse, acceder y gestionar sus bases de datos de Aurora compatible con PostgreSQL y Amazon RDS para PostgreSQL. (Estas herramientas no se usan en este patrón).

- pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.
- DBeaveres una herramienta de base de datos de código abierto para desarrolladores y administradores de bases de datos. Esta herramienta le permite manipular, supervisar, analizar, administrar y migrar sus datos.

Prácticas recomendadas

Para conocer las prácticas recomendadas para migrar su base de datos de Oracle a PostgreSQL, consulte la publicación del blog de AWS Prácticas recomendadas para migrar una base de datos de Oracle a Amazon RDS PostgreSQL o Amazon Aurora PostgreSQL: consideraciones sobre el proceso de migración y la infraestructura.

Para obtener información sobre las prácticas recomendadas para configurar la tarea de AWS DMS para migrar objetos binarios grandes, consulte Migración de objetos binarios grandes (LOBs) en la documentación de AWS DMS.

Epics

Identifique los datos de CLOB

Tarea	Descripción	Habilidades requeridas
Analice los datos de CLOB.	En la base de datos de Oracle de origen, analice los datos de CLOB para comprobar si contienen encabezad os de columna y así poder determinar el método de carga de los datos en la tabla de destino. Para analizar los datos de entrada, ejecute la siguiente consulta. `SELECT * FROM clobdata_or;`	Desarrollador
Cargue los datos de CLOB en la base de datos de destino.	Migre la tabla que contiene datos de CLOB a una tabla provisional (transitoria) en la base de datos de destino de Aurora o Amazon RDS. Puede usar AWS DMS o cargar los datos en formato de archivo CSV a un bucket de Amazon S3. Para obtener más informaci ón sobre el uso de AWS DMS para esta tarea, consulte	Ingeniero de migraciones, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	Uso de una base de datos de Oracle como fuente y Uso de una base de datos PostgreSQL como destino en la documentación de AWS DMS. Para obtener más información sobre el uso de Amazon S3 para esta tarea, consulte Uso de Amazon S3 como destino en la documentación de AWS DMS.	

Valide la tabla PostgreSQL de destino.	Valide los datos de destino, incluidos los encabezados, comparándolos con los datos de origen. Para ello, ejecute las siguientes consultas en la base de datos de destino.
	
	`SELECT * FROM clobdata_pg;`
	`SELECT * FROM clobdatatarget;`
	
	Compare los resultados con los resultados de las consultas a la base de datos de origen (desde el primer paso).
		Desarrollador

Tarea	Descripción	Habilidades requeridas
Divida los datos de CLOB en filas independientes.	Ejecute el código PostgreSQL personalizado que se proporciona en la sección Información adicional para dividir los datos CLOB e insertarlos en filas independientes en la tabla PostgreSQL de destino.	Desarrollador

Valide los datos.

Tarea	Descripción	Habilidades requeridas

Valide los datos en la tabla de destino.	Valide los datos insertados en la tabla de destino ejecutando las siguientes consultas.
	`SELECT * FROM clobdata_pg;`
	`SELECT * FROM clobdatatarget;`
		Desarrollador

Recursos relacionados

- Tipo de datos CLOB (documentación de Oracle)
- Tipos de datos (documentación de PostgreSQL)

Información adicional

Función de PostgreSQL para dividir datos CLOB

```
do
$$
```

```
declare
totalstr varchar;
str1 varchar;
str2 varchar;
pos1 integer := 1;
pos2 integer ;
len integer;


begin
        select rawdata||chr(10) into totalstr from clobdata_pg;
        len :=  length(totalstr) ;
        raise notice 'Total length : %',len;
        raise notice 'totalstr : %',totalstr;
        raise notice 'Before while loop';


        while pos1 < len  loop


                  select position (chr(10) in totalstr) into pos2;
                 raise notice '1st position of new line : %',pos2;


                str1 := substring (totalstr,pos1,pos2-1);
                raise notice 'str1 : %',str1;


                   insert into clobdatatarget(data) values (str1);
                   totalstr := substring(totalstr,pos2+1,len);
                   raise notice 'new totalstr :%',totalstr;
                len :=  length(totalstr) ;


        end loop;
end
$$
LANGUAGE 'plpgsql' ;
```

Ejemplos de entrada y salida

Puede usar los siguientes ejemplos para probar el código PostgreSQL antes de migrar los datos.

Cree una base de datos de Oracle con tres líneas de entrada.

```
CREATE TABLE clobdata_or (
id INTEGER GENERATED ALWAYS AS IDENTITY,
rawdata clob  );


insert into clobdata_or(rawdata) values (to_clob('test line 1') || chr(10) ||
 to_clob('test line 2') || chr(10) || to_clob('test line 3') || chr(10));
COMMIT;


SELECT * FROM clobdata_or;
```

Se mostrarán los siguientes valores.

id	rawdata
1	test line 1 test line 2 test line 3

Cargue los datos de origen en una tabla transitoria de PostgreSQL (`clobdata_pg`) para su procesamiento.

```
SELECT * FROM clobdata_pg;

CREATE TEMP TABLE clobdatatarget (id1 SERIAL,data VARCHAR );

<Run the code in the additional information section.>

SELECT * FROM clobdatatarget;
```

Se mostrarán los siguientes valores.

id1	datos
1	Línea de prueba 1
2	Línea de prueba 2
3	Línea de prueba 3

Migre Oracle PeopleSoft a Amazon RDS Custom

Gaurav Gupta, Amazon Web Services

Resumen

Oracle PeopleSoft es una solución de planificación de recursos empresariales (ERP) para procesos de toda la empresa. PeopleSoft tiene una arquitectura de tres niveles: cliente, aplicación y base de datos. PeopleSoft se puede ejecutar en Amazon Relational Database Service (Amazon RDS). Ahora, también puede ejecutar PeopleSoft en Amazon RDS Custom, que proporciona acceso al sistema operativo subyacente.

Amazon RDS Custom para Oracle es un servicio de base de datos administrado para aplicaciones heredadas, personalizadas y empaquetadas que requieren acceso al sistema operativo y al entorno de base de datos subyacentes. Al migrar la base de datos de Oracle a Amazon RDS Custom, Amazon Web Services (AWS) puede gestionar las tareas de backup y la alta disponibilidad, al tiempo que usted puede centrarse en el mantenimiento de la PeopleSoft aplicación y la funcionalidad. Para conocer los factores clave a tener en cuenta durante la planificación de una migración, consulte Estrategias de migración de bases de datos de Oracle en Recomendaciones de AWS.

Este patrón se centra en los pasos para migrar una PeopleSoft base de datos de Amazon Elastic Compute Cloud (Amazon EC2) a Amazon RDS Custom mediante una copia de seguridad de Oracle Recovery Manager (RMAN). Utiliza un sistema de archivos compartido Amazon Elastic File System (Amazon EFS) entre la instancia EC2 y Amazon RDS Custom, aunque también puede utilizar Amazon FSx o cualquier unidad compartida. El patrón utiliza una copia de seguridad completa en RMAN (a veces denominada copia de seguridad de nivel 0).

Requisitos previos y limitaciones

Requisitos previos

- Base de datos de origen de Oracle versión 19C que se ejecuta en Amazon EC2 con Oracle Linux 7, Oracle Linux 8, Red Hat Enterprise Linux (RHEL) 7 o RHEL 8. En los ejemplos de este patrón, el nombre de la base de datos de origen es `FSDM092`, pero no es obligatorio.

> **Note**
>
> También puede utilizar este patrón con las bases de datos de origen de Oracle en las instalaciones. Debe tener la conectividad de red adecuada entre la red en las instalaciones y una nube privada virtual (VPC).

- Una instancia de demostración de PeopleSoft 9.2.
- Un único nivel PeopleSoft de aplicación. Sin embargo, puede adaptar este patrón para que funcione con varios niveles de aplicación.
- Amazon RDS Custom está configurado con al menos 8 GB de espacio de intercambio.

Limitaciones

Este patrón no admite las siguientes configuraciones:

- Cómo establecer el parámetro `ARCHIVE_LAG_TARGET` de la base de datos en un valor fuera del rango de 60 a 7200
- Cómo inhabilitar el modo de registro de la instancia de base de datos (`NOARCHIVELOG`)
- Cómo desactivar el atributo optimizado Amazon Elastic Block Store (Amazon EBS) de la instancia EC2
- Cómo modificar los volúmenes de EBS originales adjuntos a la instancia EC2
- Cómo añadir nuevos volúmenes de EBS o cambiar el tipo de volumen de gp2 a gp3
- Cómo cambiar el formato de extensión del parámetro `LOG_ARCHIVE_FORMAT` (requiere `*.arc`)
- Multiplexar o cambiar la ubicación y el nombre del archivo de control (tiene que ser `/rdsdbdata/db/*DBNAME*/controlfile/control-01.ctl`)

Para obtener información adicional sobre estas y otras configuraciones no compatibles, consulte la documentación de Amazon RDS.

Versiones de producto

Para ver las versiones de Oracle Database y clases de instancia compatibles con Amazon RDS Custom, consulte Requisitos y limitaciones de Amazon RDS Custom para Oracle.

Arquitectura

Pila de tecnología de destino

- Equilibrador de carga de aplicación
- Amazon EFS
- Amazon RDS Custom para Oracle
- AWS Secrets Manager

- Amazon Simple Storage Service (Amazon S3)

Arquitectura de destino

El siguiente diagrama de arquitectura representa un PeopleSoft sistema que se ejecuta en una única zona de disponibilidad en AWS. Se accede al nivel de aplicación a través de un Equilibrador de carga de aplicación. Tanto la aplicación como las bases de datos se encuentran en subredes privadas, y las instancias de base de datos Amazon RDS Custom y Amazon EC2 utilizan un sistema de archivos compartidos Amazon EFS para almacenar y acceder a los archivos de copia de seguridad de RMAN. Amazon S3 se utiliza para crear el motor RDS Oracle personalizado y para almacenar los metadatos de redo logs.

Tools (Herramientas)

Herramientas

Servicios de AWS

- Amazon RDS Custom para Oracle es un servicio de base de datos administrado para aplicaciones heredadas, personalizadas y empaquetadas que requieren acceso al sistema operativo y al entorno de base de datos subyacentes. Automatiza las tareas de administración de bases de datos, como las copias de seguridad y la alta disponibilidad.
- Amazon Elastic File System (Amazon EFS) le ayuda a crear y configurar sistemas de archivos compartidos en la nube de AWS. Este patrón emplea un sistema de archivos compartidos de Amazon EFS para almacenar y acceder a los archivos de copia de seguridad de RMAN.
- AWS Secrets Manager le permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación. En este patrón, se recuperan las contraseñas de usuario de la base de datos de Secrets Manager para crear los usuarios `RDSADMIN` y `ADMIN` y cambiar las contraseñas `sys` y `system`.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos. Así, por ejemplo, puede distribuir el tráfico a través de instancias de Amazon Elastic Compute Cloud (Amazon EC2), contenedores y direcciones IP de una o varias zonas de disponibilidad. Este patrón utiliza un equilibrador de carga de aplicación.

Otras herramientas

- Oracle Recovery Manager (RMAN) proporciona soporte de copia de seguridad y recuperación para bases de datos de Oracle. Este patrón utiliza RMAN para realizar una copia de seguridad activa de la base de datos de Oracle de origen en Amazon EC2 que se restaura en Amazon RDS Custom.

Prácticas recomendadas

- Para los parámetros de inicialización de la base de datos, personalice el perfil estándar que proporciona la instancia de base de datos personalizada de Amazon RDS PeopleSoft en lugar de utilizar el archivo spfile de la base de datos de origen de Oracle. El motivo de esto es que los espacios en blanco y los comentarios causan problemas al crear réplicas de lectura en Amazon RDS Custom. Para obtener más información sobre los parámetros de inicialización de la base de datos, consulte la nota de soporte de Oracle 1100831.1 (requiere una cuenta de Oracle Support).
- Amazon RDS Custom utiliza la administración automática de memoria de Oracle de forma predeterminada. Si desea utilizar el núcleo de Hugemem, puede configurar Amazon RDS Custom para que utilice en su lugar la gestión automática de la memoria compartida.
- Mantenga el parámetro `memory_max_target` habilitado de forma predeterminada. El marco lo utiliza en segundo plano para crear réplicas de lectura.
- Habilite la base de datos de Oracle Flashback. Esta característica resulta útil para restablecer el modo de espera en escenarios de pruebas de conmutación por error (no de transición).

Epics

Configure la instancia de base de datos y el sistema de archivos

Tarea	Descripción	Habilidades requeridas
Crear la instancia de base de datos.	En la consola de Amazon RDS, cree una instancia de base de datos Amazon RDS Custom for Oracle con un nombre de base de datos denominado FSDMO92 (o el nombre de la base de datos de origen).	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Para obtener más instrucciones, consulte Trabajo con Amazon RDS Custom en la documentación de AWS, y la publicación del blog Amazon RDS Custom for Oracle – New Control Capabilities in Database Environment. Este paso garantiza que la base de datos tenga el mismo nombre que la base de datos de origen. (Si se deja en blanco, la instancia de EC2 y el nombre de la base de datos se definirán como `ORCL`).	

Realice una copia de seguridad completa de RMAN de la base de datos de Amazon EC2 de origen

Tarea	Descripción	Habilidades requeridas

Cree un script de copia de seguridad.	Cree un script de copia de seguridad de RMAN para hacer una copia de seguridad de la base de datos en el sistema de archivos Amazon EFS que montó (`/efs` en el siguiente ejemplo). Puede usar el código de ejemplo o ejecutar uno de sus scripts de RMAN existentes.
	`#!/bin/bash`
	`Dt=`date +'%Y%m%d-%H%M'``
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	BACKUP_LOG="rman-${O RACLE_SID}-$Dt" export TAGDATE=`date + %Y%m%d%H%M`; LOGPATH=/u01/scripts/l ogs rman target / >> $LOGPATH/rman-${OR ACLE_SID}-$Dt << EOF SQL "ALTER SYSTEM SWITCH LOGFILE"; SQL "ALTER SESSION SET NLS_DATE_FORMAT="D D.MM.YYYY HH24:MI:S S""; RUN { ALLOCATE CHANNEL ch11 TYPE DISK MAXPIECESIZE 5G; ALLOCATE CHANNEL ch12 TYPE DISK MAXPIECESIZE 5G; BACKUP AS COMPRESSED BACKUPSET FULL DATABASE FORMAT '/efs/rma n_backup/FSCM/%d_%T_ %s_%p_FULL' ; SQL "ALTER SYSTEM ARCHIVE LOG CURRENT"; BACKUP FORMAT '/efs/ rman_backup/FSCM/%d_ %T_%s_%p_ARCHIVE' ARCHIVELOG ALL DELETE ALL INPUT ; BACKUP CURRENT CONTROLFILE FORMAT '/ efs/rman_backup/FSCM/ %d_%T_%s_%p_CONTROL'; } EXIT; EOF	

Tarea	Descripción	Habilidades requeridas

Ejecute el script de copia de seguridad.	Para ejecutar el script de copia de seguridad de RMAN, inicie sesión como Oracle Home User y ejecute el script.
	`$ chmod a+x rman_backup.sh`
	`$ ./rman_backup.sh &`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

Compruebe que no haya errores y anote el nombre del archivo de copia de seguridad.	Compruebe si hay errores en el archivo de registro RMAN. Si todo parece correcto, publique la copia de seguridad del archivo de control ejecutando el siguiente comando.
	`RMAN> list backup of controlfile;`
	`using target database control file instead of recovery catalog`
	Anote el nombre del archivo de salida.
	`List of Backup Sets ==================`
	`BS Key Type LV Size Device Type Elapsed Time Completion Time ------- ---- -- ---------- --------- -- ------------ ---------- 12 Full 21.58M DISK 00:00:01 13-JUL-22 BP Key: 12 Status: AVAILABLE Compressed: NO Tag: TAG20220713T150155 Piece Name: /efs/rman_backup/FSCM/FSDMO92_20220713_12_1_CONTROL`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`Control File Included: Ckp SCN: 165591599 85898 Ckp time: 13-JUL-22` Utilizará el archivo de control de la copia de seguridad `/efs/rman_backup/FSCM/FSDM092_20220713_12_1_CONTROL` cuando restaure la base de datos en Amazon RDS Custom.	

Apague el nivel de aplicación de origen

Tarea	Descripción	Habilidades requeridas
Cierre la aplicación.	Para cerrar el nivel de la aplicación de origen, utilice la utilidad `psadmin` o la utilidad de línea de comandos `psadmin`. 1. Para cerrar el servidor web, ejecute el siguiente comando. `psadmin -w shutdown -d "webserver domain name"` 2. Para cerrar el servidor de la aplicación, ejecute el siguiente comando.	DBA, administrador PeopleSoft

Tarea	Descripción	Habilidades requeridas

	`psadmin -c shutdown -d "application server domain name"`
	3. Para cerrar el programador de procesos, ejecute el siguiente comando.
	`psadmin -p stop -d "process scheduler domain name"`	

Configure la base de datos Amazon RDS Custom de destino

Tarea	Descripción	Habilidades requeridas
Instale el paquete nfs-utils rpm.	Para instalar el paquete `nfs-utils rpm`, ejecute el comando siguiente. `$ yum install -y nfs-utils`	Administrador de base de datos
Monte el almacenamiento EFS.	Obtenga el comando de montaje de Amazon EFS en la página de la consola de Amazon EFS. Monte el sistema de archivos EFS en la instancia de Amazon RDS mediante un cliente de Network File System (NFS). `sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsize=1048`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`576,hard,timeo=600 ,retrans=2,noresvp ort fs-xxxxxxxxxx.efs. eu-west-1.amazonaw s.com:/ /efs sudo mount -t nfs4 -o nfsvers=4.1,rsize= 1048576,wsize=1048 576,hard,timeo=600 ,retrans=2,noresvp ort fs-xxxxxxxxxx.efs. eu-west-1.amazonaw s.com:/ /efs`	

Elimine la base de datos inicial y cree los directorios para almacenar los archivos de la base de datos

Tarea	Descripción	Habilidades requeridas
Pause el modo de automatiz ación.	Debe pausar el modo de automatización en su instancia de base de datos de Amazon RDS Custom antes de continuar con los siguiente s pasos, para asegurarse de que la automatización no interfiera con la actividad de restauración de RMAN. Puede pausar la automatiz ación mediante la consola de AWS o el comando Interfaz de la línea de comandos de AWS (AWS CLI) (asegúres e de haber configurado AWS CLI primero).	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`aws rds modify-db-instance \ --db-instance-id entifier peoplesoft-fscm-92 \ --automation-mode all-paused \ --resume-full-au tomation-mode-minute 360 \ --region eu-west-1` Cuando especifique la duración de la pausa, asegúrese de dejar tiempo suficiente para la restauración de RMAN. Este tiempo dependerá del tamaño de la base de datos de origen, por lo que deberá modificar el valor 360 en consecuencia. Además, asegúrese de que el tiempo total de la automatización pausada no se superponga con la ventana de copia de seguridad o mantenimiento de la base de datos.	

Tarea	Descripción	Habilidades requeridas

Cree y modifique el archivo de parámetros para PeopleSoft	Para crear y modificar el perfil PeopleSoft, utilice el perfil estándar creado con la instancia de base de datos personalizada de Amazon RDS. Añada los parámetros que necesite. PeopleSoft
	
	1. Cambie a `rds user rdsdb` ejecutando el siguiente comando.
	
	`$ sudo su - rdsdb`
	
	2. Inicie sesión en SQL*Plus en la base de datos inicial y cree el pfile ejecutando el siguiente comando.
	
	`SQL> create pfile from spfile;`
	
	Esto crea el archivo en `$ORACLE_HOME/dbs` .
	
	3. Haga una copia de seguridad de este perfil.
	4. Edite el perfil para añadir o actualizar PeopleSoft los parámetros.
	
	`*._gby_hash_aggregation_enabled=false`
	
	`*._unnest_subquery=false`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	`*.nls_language='AMERICAN'`
	
	`*.nls_length_semantics='CHAR'`
	
	`*.nls_territory='AMERICA'`
	
	`*.open_cursors=1000`
	
	`*.db_files=1200`
	
	`*.undo_tablespace='UNDOTBS1'`
	
	PeopleSoft Los parámetros relacionados se encuentran en la nota de soporte de Oracle 1100831.1.
	5. Elimine la referencia al spfile del perfil.
	
	`*.spfile='/rdsdbin/oracle/dbs/spfileFSDM092.ora'`	

Tarea	Descripción	Habilidades requeridas

Elimine la base de datos inicial.	Para eliminar la base de datos Amazon RDS Custom existente, utilice el siguiente código.
	`$ sqlplus / as sysdba`
	`SQL> shutdown immediate ;`
	`SQL> startup mount exclusive restrict;`
	`SQL> drop database;`
	`SQL> exit`	

Tarea	Descripción	Habilidades requeridas
Restaure la base de datos Amazon RDS Custom a partir de la copia de seguridad.	Restaure la base de datos mediante el siguiente script. El script restaurará primero el archivo de control y, a continuación, restaurará toda la base de datos a partir de las piezas de respaldo almacenadas en el soporte EFS. #!/bin/bash Dt=`date +'%Y%m%d-%H%M'` BACKUP_LOG="rman-${ORACLE_SID}-$Dt" export TAGDATE=`date +%Y%m%d%H%M`; LOGPATH=/rdsdbdata/scripts/logs rman target / >> $LOGPATH/rman-${ORACLE_SID}-$Dt << EOF restore controlfile from "/efs/rman_backup/FSCM/FSDMO92_20220713_12_1_CONTROL"; alter database mount; run { set newname for database to '/rdsdbdata/db/FSDMO92_A/datafile/%f_%b'; SET NEWNAME FOR TEMPFILE 1 TO '/rdsdbdata/db/FSDMO92_A/datafile/%f_%b'; RESTORE DATABASE; SWITCH DATAFILE ALL; SWITCH TEMPFILE ALL;	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	RECOVER DATABASE; } EOF sqlplus / as sysdba >> $LOGPATH/rman-${OR ACLE_SID}-$Dt<<-EOF ALTER DATABASE RENAME FILE '/u01/psoft/db/ oradata/FSDMO92/redo0 1.log' TO '/rdsdbda ta/db/FSDMO92_A/on linelog/redo01.log'; ALTER DATABASE RENAME FILE '/u01/psoft/db/ oradata/FSDMO92/redo0 2.log' TO '/rdsdbda ta/db/FSDMO92_A/on linelog/redo02.log'; ALTER DATABASE RENAME FILE '/u01/psoft/db/ oradata/FSDMO92/redo0 3.log' TO '/rdsdbda ta/db/FSDMO92_A/on linelog/redo03.log'; alter database clear unarchived logfile group 1; alter database clear unarchived logfile group 2; alter database clear unarchived logfile group 3; alter database open resetlogs; EXIT EOF	

Recupere contraseñas de Secrets Manager, cree usuarios y cambie contraseñas

Tarea	Descripción	Habilidades requeridas
Recupere la contraseña de Secrets Manager.	Puede ejecutar este paso mediante la consola de AWS o la AWS CLI. Los siguientes pasos muestran instrucciones para la consola. 1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon RDS. 2. En el panel de navegación, seleccione Bases de datos y, a continuación, seleccione la base de datos Amazon RDS. 3. Seleccione la pestaña Configuración y anote el ID del recurso de la instancia. Tendrá el formato `db-<ID>` (por ejemplo, `db-73GJNHLGDNZNDOXNWXSECUW6LE`). 4. Abra la consola de Secrets Manager. 5. Elija el secreto que tenga el mismo nombre que `do-not-delete-custom-<resource_id>` , donde `resource-id` se refiere al Identificador de recurso que anotó en el paso 3.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	6. Seleccione Retrieve secret value (Recuperar valor secreto). Esta contraseña será la misma para los usuarios `sys`, `system`, `rdsadmin` y `admin`.	

Tarea	Descripción	Habilidades requeridas

Cree el usuario RDSADMIN.	`RDSADMIN` es el usuario de la base de datos para monitorear y orquestar la instancia de base de datos de Amazon RDS Custom. Ya que la base de datos inicial se ha eliminado y la base de datos de destino se ha restaurado desde el origen mediante RMAN, deberá volver a crear este usuario tras la operación de restauración para asegurarse de que la supervisión de Amazon RDS Custom funciona según lo previsto. También debe crear un perfil y un espacio de tabla independientes para el usuario de `RDSADMIN`.
	
	1. Ingrese los siguientes comandos en la pregunta de SQL.
	
	`SQL> set echo on feedback on serverout on`
	`SQL> @?/rdbms/admin/utlpwdmg.sql`
	`SQL> ALTER PROFILE DEFAULT LIMIT FAILED_LOGIN_ ATTEMPTS UNLIMITED PASSWORD_LIFE_TIME UNLIMITED`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	PASSWORD_VERIFY_F UNCTION NULL; 2. Crear el perfil RDSADMIN. SQL> set echo on feedback on serverout on SQL> alter session set "_oracle_script"=t rue; SQL> CREATE PROFILE RDSADMIN LIMIT COMPOSITE_LIMIT UNLIMITED SESSIONS_PER_USER UNLIMITED CPU_PER_SESSION UNLIMITED CPU_PER_CALL UNLIMITED LOGICAL_READS_PER _SESSION UNLIMITED LOGICAL_READS_PER _CALL UNLIMITED IDLE_TIME UNLIMITED CONNECT_TIME UNLIMITED PRIVATE_SGA UNLIMITED FAILED_LOGIN_ATTE MPTS 10 PASSWORD_LIFE_TIME UNLIMITED PASSWORD_REUSE_TIME UNLIMITED PASSWORD_REUSE_MAX UNLIMITED PASSWORD_VERIFY_F UNCTION NULL	

Tarea	Descripción	Habilidades requeridas
	PASSWORD_LOCK_TIME 86400/86400 PASSWORD_GRACE_TIME 604800/86400; 3. Cree el espacio de tabla RDSADMIN. SQL> CREATE BIGFILE TABLESPACE rdsadmin '/rdsdbdata/db/FSDMO92_A/datafile/rdsadmin.dbf' DATAFILE SIZE 7M AUTOEXTEND ON NEXT 1m LOGGING ONLINE PERMANENT BLOCKSIZE 8192 EXTENT MANAGEMENT LOCAL AUTOALLOCATE DEFAULT NOCOMPRESS SEGMENT SPACE MANAGEMENT AUTO; 4. Cree el usuario RDSADMIN. Sustituya la contraseña RDSADMIN por la contraseña que obtuvo anteriormente de Secrets Manager. SQL> CREATE USER rdsadmin IDENTIFIED BY xxxxxxxxxx DEFAULT TABLESPACE rdsadmin TEMPORARY TABLESPACE TEMP profile rdsadmin ; 5. Otorgue privilegios a RDSADMIN.	

Tarea	Descripción	Habilidades requeridas
	``` SQL> GRANT "CONNECT" TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT "RESOURCE " TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT "DBA" TO RDSADMIN; SQL> GRANT "SELECT_C ATALOG_ROLE" TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT ALTER SYSTEM TO RDSADMIN; SQL> GRANT UNLIMITED TABLESPACE TO RDSADMIN; SQL> GRANT SELECT ANY TABLE TO RDSADMIN; SQL> GRANT ALTER DATABASE TO RDSADMIN; SQL> GRANT ADMINISTER DATABASE TRIGGER TO RDSADMIN; SQL> GRANT ANY OBJECT PRIVILEGE TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT INHERIT ANY PRIVILEGES TO RDSADMIN; SQL> ALTER USER RDSADMIN DEFAULT ROLE ALL; ``` 6. Set the SYS, SYSTEM, and DBSNMP user profiles to RDSADMIN.	

Tarea	Descripción	Habilidades requeridas

	`SQL> set echo on feedback on serverout on`
	`SQL> alter user SYS profile RDSADMIN;`
	`SQL> alter user SYSTEM profile RDSADMIN;`
	`SQL> alter user DBSNMP profile RDSADMIN;`	

Cree el usuario maestro.	Ya que la base de datos inicial se ha eliminado y la base de datos de destino se ha restaurado desde el origen mediante RMAN, deberá volver a crear el usuario principal. En este ejemplo, el nombre del usuario principal es `admin`.
	`SQL> create user admin identified by <password>;`
	`SQL> grant dba to admin`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

Cambie las contraseñas del sistema.	Cambie las contraseñas del sistema usando la contraseña que obtuvo de Secrets Manager.
	`SQL> alter user sys identified by xxxxxxxxxx;`
	`SQL> alter user system identified by xxxxxxxxxx;`
	Si no cambia estas contraseñas, Amazon RDS Custom mostrará el mensaje de error “El usuario o las credenciales de usuario que supervisa la base de datos han cambiado”.
		Administrador de base de datos

Configure las entradas de TNS para Amazon RDS Custom y PeopleSoft

Tarea	Descripción	Habilidades requeridas
Configure el archivo tnsnames.	Para conectarse a la base de datos desde el nivel de aplicación, configure el archivo `tnsnames.ora` de forma que pueda conectarse a la base de datos desde el nivel de aplicación. En el siguiente ejemplo, puede ver que hay un enlace temporal al archivo `tnsnames.ora`, pero el archivo está vacío de forma predeterminada.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	<pre>$ cd /rdsdbbin/oracle/network/admin
	$ ls -ltr
	-rw-r--r-- 1 rdsdb database 1536 Feb 14 2018 shrept.lst
	lrwxrwxrwx 1 rdsdb database 30 Apr 5 13:19 listener.ora -> /rdsdbdata/config/listener.ora
	lrwxrwxrwx 1 rdsdb database 28 Apr 5 13:19 sqlnet.ora -> /rdsdbdata/config/sqlnet.ora
	lrwxrwxrwx 1 rdsdb database 30 Apr 5 13:19 tnsnames.ora -> /rdsdbdata/config/tnsnames.ora</pre>	

	1. Cree la entrada `tsnames.ora` . Debido a la forma en que la automatización de Amazon RDS analiza los archivos, deberá asegurarse de que la entrada no contenga espacios en blanco, comentarios ni líneas adicionales. De lo contrario , es posible que tenga problemas al utilizar algunos de ellos APIs, como create-db-instance-read -replica.	

Tarea	Descripción	Habilidades requeridas

	2. Sustituya el puerto, el host y el SID de acuerdo con los requisitos de la PeopleSoft base de datos. Utilice el siguiente código como ejemplo.
	`$ vi tnsnames.ora`
	`FSDMO92=(DESCRIP TION = (ADDRESS_ LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = x.x.x.x)(PORT = 1521))) (CONNECT_ DATA = (SERVER = DEDICATED) (SID = FSDMO92)))`
	3. Para confirmar que se puede acceder a la PeopleSoft base de datos, ejecute el siguiente comando.
	`$ tnsping FSDMO92`
	`TNS Ping Utility for Linux: Version 19.0.0.0.0 - Production on 14-JUL-2022 10:16:45`
	`Copyright (c) 1997, 2021, Oracle. All rights reserved.`
	`Used parameter files:`	

Tarea	Descripción	Habilidades requeridas

	`/rdsdbbin/oracle/network/admin/sqlnet.ora`
	
	`Used TNSNAMES adapter to resolve the alias`
	`Attempting to contact (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = x.x.x.x)(PORT = 1521))) (CONNECT_DATA = (SERVER = DEDICATED) (SID = FSDMO92)))`
	`OK (0 msec)`	

Cree el enlace temporal de spfile

Tarea	Descripción	Habilidades requeridas
Cree el enlace temporal de spfile.	1. Para crear spfile en la ubicación `/rdsdbdata/admin/FSDMO92/pfile` , ejecute el siguiente comando. `SQL> create spfile='/rdsdbdata/admin/FSDMO92/pfile/spfileFSDMO92.ora' from pfile;` 2. Navegue hasta `$ORACLE_HOME/dbs` y cree un enlace temporal para spfile.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`ln -s '/rdsdbdata/admin/FSDMO92/pfile/spfileFSDMO92.ora' spfileFSDMO92.ora` 3. Una vez creado este archivo, puede cerrar e iniciar la base de datos mediante el spfile.	

Realice los pasos posteriores a la migración

Tarea	Descripción	Habilidades requeridas
Valide el esquema, las conexiones y las tareas de mantenimiento.	Para finalizar la migración, realice las siguientes tareas. • Recopile las estadísticas del esquema. • Asegúrese de que el nivel de PeopleSoft aplicación se pueda conectar a la nueva base de datos Amazon RDS Custom. • Configure sus programas de respaldo y mantenimiento.	Administrador de base de datos

Recursos relacionados

- Trabajar con Amazon RDS Custom
- Amazon RDS Custom for Oracle – New Control Capabilities in Database Environment (entrada del blog)
- Integrate Amazon RDS Custom for Oracle with Amazon EFS (entrada del blog)

- Configuración de Amazon RDS como una PeopleSoft base de datos de Oracle (documento técnico de AWS)

Migración de la funcionalidad ROWIdentificador de Oracle a PostgreSQL en AWS

Rakesh Raghav y Ramesh Pathuri, Amazon Web Services

Resumen

Este patrón describe las opciones para migrar la funcionalidad de `ROWID` pseudocolumnas de Oracle Database a una base de datos PostgreSQL en Amazon Relational Database Service (Amazon RDS) para PostgreSQL, Amazon Aurora PostgreSQL Compatible Edition o Amazon Elastic Compute Cloud (Amazon). EC2

En una base de datos de Oracle, la pseudocolumna `ROWID` es la dirección física de una fila de una tabla. Esta pseudocolumna se utiliza para identificar de forma exclusiva una fila, incluso si la clave principal no está presente en la tabla. PostgreSQL tiene una pseudocolumna similar llamada `ctid`, pero no se puede usar como `ROWID`. Como se explica en la documentación de PostgreSQL, `ctid` puede cambiar si se actualiza o después de cada proceso `VACUUM`.

Hay tres maneras de crear la funcionalidad de pseudocolumnas `ROWID` en PostgreSQL:

- Utilice una columna de clave principal en lugar de `ROWID` para identificar una fila de una tabla.
- Utilice una primary/unique clave lógica (que puede ser una clave compuesta) en la tabla.
- Agregue una columna con valores generados automáticamente y conviértala en una primary/unique clave para imitar`ROWID`.

Este patrón le guía por las tres implementaciones y describe las ventajas y desventajas de cada opción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Experiencia en codificación procedimental Language/PostgreSQL (PL/pgSQL)
- Base de datos de origen de Oracle
- Un clúster de Amazon RDS for PostgreSQL o Aurora compatible con PostgreSQL, o una instancia para alojar la base de datos de PostgreSQL EC2

Limitaciones

- Este patrón proporciona soluciones alternativas para la funcionalidad de `ROWID`. PostgreSQL no proporciona un equivalente a `ROWID` en Oracle Database.

Versiones de producto

- PostgreSQL 11.9 o posterior

Arquitectura

Pila de tecnología de origen

- Base de datos de Oracle

Pila de tecnología de destino

- Aurora compatible con PostgreSQL, Amazon RDS for PostgreSQL o una instancia con una base de datos PostgreSQL EC2

Opciones de implementación

Existen tres opciones para solucionar la falta de compatibilidad de `ROWID` con PostgreSQL, en función de si la tabla tiene una clave principal o un índice único, una clave principal lógica o un atributo de identidad. La elección depende de los plazos del proyecto, de la fase de migración actual y de las dependencias del código de la aplicación y de la base de datos.

Opción	Description (Descripción)	Ventajas	Desventajas
Clave principal o índice único	Si la tabla de Oracle tiene una clave principal, puede utilizar los atributos de esta clave para identificar de forma exclusiva una fila.	• No depende de las funciones de la base de datos patentada. • El impacto en el rendimiento es mínimo, ya que los	• Requiere cambios en el código de la aplicación y la base de datos en el que se basa en `ROWID` para cambiar a los

		campos de clave principal están indexados.	campos de clave principal.
primary/unique Clave lógica	Si la tabla de Oracle tiene una clave principal lógica, puede utilizar los atributos de esta clave para identificar de forma exclusiva una fila. Una clave principal lógica consta de un atributo o un conjunto de atributos que pueden identificar de forma única una fila, pero no se aplica a la base de datos mediante una restricción.	• No depende de las funciones de la base de datos patentada.	• Requiere cambios en el código de la aplicación y la base de datos en el que se basa en `ROWID` para cambiar a los campos de clave principal. • Si los atributos de la clave principal lógica no están indexados, se produce un impacto significativo en el rendimiento. No obstante, puede añadir un índice único para evitar problemas de rendimiento.

Atributo de identidad	si la tabla de Oracle no tiene una clave principal, puede crear un campo adicional como `GENERATED ALWAYS AS IDENTITY`. Este atributo genera un valor único cada vez que se insertan datos en la tabla, por lo que se puede utilizar para identificar de forma única una fila para las operaciones del lenguaje de manipulación de datos (DML).	• No depende de las funciones de la base de datos patentada. • La base de datos PostgreSQL rellena el atributo y mantiene su exclusividad.	• Requiere cambios en el código de la aplicación y la base de datos en el que se basa en `ROWID` para cambiar el atributo de identidad. • Si el campo adicional no está indexado, tiene un impacto significativo en el rendimiento. No obstante, puede añadir un índice para evitar problemas de rendimiento.

Tools (Herramientas)

- Amazon Relational Database Service (Amazon RDS) para PostgreSQL le ayuda a configurar, utilizar y escalar una base de datos relacional de PostgreSQL en la nube de AWS.
- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos. En este patrón, puede usar la AWS CLI para ejecutar comandos SQL a través de pgAdmin.
- pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.
- La Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de

origen y la mayor parte del código personalizado, lo que incluye las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino.

Epics

Identificar las tablas de origen

Tarea	Descripción	Habilidades requeridas
Identifique las tablas de Oracle que utilizan el atributo `ROWID`.	Utilice la herramienta de conversión de esquemas de AWS (AWS SCT) para identificar las tablas de Oracle que tienen funcionalidad de `ROWID`. Para obtener más información, consulte la documentación de AWS SCT. —o— En Oracle, utilice la vista de `DBA_TAB_COLUMNS` para identificar las tablas que tienen un atributo `ROWID`. Estos campos se pueden utilizar para almacenar caracteres alfanuméricos de 10 bytes. Determine el uso y conviértalos en un campo `VARCHAR`, si procede.	Administrador de base de datos o desarrollador
Identifique el código que hace referencia a estas tablas.	Utilice AWS SCT para generar un informe de evaluación de la migración a fin de identificar los procedimientos afectados por `ROWID`. Para obtener más información, consulte la documentación de AWS SCT.	Administrador de base de datos o desarrollador

Tarea	Descripción	Habilidades requeridas
	—o— En la base de datos de Oracle de origen, utilice el campo de texto de la tabla `dba_source` para identificar los objetos que utilizan la funcionalidad de `ROWID`.	

Determine el uso de clave principal

Tarea	Descripción	Habilidades requeridas
Identifica las tablas que no tienen claves principales.	En la base de datos de Oracle de origen, utilice `DBA_CONSTRAINTS` para identificar las tablas que no tienen claves principales. Esta información le ayudará a determinar la estrategia de cada tabla. Por ejemplo: `select dt.* from dba_tables dt where not exists (select 1 from all_constraints ct where ct.owner = Dt.owner and ct.table_name = Dt.table_name and ct.constraint_type = 'P' )`	Administrador de base de datos o desarrollador

Tarea	Descripción	Habilidades requeridas
	`and dt.owner = '{schema}'`	

Identifique y aplique la solución

Tarea	Descripción	Habilidades requeridas
Aplique cambios a las tablas que tengan una clave principal lógica o definida.	Realice los cambios en el código de la aplicación y la base de datos que se muestran en la sección Información adicional para utilizar una clave principal única o una clave principal lógica para identificar una fila de la tabla.	Administrador de base de datos o desarrollador
Agregue un campo adicional a las tablas que no tengan una clave principal lógica o definida.	Añada un atributo de tipo `GENERATED ALWAYS AS IDENTITY`. Realice los cambios en el código de la aplicación y la base de datos que se muestran en la sección Información adicional.	Administrador de base de datos o desarrollador
Añada un índice si es necesario.	Agregue un índice al campo adicional o a la clave principal lógica para mejorar el rendimiento de SQL.	Administrador de base de datos o desarrollador

Recursos relacionados

- CTID de PostgreSQL (documentación de PostgreSQL)
- Columnas generadas (documentación de PostgreSQL)

- Pseudocolumna ROWID (documentación de Oracle)

Información adicional

En las siguientes secciones se proporcionan ejemplos de código de Oracle y PostgreSQL para ilustrar los tres enfoques.

Escenario 1: Uso de una clave única principal

En los siguientes ejemplos, se crea la tabla `testrowid_s1` con `emp_id` la clave principal.

Código de Oracle:

```
create table testrowid_s1 (emp_id integer, name varchar2(10), CONSTRAINT testrowid_pk
 PRIMARY KEY (emp_id));
INSERT INTO testrowid_s1(emp_id,name) values (1,'empname1');
INSERT INTO testrowid_s1(emp_id,name) values (2,'empname2');
INSERT INTO testrowid_s1(emp_id,name) values (3,'empname3');
INSERT INTO testrowid_s1(emp_id,name) values (4,'empname4');
commit;

SELECT rowid,emp_id,name FROM testrowid_s1;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3pAAAAAAAMOAAA          1 empname1
AAAF3pAAAAAAAMOAAB          2 empname2
AAAF3pAAAAAAAMOAAC          3 empname3
AAAF3pAAAAAAAMOAAD          4 empname4

UPDATE testrowid_s1 SET name = 'Ramesh' WHERE rowid = 'AAAF3pAAAAAAAMOAAB' ;
commit;

SELECT rowid,emp_id,name FROM testrowid_s1;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3pAAAAAAAMOAAA          1 empname1
AAAF3pAAAAAAAMOAAB          2 Ramesh
AAAF3pAAAAAAAMOAAC          3 empname3
AAAF3pAAAAAAAMOAAD          4 empname4
```

Código PostgreSQL:

```
CREATE TABLE public.testrowid_s1
```

```
(
    emp_id integer,
    name character varying,
    primary key (emp_id)
);

insert into public.testrowid_s1 (emp_id,name) values
(1,'empname1'),(2,'empname2'),(3,'empname3'),(4,'empname4');

select emp_id,name from testrowid_s1;
 emp_id |   name
--------+----------
      1 | empname1
      2 | empname2
      3 | empname3
      4 | empname4

update testrowid_s1 set name = 'Ramesh' where emp_id = 2 ;

select emp_id,name from testrowid_s1;
 emp_id |   name
--------+----------
      1 | empname1
      3 | empname3
      4 | empname4
      2 | Ramesh
```

Escenario 2: uso de una clave principal lógica

En los ejemplos siguientes, se crea la tabla `testrowid_s2` con `emp_id` la clave principal lógica.

Código de Oracle:

```
create table testrowid_s2 (emp_id integer, name varchar2(10) );
INSERT INTO testrowid_s2(emp_id,name) values (1,'empname1');
INSERT INTO testrowid_s2(emp_id,name) values (2,'empname2');
INSERT INTO testrowid_s2(emp_id,name) values (3,'empname3');
INSERT INTO testrowid_s2(emp_id,name) values (4,'empname4');
commit;

SELECT rowid,emp_id,name FROM testrowid_s2;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3rAAAAAAAMeAAA          1 empname1
```

```
AAAF3rAAAAAAAMeAAB          2 empname2
AAAF3rAAAAAAAMeAAC          3 empname3
AAAF3rAAAAAAAMeAAD          4 empname4

UPDATE testrowid_s2 SET name = 'Ramesh' WHERE rowid = 'AAAF3rAAAAAAAMeAAB' ;
commit;

SELECT rowid,emp_id,name FROM testrowid_s2;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3rAAAAAAAMeAAA          1 empname1
AAAF3rAAAAAAAMeAAB          2 Ramesh
AAAF3rAAAAAAAMeAAC          3 empname3
AAAF3rAAAAAAAMeAAD          4 empname4
```

Código PostgreSQL:

```
CREATE TABLE public.testrowid_s2
(
    emp_id integer,
    name character varying
);

insert into public.testrowid_s2 (emp_id,name) values
(1,'empname1'),(2,'empname2'),(3,'empname3'),(4,'empname4');

select emp_id,name from testrowid_s2;
 emp_id |   name
--------+----------
      1 | empname1
      2 | empname2
      3 | empname3
      4 | empname4

update testrowid_s2 set name = 'Ramesh' where emp_id = 2 ;

select emp_id,name from testrowid_s2;
 emp_id |   name
--------+----------
      1 | empname1
      3 | empname3
      4 | empname4
      2 | Ramesh
```

Escenario 3: Uso de un atributo de identidad

En los ejemplos siguientes, se crea la tabla `testrowid_s3` sin clave principal y mediante un atributo de identidad.

Código de Oracle:

```
create table testrowid_s3 (name varchar2(10));
INSERT INTO testrowid_s3(name) values ('empname1');
INSERT INTO testrowid_s3(name) values ('empname2');
INSERT INTO testrowid_s3(name) values ('empname3');
INSERT INTO testrowid_s3(name) values ('empname4');
commit;

SELECT rowid,name FROM testrowid_s3;
ROWID              NAME
------------------ ----------
AAAF3sAAAAAAAMmAAA empname1
AAAF3sAAAAAAAMmAAB empname2
AAAF3sAAAAAAAMmAAC empname3
AAAF3sAAAAAAAMmAAD empname4

UPDATE testrowid_s3 SET name = 'Ramesh' WHERE rowid = 'AAAF3sAAAAAAAMmAAB' ;
commit;

SELECT rowid,name FROM testrowid_s3;
ROWID              NAME
------------------ ----------
AAAF3sAAAAAAAMmAAA empname1
AAAF3sAAAAAAAMmAAB Ramesh
AAAF3sAAAAAAAMmAAC empname3
AAAF3sAAAAAAAMmAAD empname4
```

Código PostgreSQL:

```
CREATE TABLE public.testrowid_s3
(
    rowid_seq bigint generated always as identity,
    name character varying
);

insert into public.testrowid_s3 (name) values
('empname1'),('empname2'),('empname3'),('empname4');
```

```
select rowid_seq,name from testrowid_s3;
 rowid_seq |   name
-----------+----------
         1 | empname1
         2 | empname2
         3 | empname3
         4 | empname4

update testrowid_s3 set name = 'Ramesh' where rowid_seq = 2 ;

select rowid_seq,name from testrowid_s3;
 rowid_seq |   name
-----------+----------
         1 | empname1
         3 | empname3
         4 | empname4
         2 | Ramesh
```

Migración de códigos de error de Oracle Database a una base de datos Amazon Aurora compatible con PostgreSQL

Sai Parthasaradhi y Veeranjaneyulu Grandhi, Amazon Web Services

Resumen

Este patrón muestra cómo migrar los códigos de error de Oracle Database a una base de datos de Amazon Aurora compatible con PostgreSQL mediante una tabla de metadatos predefinida.

Los códigos de error de Oracle Database no siempre tienen un código de error de PostgreSQL correspondiente. Esta diferencia en los códigos de error puede dificultar la configuración de la lógica de procesamiento de los procedimientos o funciones en la arquitectura PostgreSQL de destino.

Puede simplificar el proceso almacenando los códigos de error de la base de datos de origen y destino que son significativos para el PL/pgSQL programa en una tabla de metadatos. Configure la tabla para marcar los códigos de error válidos de Oracle Database y asignarlos a sus equivalentes de PostgreSQL antes de continuar con el resto de la lógica del proceso. Si el código de error de Oracle Database no está en la tabla de metadatos, el proceso finaliza con una excepción. Podrá revisar manualmente los detalles del error y añadir el nuevo código de error a la tabla si su programa lo requiere.

Al usar esta configuración, su base de datos Amazon Aurora compatible con PostgreSQL puede gestionar los errores de la misma manera que lo hace su base de datos de Oracle de origen.

> **Note**
>
> La configuración de una base de datos PostgreSQL para gestionar correctamente los códigos de error de Oracle Database suele requerir cambios en el código de la base de datos y de la aplicación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de Oracle de origen con servicios de instancia y oyente en ejecución
- Un clúster de Amazon Aurora compatible con PostgreSQL en ejecución

- Familiaridad con Oracle Database
- Familiaridad con bases de datos PostgreSQL

Arquitectura

El siguiente diagrama muestra un ejemplo de flujo de trabajo de base de datos Amazon Aurora compatible con PostgreSQL para la validación y gestión de códigos de error de datos:

En el diagrama, se muestra el siguiente flujo de trabajo:

1. La tabla contiene los códigos de error y clasificaciones de Oracle Database, así como los códigos de error y clasificaciones de PostgreSQL equivalentes. La tabla incluye una columna valid_error que clasifica si los códigos de error específicos y predefinidos son válidos o no.
2. Cuando una PL/pgSQL función (func_processdata) genera una excepción, invoca una segunda PL/pgSQL función (error_validation).
3. La función error_validation acepta el código de error de la base de datos de Oracle como argumento de entrada. A continuación, la función compara el código de error entrante con la tabla para comprobar si el error está incluido en la tabla.
4. Si el código de error de la base de datos de Oracle está incluido en la tabla, la función error_validation devuelve un valor TRUE y la lógica del proceso continúa. Si el código de error no está incluido en la tabla, la función devuelve un valor FALSE y la lógica del proceso se cierra con una excepción.
5. Cuando la función devuelve un valor FALSE, el responsable funcional de la aplicación revisa manualmente los detalles del error para determinar su validez.
6. A continuación, el nuevo código de error se añade manualmente a la tabla o no. Si el código de error es válido y se añade a la tabla, la función error_validation devolverá un valor TRUE la próxima vez que se produzca la excepción. Si el código de error no es válido y el proceso debe fallar cuando se produzca la excepción, el código de error no se agregará a la tabla.

Pila de tecnología

- PostgreSQL de Amazon Aurora
- pgAdmin
- Oracle SQL Developer

Tools (Herramientas)

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.
- pgAdmin es una plataforma de administración y desarrollo de código abierto para PostgreSQL. Proporciona una interfaz gráfica que ayuda a crear, mantener y usar objetos de base de datos.
- Oracle SQL Developer es un entorno de desarrollo integrado que simplifica el desarrollo y la administración de bases de datos de Oracle, tanto en implementaciones tradicionales como en implementaciones basadas en la nube.

Epics

Migración de códigos de error de Oracle Database a una base de datos Amazon Aurora compatible con PostgreSQL

Tarea	Descripción	Habilidades requeridas
Cree una tabla en la base de datos de Amazon Aurora compatible con PostgreSQL.	Ejecute el comando de PostgreSQL CREATE TABLE: `( source_error_code numeric NOT NULL, target_error_code character varying NOT NULL, valid_error character varying(1) NOT NULL );`	Desarrollador de PostgreSQL, Oracle, para PostgreSQL RDS/Aurora
Añada los códigos de error de PostgreSQL y sus correspon	Ejecute el comando de PostgreSQL INSERT para añadir los valores de código	Desarrollador de PostgreSQL, Oracle, para PostgreSQL RDS/Aurora

Tarea	Descripción	Habilidades requeridas
dientes códigos de error de Oracle Database a la tabla.	de error necesarios a la tabla error_codes. Los códigos de error de PostgreSQL deben usar un tipo de datos que varíe en caracteres (valor SQLSTATE). Los códigos de error de Oracle deben usar un tipo de datos numéricos (valor SQLCODE). Ejemplo de instrucciones de inserción: `insert into error_cod es values (-1817,'2 2007','Y'); insert into error_cod es values (-1816,'2 2007','Y'); insert into error_cod es values (-3114,'0 8006','N');` **Note** Si detecta excepcion es de conectividad de bases de datos Java (JDBC) específicas de Oracle, debe sustituir las por excepciones genéricas entre bases de datos o cambiar a	

Tarea	Descripción	Habilidades requeridas
	excepciones específicas de PostgreSQL.	
Cree una PL/pgSQL función para validar los códigos de error.	Cree una PL/pgSQL función ejecutando el comando CREATE FUNCTION de PostgreSQL. Asegúrese de que la función haga lo siguiente: • Aceptar los códigos de error de Oracle generados por un programa. • Comprobar si hay códigos de error en la tabla error_codes. • Devolver un valor TRUE o FALSE, en función de si el código de error está presente en la tabla de metadatos o no.	Desarrollador de PostgreSQL, Oracle, para PostgreSQL RDS/Aurora

Tarea	Descripción	Habilidades requeridas
Revise manualmente los nuevos códigos de error a medida que los vaya registrando la función. PL/pgSQL	Revise manualmente los nuevos códigos de error. Si un nuevo código de error es válido para su caso de uso, agréguelo a la tabla error_codes ejecutando el comando de PostgreSQL INSERT. -o bien- Si un código de error nuevo no es válido para su caso de uso, no lo añada a la tabla. La lógica del proceso seguirá fallando y se cerrará con una excepción cuando se produzca el error.	Desarrollador de PostgreSQL, Oracle, para PostgreSQL RDS/Aurora

Recursos relacionados

Apéndice A. Códigos de error de PostgreSQL (documentación de PostgreSQL)

Mensajes de error de base de datos (documentación de Oracle Database)

Migre SAP ASE de Amazon EC2 a Amazon Aurora compatible con PostgreSQL mediante AWS SCT y AWS DMS

Amit Kumar y Ankit Gupta, Amazon Web Services

Resumen

Este patrón describe cómo migrar una base de datos de SAP Adaptive Server Enterprise (SAP ASE) alojada en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) a una edición compatible con PostgreSQL de Amazon Aurora mediante la herramienta de conversión de esquemas de AWS (AWS SCT) y el Servicio de migración de bases de datos de AWS (AWS DMS). El patrón se centra tanto en la conversión del lenguaje de definición de datos (DDL) para los objetos almacenados como en la migración de datos.

Compatible con Aurora PostgreSQL, admite las cargas de trabajo de procesamiento de transacciones online (OLTP). Este servicio gestionado proporciona configuraciones que se escalan automáticamente según la demanda. Puede iniciar, cerrar, ampliar o reducir automáticamente la base de datos en función de las necesidades de la aplicación. Puede ejecutar su base de datos en la nube sin administrar ninguna instancia de base de datos. Compatible con Aurora PostgreSQL ofrece una opción rentable para las cargas de trabajo poco frecuentes, intermitentes o impredecibles.

El proceso de migración consta de dos fases principales:

- Conversión de esquemas de bases de datos con AWS SCT
- Migración de los datos mediante AWS DMS

En la sección Epics se proporcionan instrucciones detalladas para ambas fases. Para obtener información sobre la solución de problemas específicos del uso de AWS DMS con bases de datos de SAP ASE, consulte Solución de problemas con SAP ASE en la documentación de AWS DMS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos SAP ASE de origen en una EC2 instancia con servicios de servidor, base de datos y escucha en funcionamiento
- Una base de datos de destino Aurora compatible con PostgreSQL

Limitaciones

- El número de puerto para las conexiones puede ser 5432.
- La función huge_pages está activada de forma predeterminada, pero se puede modificar.
- Point-in-time La granularidad de la recuperación (PITR) es de 5 minutos.
- La replicación entre regiones no está disponible actualmente.
- El tamaño máximo de almacenamiento para una base de datos Aurora es de 128 TiB.
- Puede crear un máximo de 15 réplicas de lectura.
- El límite de tamaño de la tabla está limitado únicamente por el tamaño del volumen del clúster de Aurora, por lo que el tamaño máximo de la tabla para un clúster de base de datos compatible con Aurora PostgreSQL es de 32 TiB. Le recomendamos que siga estas prácticas recomendadas de diseño de tabla, como la partición de tablas grandes.

Versiones de producto

- Base de datos de origen: AWS DMS actualmente es compatible con SAP ASE 15, 15.5, 15.7 y 16.x. Consulte la Guía del usuario de AWS DMS para obtener la información más reciente sobre el soporte de versiones de SAP ASE.
- Base de datos de destino: PostgreSQL 9.4 y versiones posteriores (para la versión 9.x), 10.x, 11.x, 12.x, 13.x y 14.x. Consulte la Guía del usuario de AWS DMS para ver las últimas versiones compatibles de PostgreSQL.
- Amazon Aurora 1.x o posterior. Para obtener la información más reciente, consulte las versiones compatibles con Aurora PostgreSQL y las versiones del motor en la documentación de Aurora.

Arquitectura

Pila de tecnología de origen

- Base de datos SAP ASE que se ejecuta en Amazon EC2

Pila de tecnología de destino

- Base de datos Aurora compatible con PostgreSQL

Arquitectura de migración

Tools (Herramientas)

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.
- La herramienta de conversión de esquemas de AWS (AWS SCT) admite migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado a un formato compatible con la base de datos de destino.
- AWS DMS admite varias bases de datos de origen y destino diferentes. Para obtener más información, consulte Fuentes de migración de datos y Objetivos de migración de datos en la documentación de AWS DMS. Para obtener el soporte más completo de versiones y funciones, recomendamos que utilice la última versión de AWS DMS.

Epics

Configuración del entorno

Tarea	Descripción	Habilidades requeridas
Configure el acceso a la red en la EC2 instancia de origen.	Configure grupos de seguridad en la EC2 instancia que aloja la base de datos SAP ASE de origen. Para obtener instrucciones, consulta los grupos EC2 de seguridad de Amazon para instancias de Linux en la EC2 documentación de Amazon.	Administrador de sistemas
Cree su clúster de base de datos Aurora compatible con PostgreSQL de destino.	Instale, configure y lance un clúster compatible con Aurora PostgreSQL para la base de datos de destino.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte Creación de un clúster de base de datos de Amazon Aurora, en la documentación de Aurora.	
Configure la autorización para el clúster de base de datos de destino.	Configure grupos de seguridad y firewalls para la base de datos de destino. Para obtener instrucciones, consulte Creación de un clúster de base de datos de Amazon Aurora en la documentación de Aurora.	Administrador de base de datos, administrador de sistemas

Convierta el esquema de su base de datos con AWS SCT

Tarea	Descripción	Habilidades requeridas
Iniciar AWS SCT.	Para iniciar AWS SCT, siga las instrucciones de la documentación de AWS SCT. AWS SCT proporciona una interfaz de usuario basada en el proyecto para convertir automáticamente el esquema de la base de datos de su base de datos SAP ASE de origen en un formato compatible con su instancia de base de datos de Aurora compatible con PostgreSQL de destino.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree puntos de enlace SCT de AWS.	Cree puntos de conexión para las bases de datos de origen SAP ASE, y las bases de datos de desino PostgreSQL. Para obtener instrucciones, consulte la documentación de AWS SCT.	Administrador de base de datos
Generar un informe de evaluación.	Cree un informe de evaluació n de la migración de la base de datos para evaluar la migración y detectar cualquier objeto o función incompatible. Para obtener instrucciones, consulte la documentación de AWS SCT.	Administrador de base de datos
Convierta el esquema.	Convierta el esquema de la base de datos siguiendo las instrucciones de la documenta ción de AWS SCT.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Valide los objetos de la base de datos.	Si AWS SCT no puede convertir un objeto de base de datos, identificará su nombre y otros detalles. Debe convertir estos objetos manualmente. Para identificar estas discrepancias, siga las instrucciones de la entrada del blog de AWS sobre cómo Validar los objetos de la base de datos después de migrar de SAP ASE a Amazon RDS para PostgreSQL o Amazon Aurora PostgreSQL.	Administrador de base de datos

Analice la migración a AWS DMS

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.	Compruebe la compatibilidad de las versiones de las bases de datos SAP ASE con AWS DMS. Para obtener más informaci ón, consulte Orígenes de AWS DMS y Objetivos de AWS DMS en la documentación de AWS DMS.	Administrador de base de datos
Identifique los requisitos para el tipo y la capacidad de almacenamiento.	Elija la capacidad de almacenamiento adecuada para la base de datos de	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	destino en función del tamaño de la base de datos de origen.	
Elija el tipo de instancia, la capacidad y otras caracterí sticas de la instancia de replicación.	Elija el tipo de instancia, la capacidad, las funciones de almacenamiento y las funciones de red que mejor se adapten a sus necesidades. Para obtener orientación, consulte Elegir la instancia de replicación de AWS DMS correcta para la migración en la documentación de AWS DMS.	Administrador de base de datos, administrador de sistemas
Identifique los requisitos de seguridad de acceso a la red.	Identifique los requisitos de seguridad de acceso a la red para las bases de datos de origen y destino. Siga las instrucciones de Configuración de una red para una instancia de replicación en la documentación de AWS DMS.	Administrador de base de datos, administrador de sistemas

Migración de datos

Tarea	Descripción	Habilidades requeridas
Migre los datos mediante la creación de una tarea de migración en AWS DMS.	Para migrar datos, cree una tarea y siga las instrucciones en la documentación de AWS DMS.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características.	
Valide los datos.	Para validar que los datos se migraron con precisión de la base de datos de origen a la base de datos de destino, siga las pautas de validación de datos que se proporcionan en la documentación de AWS DMS.	Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Identificar la estrategia de migración de aplicaciones.	Elija una de las siete estrategias (7R) para migrar aplicaciones a la nube.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Seguir la estrategia de migración de aplicaciones.	Complete las tareas de la base de datos identificadas por el equipo de la aplicación, incluida la actualización de los detalles de la conexión DNS de la base de datos de destino y la actualización de las consultas dinámicas.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Realizar la transición a la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Cambie los clientes de la aplicación a la nueva infraestructura.	Cambie la conexión de la base de datos de origen a la base de datos de destino. Para obtener más información, consulte la sección de Transición de la Estrategia de migración para bases de datos relacionales.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.	Finalice todas las tareas de migración, las instancias de replicación, los puntos de enlace y otros recursos de AWS SCT y AWS DMS. Para obtener más información, consulte la documentación de AWS DMS.	Administrador de base de datos, administrador de sistemas
Revise y valide los documentos del proyecto.	Valide todos los pasos de la documentación del proyecto para asegurarse de que todas las tareas se hayan completado correctamente.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Cierre el proyecto.	Cierre el proyecto de migración y envíe sus comentarios.	Administrador de base de datos, propietario de la

Tarea	Descripción	Habilidades requeridas
		aplicación, administrador de sistemas

Recursos relacionados

Referencias

- Habilite las conexiones cifradas para las instancias de base de datos de PostgreSQL en Amazon RDS (Recomendaciones de AWS)
- Transporte bases de datos PostgreSQL entre dos instancias de base de datos de Amazon RDS mediante pg_transport (Recomendaciones de AWS)
- Precios de Amazon Aurora
- Prácticas recomendadas con Edición compatible con Amazon Aurora PostgreSQL (documentación de Amazon Aurora)
- Documentación de AWS SCT
- Documentación de AWS DMS
- Uso de una base de datos SAP ASE como origen para AWS DMS

Tutoriales y videos

- Introducción a AWS Database Migration Service (AWS DMS)
- AWS Database Migration Service (AWS DMS) (video)

Migración de los certificados SSL de Windows a un equilibrador de carga de aplicación mediante ACM

Chandra Sekhar Yaratha e Igor Kovalchuk, Amazon Web Services

Resumen

El patrón proporciona orientación sobre el uso de AWS Certificate Manager (ACM) para migrar los certificados Secure Sockets Layer (SSL) existentes de sitios web alojados en servidores locales o instancias de Amazon Elastic Compute Cloud (Amazon EC2) en Microsoft Internet Information Services (IIS). Después, los certificados SSL se pueden usar con Elastic Load Balancing en AWS.

SSL protege sus datos, afirma su identidad, proporciona una mejor clasificación en los motores de búsqueda, ayuda a cumplir los requisitos de la norma de seguridad de datos del sector de las tarjetas de pago (PCI DSS) y mejora la confianza de los clientes. Los desarrolladores y los equipos de TI que administran estas cargas de trabajo desean que sus aplicaciones e infraestructuras web, incluidos el servidor IIS y Windows Server, sigan cumpliendo con sus políticas básicas.

Este patrón incluye la exportación manual de los certificados SSL existentes desde Microsoft IIS, su conversión del formato de intercambio de información personal (PFX) al formato de correo privado mejorado (PEM) compatible con ACM y, a continuación, su importación a ACM en la cuenta de AWS. También se describe cómo crear un equilibrador de carga de aplicación para la aplicación y cómo configurar el equilibrador de carga de aplicación para que utilice los certificados importados. A continuación, las conexiones HTTPS finalizan en el equilibrador de carga de aplicación y no se necesita más sobrecarga de configuración en el servidor web. Para obtener más información, consulte Create an HTTPS listener for your Application Load Balancer (Crear un oyente HTTPS para el equilibrador de carga de aplicación).

Los servidores Windows utilizan archivos .pfx o .p12 para contener el archivo de clave pública (certificado SSL) y el archivo de clave privada exclusivo. La autoridad de certificación (CA) le proporciona su archivo de clave pública. El servidor se utiliza para generar el archivo de clave privada asociado en el que se creó la solicitud de firma de certificados (CSR).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una nube privada virtual (VPC) en AWS con al menos una subred privada y una pública en cada zona de disponibilidad utilizada por los destinos

- La versión 8.0 o posterior de IIS se ejecuta en Windows Server 2012 o posterior
- Una aplicación web que se ejecute en IIS
- Acceso de administrador al servidor IIS

Arquitectura

Pila de tecnología de origen

- Implementación de un servidor web IIS con SSL para garantizar que los datos se transmitan de forma segura en una conexión cifrada (HTTPS)

Arquitectura de origen

Pila de tecnología de destino

- Certificados ACM en su cuenta de AWS
- Un equilibrador de carga de aplicación configurado para usar certificados importados
- Instancias de Windows Server en las subredes privadas

Arquitectura de destino

Tools (Herramientas)

- AWS Certificate Manager (ACM) le ayuda a crear, almacenar y renovar claves y certificados SSL/TLS X.509 públicos y privados que protegen sus sitios web y aplicaciones de AWS.
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos. Por ejemplo, puede distribuir el tráfico entre EC2 instancias, contenedores y direcciones IP en una o más zonas de disponibilidad.

Prácticas recomendadas

- Imponga redireccionamientos de tráfico de HTTP a HTTPS.
- Configure correctamente los grupos de seguridad para su equilibrador de carga de aplicación para permitir el tráfico entrante solo a puertos específicos.

- Lance sus EC2 instancias en diferentes zonas de disponibilidad para garantizar una alta disponibilidad.
- Configure el dominio de la aplicación para que apunte al nombre DNS del equilibrador de carga de aplicación en lugar de a su dirección IP.
- Asegúrese de que el equilibrador de carga de aplicación tenga configuradas las comprobaciones de estado de la capa de aplicación.
- Configure el umbral para las comprobaciones de estado.
- Usa Amazon CloudWatch para monitorear el Application Load Balancer.

Epics

Exportar un archivo .pfx

Tarea	Descripción	Habilidades requeridas
Exporte el archivo .pfx desde Windows Server.	Para exportar el certificado SSL como un archivo .pfx desde el administrador de IIS en las instalaciones de Windows Server: 1. Seleccione Start (iniciar) , Administrative (Admin), Internet Information Services (IIS) Manager. 2. Seleccione el nombre del servidor y, en Security (Seguridad), haga doble clic en Server Certificates (Certificados de servidor). 3. Seleccione el certificado que desea exportar y, a continuación, Export. 4. En el cuadro Export Certificate (Exportar certificado) seleccione una	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	ubicación, una ruta y un nombre para el archivo .pfx. 5. Especifique y confirme una contraseña para el archivo .pfx. **Note** Necesitará esta contraseña al instalar el archivo .pfx. 6. Seleccione Aceptar. El archivo .pfx ahora debería guardarse en la ubicación y la ruta que especificó.	

Convertir el certificado codificado en PFX al formato PEM

Tarea	Descripción	Habilidades requeridas
Descargue e instale el kit de herramientas de OpenSSL.	1. Descargue e instale Win32/Win64 OpenSSL desde el sitio web de Shining Light Productions. 2. Agregue la ubicación de los archivos binarios de OpenSSL a la variable PATH de sistema para que estén disponibles para su uso en la línea de comandos.	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Convertir el certificado codificado en PFX al formato PEM.	Los pasos siguientes convierten el archivo de certificado firmado y codificado en PFX en tres archivos en formato PEM: • `cert-file.pem` contiene el SSL/TLS certificado del recurso. • `privatekey.pem` contiene la clave privada del certificado sin protección por contraseña. • `ca-chain.pem` contiene el certificado raíz de la CA. Para convertir el certificado codificado en PFX: 1. Ejecute Windows PowerShell. 2. Utilice el comando siguiente para extraer la clave pública del certificado del archivo PFX. Escriba la contraseña del certificado cuando se le pida. `openssl pkcs12 -in <filename>.pfx -nocerts -out withpw-privatekey.pem` El comando genera un archivo de clave	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas

	privada codificado en PEM denominado `privatekey.pem` . Escriba una contraseña para proteger el archivo de clave privada cuando se le solicite.
	3. Ejecute el comando siguiente para eliminar la contraseña. Cuando se le pida, proporcione la contraseña que creó en el paso 2.
	`openssl rsa -in withpw-privatekey.pem -out privatekey.pem`
	Si el comando se ejecuta correctamente, se muestra el mensaje “writing RSA key”.
	4. Utilice el comando siguiente para transferir el certificado del archivo PFX al archivo PEM.
	`openssl pkcs12 -in <file_name>.pfx -clcerts -nokeys -out cert-file.pem`
	Esto crea un archivo de certificado codificado para PEM denominado `cert-`	

Tarea	Descripción	Habilidades requeridas
	`file.pem` . Si el comando se ejecuta correctamente, se muestra el mensaje “MAC verified OK”. 5. Cree un archivo de cadena CA a partir del archivo PFX. Ejecute el comando siguiente para crear un archivo de cadena CA llamado `ca-chain.pem` . `openssl pkcs12 -in <file_name>.pfx -cacerts -nokeys -chain -out ca-chain.pem` Si el comando se ejecuta correctamente, se muestra el mensaje “MAC verified OK”.	

Importar un certificado a ACM

Tarea	Descripción	Habilidades requeridas
Prepárese para importar el certificado.	En la consola ACM, seleccione Import a certificate (Importar un certificado).	Administrador de la nube
Proporcione el cuerpo del certificado.	En el Certificate body, pegue el certificado codificado en PEM para importar. Para obtener más información sobre los comandos y	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	los pasos descritos en esta y otras tareas de esta Epic, consulte Import a certificate (Importar un certificado) en la documentación de ACM.	
Proporcione la clave privada del certificado.	En Certificate private key, pegue la clave privada codificada en PEM y sin cifrar que coincida con la clave pública del certificado.	Administrador de la nube
Proporcione la cadena del certificado.	En Certificate chain (Cadena del certificado), pegue la cadena del certificado codificada en PEM, que se almacena en el archivo `CertificateChain.pem` .	Administrador de la nube
Importe el certificado.	Seleccione Review and import. Confirme que la información sobre su certificado es correcta y, a continuación, seleccione Import.	Administrador de la nube

Creación de un equilibrador de carga de aplicación

Tarea	Descripción	Habilidades requeridas
Cree y configure el equilibrador de carga y los oyentes.	Siga las instrucciones de la documentación de Elastic Load Balancing para configurar un grupo objetivo, registrar los objetivos y crear un equilibrador de carga de	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	aplicación y un oyente. Agregue un segundo oyente (HTTPS) para el puerto 443.	

Resolución de problemas

Problema	Solución
Windows PowerShell no reconoce el comando OpenSSL incluso después de agregarlo a la ruta del sistema.	Compruebe que `$env:path` incluya la ubicación de los binarios de OpenSSL. Si no es así, ejecute el siguiente comando en: PowerShell `$env:path = $env:path + ";C:\OpenSSL-Win64\bin"`

Recursos relacionados

Importing a certificate into ACM (Importar un certificado a ACM)

- Consola de ACM
- Certificate and key format for importing (Formato de certificado y de clave para importación)
- Importing a certificate (Importar un certificado)
- AWS Certificate Manager User Guide (Guía del usuario de AWS Certificate Manager)

Creating an Application Load Balancer (Crear un equilibrador de carga de aplicación)

- Creación de un equilibrador de carga de aplicación
- Application Load Balancer User Guide (Guía del usuario del equilibrador de carga de aplicación)

Migración de una cola de mensajes de Microsoft Azure Service Bus a Amazon SQS

Nisha Gambhir, Amazon Web Services

Resumen

Este patrón describe cómo migrar una aplicación web o de consola .NET Framework o .NET Core desde la plataforma de mensajería en cola Service Bus de Microsoft Azure a Amazon Simple Queue Service (Amazon SQS).

Las aplicaciones utilizan los servicios de mensajería para enviar y recibir datos de otras aplicaciones. Estos servicios ayudan a compilar microservicios disociados y altamente escalables, sistemas distribuidos y aplicaciones sin servidor en la nube.

Las colas de Azure Service Bus forman parte de una infraestructura de mensajería de Azure más amplia que admite las colas y publish/subscribe la mensajería.

Amazon SQS es un servicio de colas de mensajes completamente administrado que permite el desacople y el escalado de microservicios, sistemas distribuidos y aplicaciones sin servidor. Amazon SQS elimina la complejidad y la sobrecarga asociadas a la administración y el funcionamiento del middleware orientado a mensajes y permite a los desarrolladores centrarse en diferenciar el trabajo. Con Amazon SQS, puede enviar, almacenar y recibir mensajes entre componentes de software a cualquier volumen, sin perder mensajes ni requerir la disponibilidad de otros servicios.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una aplicación web o de consola .NET Framework o .NET Core que utiliza colas de Azure Service Bus (se adjunta un código de muestra)

Versiones de producto

- .NET Framework 3.5 o posterior, o .NET Core 1.0.1, 2.0.0 o posterior

Arquitectura

Pila de tecnología de origen

- Una aplicación web o de consola .NET (Core o Framework) que utiliza una cola de Azure Service Bus para enviar mensajes

Pila de tecnología de destino

- Amazon SQS

Tools (Herramientas)

Herramientas

- Microsoft Visual Studio

Código

Para crear una política de AWS Identity and Access Management (IAM) para Amazon SQS:

1. Inicie sesión en la consola de administración de AWS y abra la consola de IAM en https://console.aws.amazon.com/iam/.

2. En el panel de navegación de la izquierda, elija Políticas y, a continuación, elija Crear política.

3. Elija la pestaña JSON y pegue el siguiente código:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "sqs:DeleteMessage",
            "sqs:GetQueueUrl",
            "sqs:ChangeMessageVisibility",
            "sqs:SendMessageBatch",
            "sqs:ReceiveMessage",
            "sqs:SendMessage",
            "sqs:GetQueueAttributes",
            "sqs:ListQueueTags",
            "sqs:ListDeadLetterSourceQueues",
            "sqs:DeleteMessageBatch",
```

```
            "sqs:PurgeQueue",
            "sqs:DeleteQueue",
            "sqs:CreateQueue",
            "sqs:ChangeMessageVisibilityBatch",
            "sqs:SetQueueAttributes"
         ],
         "Resource": "arn:aws:sqs:*:<AccountId>:*"
      },
      {
         "Sid": "VisualEditor1",
         "Effect": "Allow",
         "Action": "sqs:ListQueues",
         "Resource": "*"
      }
   ]
}
```

4. Elija Revisar política, escriba un nombre y seleccione Crear política.

5. Adjunte la política recién creada a su rol de IAM existente o cree un rol nuevo.

Epics

Configuración de Amazon SQS en AWS

Tarea	Descripción	Habilidades requeridas
Cree una política de IAM para Amazon SQS.	Cree la política de IAM que proporcionará acceso a Amazon SQS. Consulte la sección Código para ver una muestra de política.	Ingeniero de sistemas
Crear un perfil de AWS.	Cree un perfil nuevo ejecutando las herramientas de AWS para PowerShell el comando Set-AWSCredential. Este comando almacena la clave de acceso y la clave secreta en el archivo de credenciales predeterminado bajo el	Ingeniero de sistemas

Tarea	Descripción	Habilidades requeridas
	nombre de perfil que especifiq ue. Vincule la política de Amazon SQS que creó anteriormente con esta cuenta. Conserve el ID de clave de acceso y la clave de acceso secreta de AWS. Estos serán necesarios en los pasos siguientes.	
Crear una cola de SQS.	Puede crear una cola estándar o una cola con el primero en entrar, primero en salir (FIFO). Para obtener instrucci ones, consulte el enlace de la sección Referencias.	Ingeniero de sistemas

Revisar el código de su aplicación .NET

Tarea	Descripción	Habilidades requeridas
Instalar AWS Toolkit for Visual Studio	Este kit de herramientas es una extensión para Microsoft Visual Studio y facilita la creación e implementación de aplicaciones .NET en AWS. Para obtener instrucciones de instalación y uso, consulte el enlace de la sección Referenci as.	Desarrollador de aplicaciones
Instale el paquete AWSSDK .SQS. NuGet	Puede instalar AWSSDK .SQS seleccionando «Administ rar NuGet paquete» en Visual Studio o ejecutando el	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	comando « AWSSDKInstall-Package .SQS».	
Cree un objeto en su AWSCredentials aplicació n.NET.	La aplicación de ejemplo del archivo adjunto muestra cómo crear un AWSCredentials objeto básico, que hereda de AWSCredentials. Puede utilizar el identificador de clave de acceso y la clave de acceso secreta de antes, o dejar que el objeto los elija de la carpeta .aws como parte del perfil de usuario en tiempo de ejecución.	Desarrollador de aplicaciones
Cree un objeto de cliente de SQS.	Cree un objeto cliente SQS (AmazonSQSClient) para .NET Framework. Esto forma parte del espacio de nombres Amazon.SQS. Este objeto es obligatorio en lugar del IQueue Cliente, que forma parte de Microsoft .Azure. ServiceBus espacio de nombres.	Desarrollador de aplicaciones
Llame al SendMessageAsync método para enviar mensajes a la cola de SQS.	Cambie el código que envía el mensaje a la cola para usar el. amazonSqsClient SendMessageAsync método. Para obtener más información, consulte el código de muestra adjunto.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Llame al ReceiveMessageAsync método para recibir mensajes de la cola de SQS.	Cambie el código que recibe el mensaje para usar el. amazonSqsClient ReceiveMessageAsync método. Para obtener más información, consulte el código de muestra adjunto.	Desarrollador de aplicaciones
Llame al DeleteMessageAsync método para eliminar los mensajes de la cola de SQS.	Para eliminar mensajes, cambie el código del QueueClient. CompleteAsync método para. amazonSqs Client DeleteMessageAsync método. Para obtener más información, consulte el código de muestra adjunto.	Desarrollador de aplicaciones

Recursos relacionados

- Guía para desarrolladores de AWS SDK para .NET
- Mensajería mediante Amazon SQS
- Creación y uso de una cola de Amazon SQS con AWS SDK para .NET
- Enviar un mensaje de Amazon SQS
- Recibir un mensaje de una cola de Amazon SQS
- Eliminar un mensaje de una cola de Amazon SQS
- AWS Toolkit for Visual Studio

Información adicional

Este patrón incluye dos aplicaciones de muestra (consulte la sección de adjuntos):

- AzureSbTestAppincluye código que usa la cola del bus de servicio de Azure.

- AmazonSqsTestApputiliza Amazon SQS. Se trata de una aplicación de consola que utiliza .NET Core 2.2 e incluye ejemplos para enviar y recibir mensajes.

Notas:

- QueueClient es un objeto de IQueue Client, que forma parte de Microsoft.Azure. ServiceBus espacio de nombres (incluido en Microsoft.Azure). ServiceBus NuGet paquete).
- amazonSqsClient es un objeto de AmazonSQSClient, que forma parte del espacio de nombres Amazon.sqs (incluido en el paquete .SQS). AWSSDK NuGet
- Según dónde se ejecute el código, por ejemplo, si se está ejecutando, el rol debe tener permiso para escribir en EC2 la cola de SQS.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migre una EnterpriseOne base de datos de Oracle JD Edwards a AWS mediante Oracle Data Pump y AWS DMS

Thanigaivel Thirumalai, Amazon Web Services

Resumen

Puede migrar y ejecutar la EnterpriseOne base de datos de JD Edwards en Amazon Relational Database Service (Amazon RDS). Al migrar la base de datos a Amazon RDS, AWS puede encargarse de las tareas de backup y de la configuración de alta disponibilidad, para que pueda concentrarse en el mantenimiento de EnterpriseOne la aplicación y su funcionalidad. Para obtener una lista completa de los factores clave a tener en cuenta durante el proceso de migración, consulte Estrategias de migración de bases de datos de Oracle en Recomendaciones de AWS.

Existen varias formas de migrar una EnterpriseOne base de datos, entre las que se incluyen las siguientes:

- Uso de Oracle Universal Batch Engine (UBE) R98403 para la creación de esquemas y tablas, y uso de AWS Database Migration Service (AWS DMS) para la migración
- Uso de herramientas nativas de bases de datos para la creación de esquemas y tablas y uso de AWS DMS para la migración
- Uso de herramientas nativas de bases de datos para la migración de datos existentes (carga completa) y uso de AWS DMS para tareas de captura de datos de cambios (CDC)

Este patrón cubre la tercera opción. En él se explica cómo migrar las EnterpriseOne bases de datos locales a Amazon RDS for Oracle mediante Oracle Data Pump con AWS DMS y su función CDC.

Oracle JD Edwards EnterpriseOne es una solución de planificación de recursos empresariales (ERP) para organizaciones que fabrican, construyen, distribuyen, dan servicio o gestionan productos o activos físicos. JD Edwards EnterpriseOne es compatible con varios hardware, sistemas operativos y plataformas de bases de datos.

Al migrar aplicaciones ERP fundamentales, como JD Edwards EnterpriseOne, es fundamental minimizar el tiempo de inactividad. AWS DMS minimiza el tiempo de inactividad gracias a su replicación, tanto continua como de carga completa, desde la base de datos de origen a la base de datos de destino. AWS DMS también proporciona supervisión y registro de la migración en tiempo real, lo que le ayudará a identificar y resolver cualquier problema que pueda provocar un tiempo de inactividad.

Cuando replique cambios con AWS DMS, debe especificar una hora o un número de cambio del sistema (SCN) como punto de partida para leer los cambios de los registros de la base de datos. Es crucial mantener estos registros accesibles en el servidor durante un periodo de tiempo determinado (recomendamos 15 días) para garantizar que AWS DMS tenga acceso a estos cambios.

Requisitos previos y limitaciones

Requisitos previos

- Una base de datos de Amazon RDS para Oracle aprovisionada en su entorno de la nube de AWS como base de datos de destino. Para obtener instrucciones, consulte la Documentación de Amazon RDS.
- Una EnterpriseOne base de datos que se ejecuta localmente o en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) en AWS.

> **Note**
>
> Este patrón está diseñado para migrar de las instalaciones a AWS, pero se probó con una EnterpriseOne base de datos en una instancia de EC2. Si planea migrar desde su entorno en las instalaciones, debe configurar la conectividad de red adecuada.

- Detalles del esquema. Identifique el esquema de base de datos de Oracle (por ejemplo DV920) para el que planea migrar. EnterpriseOne Antes de iniciar el proceso de migración, recopile los siguientes detalles sobre el esquema:
  - Tamaño del esquema
  - La cantidad de objetos por tipo de objeto
  - La cantidad de objetos no válidos

Limitaciones

- Debe crear los esquemas que desee en la base de datos de Amazon RDS para Oracle de destino; AWS DMS no los crea por usted. (La sección Epics describe cómo usar Data Pump para exportar e importar esquemas). El nombre del esquema debe existir ya para la base de datos de Oracle de destino. Las tablas del esquema de origen se importan al usuario o al esquema, y AWS DMS utiliza la cuenta del administrador o del sistema para conectarse a la instancia de destino. Para migrar varios esquemas, puede crear varias tareas de replicación. También puede migrar datos a

diferentes esquemas en una instancia de destino. Para ello, utilice las reglas de transformación de esquemas en las asignaciones de tablas de AWS DMS.

- Este patrón se probó con un conjunto de datos de demostración. Le recomendamos que valide la compatibilidad y la personalización de su conjunto de datos.
- Este patrón usa una EnterpriseOne base de datos que se ejecuta en Microsoft Windows. Sin embargo, puede utilizar el mismo proceso con otros sistemas operativos compatibles con AWS DMS.

Arquitectura

El siguiente diagrama muestra un sistema que se ejecuta EnterpriseOne en una base de datos Oracle como base de datos de origen y una base de datos Amazon RDS for Oracle como base de datos de destino. Los datos se exportan desde la base de datos de Oracle de origen y se importan a la base de datos Amazon RDS para Oracle de destino mediante Oracle Data Pump, y se replican para las actualizaciones de CDC mediante AWS DMS.

1. Oracle Data Pump extrae los datos de la base de datos de origen y los envía al destino de la base de datos de Amazon RDS para Oracle.
2. Los datos de CDC se envían desde la base de datos de origen a un punto de conexión de origen en AWS DMS.
3. Desde el punto de conexión de origen, los datos se envían a la instancia de replicación de AWS DMS, donde se realiza la tarea de replicación.
4. Una vez completada la tarea de replicación, los datos se envían al punto de conexión de destino en AWS DMS.
5. Desde el punto de conexión de destino, los datos se envían a la instancia de base de datos Amazon RDS para Oracle.

Tools (Herramientas)

Servicios de AWS

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Amazon Relational Database Service (Amazon RDS) para Oracle le ayuda a configurar, utilizar y escalar una base de datos relacional de Oracle en la nube de AWS.

Otros servicios

- Oracle Data Pump le ayuda a trasladar datos y metadatos entre una base de datos y otra a alta velocidad.

Prácticas recomendadas

Migrating LOBs

Si la base de datos de origen contiene objetos binarios de gran tamaño (LOBs) que deben migrarse a la base de datos de destino, AWS DMS ofrece las siguientes opciones:

- Modo LOB completo: AWS DMS migra todas las bases de datos LOBs de origen a la de destino, independientemente de su tamaño. Aunque la migración es más lenta que en los otros modos, la ventaja es que los datos no se truncan. Para mejorar el rendimiento, puede crear una tarea independiente en la nueva instancia de replicación para migrar las tablas LOBs que tengan un tamaño superior a unos pocos megabytes.
- Modo LOB limitado: usted especifica el tamaño máximo de los datos de la columna LOB, lo que permite a AWS DMS preasignar los recursos y aplicarlos de forma masiva. LOBs Si el tamaño de las columnas LOB supera el tamaño especificado en la tarea, AWS DMS trunca los datos y envía advertencias al archivo de registro de AWS DMS. Puede mejorar el rendimiento usando el modo LOB limitado si el tamaño de los datos de LOB se encuentra dentro del tamaño de LOB limitado.
- Modo LOB en línea: puede migrar LOBs sin truncar los datos ni ralentizar el rendimiento de la tarea al replicar tanto los datos pequeños como los grandes. LOBs En primer lugar, especifique un valor para el parámetro `InlineLobMaxSize`, que sólo está disponible cuando el modo LOB completo está establecido en `true`. La tarea de AWS DMS transfiere lo pequeño LOBs en línea, lo que es más eficiente. A continuación, AWS DMS migra el tamaño grande LOBs realizando una búsqueda en la tabla de origen. Sin embargo, el modo LOB en línea funciona únicamente en la fase de carga completa.

Generación de valores de secuencia

Durante el proceso de AWS DMS CDC, los números de secuencia incrementales no se replican desde la base de datos de origen. Para evitar discrepancias en los valores de secuencia, debe generar el valor de secuencia más reciente del origen para todas las secuencias y aplicarlo a la base de datos Amazon RDS para Oracle de destino.

AWS Secrets Manager

Para ayudarle a gestionar sus credenciales, le recomendamos que siga las instrucciones de la entrada del blog Gestionar sus credenciales de punto de conexión de AWS DMS con AWS Secrets Manager.

Rendimiento

- Instancias de replicación: para obtener orientación sobre cómo elegir el mejor tamaño de instancia, consulte Selección del mejor tamaño para una instancia de replicación en la documentación de AWS DMS.
- Opciones de conectividad: para evitar problemas de latencia, le recomendamos que elija la opción de conectividad adecuada. AWS Direct Connect proporciona el camino más corto a los recursos de AWS, ya que es una conexión dedicada entre los centros de datos corporativos y AWS. Mientras se encuentra en tránsito, el tráfico de red permanece en la red global de AWS y nunca pasa por Internet. Esto reduce la posibilidad de que se produzcan cuellos de botella o aumentos inesperados de la latencia en comparación con el uso de una VPN o de la Internet pública.
- Ancho de banda de la red: para optimizar el rendimiento, compruebe que el rendimiento de la red sea rápido. Si utiliza un túnel VPN entre la base de datos de origen en las instalaciones y AWS DMS, asegúrese de que el ancho de banda sea suficiente para su carga de trabajo.
- Paralelismo de tareas: puede acelerar la replicación de datos cargando varias tablas en paralelo durante la carga completa. Este patrón utiliza puntos de conexión del RDBMS, por lo que esta opción solo se aplica al proceso de carga completa. El paralelismo de las tareas se controla mediante el parámetro `MaxFullLoadSubTasks`, que determina cuántas subtareas a plena carga se ejecutan en paralelo. De forma predeterminada, este parámetro está establecido en 8, lo que significa que ocho tablas (si se seleccionan en el mapeo de tablas) se cargan juntas durante el modo completo. Puede ajustar este parámetro en la sección de configuración de tareas de carga completa del script JSON de la tarea.
- Paralelismo de tablas: AWS DMS también le permite cargar una sola tabla grande mediante varios subprocesos paralelos. Esto resulta especialmente útil para las tablas fuente de Oracle que tienen miles de millones de registros, así como varias particiones y subparticiones. Si la tabla de origen no está particionada, puede usar límites de columna para cargas paralelas.
- Dividir las cargas: al dividir las cargas en varias tareas o instancias de AWS DMS, recuerde los límites de las transacciones al capturar los cambios.

Epics

Utilice Oracle Data Pump para exportar el esquema EnterpriseOne

Tarea	Descripción	Habilidades requeridas

Genere el SCN.	Cuando la base de datos de origen esté activa y la EnterpriseOne aplicación la utilice, inicie la exportación de datos con Oracle Data Pump. En primer lugar, debe generar un número de cambio del sistema (SCN) a partir de la base de datos de origen, tanto para la coherencia de datos durante la exportación con Oracle Data Pump como punto de partida para el CDC en AWS DMS.
	
	Para generar el SCN actual a partir de su base de datos de origen, utilice la siguiente instrucción SQL:
	
	`SQL> select current_scn from v$database;`
	
	`CURRENT_SCN`
	`-----------`
	`30009727`
	
	Guarde el SCN generado. Utilizará el SCN cuando exporte los datos y para crear la tarea de replicación de AWS DMS.
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

Cree el archivo de parámetros.	Para crear un archivo de parámetros para exportar el esquema, puede usar el siguiente código.
	
	`directory=DMS_DATA_PUMP_DIR logfile=export_dms.log dumpfile=export_dms_data.dmp schemas=<schema name> flashback_scn=<SCN from previous command>`
	
	Note
	También puede definir su propio `DATA_PUMP_DIR` mediante los siguientes comandos, en función de sus necesidades.
	
	`SQL> CREATE OR REPLACE DIRECTORY DMS_DATA_PUMP_DIR AS '<Directory for dump>'; Directory created.`
	
	`SQL> GRANT READ, WRITE ON DIRECTORY DMS_DATA_PUMP_DIR TO SYSTEM; Grant succeeded.`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Exporte el esquema.	Para realizar la exportación, utilice la utilidad expdp como se indica a continuación: C:\Users\Administrator>expdp system/********@<DB Name> PARFILE='<Path to PAR file create above>' Export: Release 19.0.0.0.0 - Production on *** *** ** **:**:** **** Version 19.3.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Connected to: Oracle Database 19c Standard Edition 2 Release 19.0.0.0.0 - Production Starting "SYSTEM"."SYS_EXPORT_SCHEMA_02": system/**********@<DB Name>PARFILE='E:\exp_dms_datapump.par' Processing object type SCHEMA_EXPORT/TABLE/TABLE_DATA Processing object type SCHEMA_EXPORT/TABLE/INDEX/STATISTICS/INDEX_STATISTICS Processing object type SCHEMA_EXPORT/TABL	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	E/STATISTICS/TABLE _STATISTICS Processing object type SCHEMA_EXPORT/STAT ISTICS/MARKER Processing object type SCHEMA_EXPORT/USER Processing object type SCHEMA_EXPORT/ROLE _GRANT Processing object type SCHEMA_EXPORT/DEFA ULT_ROLE Processing object type SCHEMA_EXPORT/TABL ESPACE_QUOTA Processing object type SCHEMA_EXPORT/PRE_ SCHEMA/PROCACT_SCHEMA Processing object type SCHEMA_EXPORT/TABLE/ TABLE Processing object type SCHEMA_EXPORT/TABL E/GRANT/OWNER_GRANT/ OBJECT_GRANT Processing object type SCHEMA_EXPORT/TABLE/ INDEX/INDEX Processing object type SCHEMA_EXPORT/TABLE/ CONSTRAINT/CONSTRAINT . . exported "<Schema Name>"."<Table Name>" 228.9 MB 496397 rows Master table "SYSTEM". "SYS_EXPORT_SCHEMA _02" successfully loaded/unloaded	

Tarea	Descripción	Habilidades requeridas
	``` ********** ********** ********** ********** **** Dump file set for SYSTEM.SYS_EXPORT_ SCHEMA_02 is: E:\DMSDUMP\EXPORT_ DMS_DATA.DMP Job "SYSTEM"."SYS_EXPO RT_SCHEMA_02" successfully completed at *** *** ** **:**:** **** elapsed 0 00:01:57 ```	

Utilice Oracle Data Pump para importar el EnterpriseOne esquema

Tarea	Descripción	Habilidades requeridas
Transfiera el archivo de volcado a la instancia de destino.	Para transferir sus archivos mediante la utilidad `DBMS_FILE_TRANSFER`, necesita crear un enlace de base de datos desde la base de datos de origen a la instancia de Amazon RDS para Oracle. Una vez establecido el enlace, la utilidad le permitirá transferir los archivos de Data Pump directamente a la instancia de Amazon RDS. Como alternativa, puede transferir los archivos de Data Pump a Amazon Simple Storage Service (Amazon S3)	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	y, a continuación, importarl os a la instancia de Amazon RDS para Oracle. Para más información sobre esta opción, consulte la sección Informaci ón adicional.
	
	Para crear un enlace de base de datos ORARDSDB que conecte con el usuario principal de Amazon RDS en la instancia de base de datos de destino, ejecute los siguientes comandos en la base de datos de origen:
	
	`sqlplus / as sysdba`
	
	`SQL*Plus: Release 19.0.0.0.0 on *** *** ** **:**:** **** Version 19.3.0.0.0`
	
	`Copyright (c) 1982, 2019, Oracle. All rights reserved.`
	
	`Connected to: Oracle Database 19c Standard Edition 2 Release 19.0.0.0.0 Version 19.3.0.0.0`
	
	`SQL> create database link orardsdb connect to admin identifie d by "******" using '(DESCRIPTION = (ADDRESS = (PROTOCOL =`	

Tarea	Descripción	Habilidades requeridas

	`TCP)(HOST = orcl.******.us-east-1.rds.amazonaws.com)(PORT = 1521))(CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = orcl)))';`
	
	`Database link created.`
	
	`SQL>`	

Pruebe el enlace de la base de datos.	Pruebe el enlace a la base de datos para asegurarse de que puede conectarse a la base de datos de destino de Amazon RDS para Oracle usando `sqlplus`.
	
	`SQL> select name from v$database@orardsdb;`
	
	`NAME`
	`---------`
	`ORCL`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

Transfiera el archivo de volcado a la base de datos de destino.	Para copiar el archivo de volcado en la base de datos de Amazon RDS para Oracle, puede utilizar el directorio `DATA_PUMP_DIR` predeterminado o crear su propio directorio mediante el código siguiente, que debe ejecutar en la instancia de Amazon RDS de destino:
	`exec rdsadmin.rdsadmin_util.create_directory(p_directory_name => 'DMS_TARGET_PUMP_DIR');`
	`PL/SQL procedure successfully completed.`
	El siguiente script copia un archivo de volcado denominado `EXPORT_DMS_DATA.DMP` desde la instancia de origen a una base de datos de Amazon RDS para Oracle usando el enlace de la base de datos denominado `orardsdb`. Debe ejecutar el script en la instancia de la base de datos de origen.
	`BEGIN DBMS_FILE_TRANSFER.PUT_FILE(`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	`source_directory_object => 'DMS_DATA_PUMP_DIR', source_file_name => 'EXPORT_DMS_DATA.DMP', destination_directory_object => 'DMS_TARGET_PUMP_DIR', destination_file_name => 'EXPORT_DMS_DATA.DMP', destination_database => 'orardsdb'); END;`
	
	`PL/SQL procedure successfully completed.`	

Incluya el archivo de volcado en la base de datos de destino.	Una vez finalizado el PL/SQL procedimiento, puede incluir el archivo de volcado de datos en la base de datos Amazon RDS for Oracle mediante el siguiente código: `select * from table (rdsadmin.rds_file_util.listdir(p_directory => 'DMS_TARGET_PUMP_DIR'));`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

Cree usuarios específicos de JDE en la instancia de destino.	Cree un perfil y un rol de JD Edwards mediante estos comandos en la instancia de destino:
	`SQL> CREATE PROFILE "JDEPROFILE" LIMIT IDLE_TIME 15;`
	`Profile created.`
	
	`SQL> CREATE ROLE "JDE_ROLE";`
	`Role created.`
	
	`SQL> CREATE ROLE "JDEADMIN";`
	`CREATE ROLE "JDEUSER";`
	`Role created.`
	`Role created.`
	
	Conceda los permisos necesarios al rol:
	`SQL> GRANT CREATE ANY SEQUENCE TO JDE_ROLE;`
	`GRANT DROP ANY SEQUENCE TO JDE_ROLE;`
	`GRANT CREATE ANY TRIGGER TO JDE_ROLE;`
	`GRANT DROP ANY TRIGGER TO JDE_ROLE;`
		Administrador de base de datos, JDE CNC

Tarea	Descripción	Habilidades requeridas

Cree espacios de tabla en la instancia de destino.	Cree los espacios de tabla necesarios en la instancia de destino mediante los siguientes comandos para los esquemas que intervienen en esta migración:
	
	`SQL> CREATE TABLESPACE <Tablespace Name for Tables>;`
	`Tablespace created.`
	
	`SQL> CREATE TABLESPACE <Tablespace Name for Indexes>;`
	`Tablespace created.`
		Administrador de base de datos, JDE CNC

Tarea	Descripción	Habilidades requeridas
Inicie la importación en la base de datos de destino.	Antes de iniciar el proceso de importación, configure los roles, esquemas y espacios de tabla en la base de datos de destino Amazon RDS para Oracle mediante el archivo de volcado de datos. Para realizar la importación, acceda a la base de datos de destino con la cuenta de usuario principal de Amazon RDS y use el nombre de la cadena de conexión del archivo `tnsnames.ora` , que incluye el `tns-entry` de la base de datos Amazon RDS para Oracle. Si es necesario , puede incluir una opción de reasignación para importar el archivo de volcado de datos a un espacio de tabla diferente o con un nombre de esquema diferente. Para iniciar la importación, utilice el siguiente código: `impdp admin@orardsdb directory=DMS_TARG ET_PUMP_DIR logfile=i mport.log dumpfile= EXPORT_DMS_DATA.DMP` Para garantizar una importaci ón correcta, compruebe	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	la ausencia de errores en el archivo de registro de importación y revise detalles como el número de objetos, el número de filas y los objetos no válidos. Si hay algún objeto no válido, repita la compilación. Compare también los objetos de la base de datos de origen y destino para confirmar que coinciden.	

Aprovisione una instancia de replicación de AWS DMS con los puntos de conexión de origen y destino

Tarea	Descripción	Habilidades requeridas
Descargue la plantilla de .	Descargue la plantilla AWS CloudFormation DMS_Instance.yaml para aprovisionar la instancia de replicación de AWS DMS y sus puntos de enlace de origen y destino.	Administrador de la nube, Administrador de bases de datos
Inicie la creación de la pila.	1. Inicie sesión en la consola de administración de AWS y abra la consola de AWS CloudFormation en https://console.aws.amazon.com/cloudformation. 2. Seleccione Creación de pila. 3. En Specify template (Especificar plantilla),	Administrador de la nube, Administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	elija Upload a template file (Cargar un archivo de plantilla). 4. Seleccione Elegir archivo. 5. Seleccione el archivo `DMS_instance.yaml` . 6. Elija Siguiente.	

Tarea	Descripción	Habilidades requeridas
Especifique los parámetros.	1. En Nombre de la pila, introduzca el nombre de la pila. 2. En Parámetros de instancia de AWS DMS, introduzca los siguientes parámetros: • DMSInstanceTipo: elija la instancia requerida para la instancia de replicación de AWS DMS, en función de las necesidades de su empresa. • DMSStorageTamaño: introduzca el tamaño de almacenamiento de la instancia de AWS DMS, en función del tamaño de la migración. 3. En Configuración de la base de datos de Oracle de origen, introduzca los siguientes parámetros: • SourceOracleEndpointID: el nombre del servidor de base de datos Oracle de origen • SourceOracleDatabaseName— El nombre del servicio de base de datos de origen o el ID de sesión (SID), según proceda	Administrador de la nube, Administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	• SourceOracleUserName— El nombre de usuario de la base de datos de origen (el predeterminado `essystem`) • SourceOracleDBPassword— La contraseña del nombre de usuario de la base de datos fuente • SourceOracleDBPort— El puerto de la base de datos de origen 4. Para Configuración de RDS para bases de datos de Oracle, introduzca los siguientes parámetros: • RDSOracleEndpointID de destino: el punto final de la base de datos RDS de destino • Destino RDSOracle DatabaseName: el nombre de la base de datos de RDS de destino • Destino RSOracle UserName: el nombre de usuario del RDS de destino • Destino RDSOracle DBPassword: la contraseña del RDS de destino	

Tarea	Descripción	Habilidades requeridas
	• TargetOracleDBPort— El puerto de la base de datos RDS de destino 5. En Configuración de VPC, subred y grupo de seguridad, introduzca los siguientes parámetros: • VPCID: la VPC de la instancia de replicación • VPCSecurityGroupId— El grupo de seguridad de VPC para la instancia de replicación • DMSSubnet1— La subred de la zona de disponibilidad 1 • DMSSubnet2— La subred de la zona de disponibilidad 2 6. Elija Siguiente.	

Tarea	Descripción	Habilidades requeridas
Cree la pila.	1. En la página Configura r opciones de pila, para Etiquetas, introduzca cualquier valor opcional. 2. Elija Siguiente. 3. En la página Revisar, verifique los detalles y, a continuación, seleccione Enviar. El aprovisionamiento debería completarse en un plazo aproximado de 5 a 10 minutos. Se completa cuando la página de AWS CloudFormation Stacks muestra CREATE_CO MPLETE.	Administrador de la nube, Administrador de bases de datos
Configure los puntos de conexión.	1. Abra la consola de AWS DMS en la https://console.a ws.amazon.com/dms/v2/. 2. En Administración de recursos, elija Instancias de replicación y, a continuac ión, revise las instancias de replicación. 3. En Administración de recursos, elija Puntos de conexión y, a continuac ión, revise los puntos de conexión.	Administrador de la nube, Administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Probar la conectividad.	Cuando los puntos de conexión de origen y destino muestren el estado Activo, pruebe la conectividad. Seleccione Ejecutar prueba en cada punto de conexión (origen y destino) para asegurarse de que el estado sea correcto.	Administrador de la nube, Administrador de bases de datos

Crear una tarea de replicación de AWS DMS para la replicación en vivo

Tarea	Descripción	Habilidades requeridas
Crear una tarea de replicación.	Cree la tarea de replicación de AWS DMS siguiendo estos pasos: 1. Abra la consola de AWS DMS en la https://console.aws.amazon.com/dms/v2/. 2. En el panel de navegación, en Migración de datos, elija Tarea de migración de bases de datos. 3. En el cuadro Configuración de tareas, para Identificador de tareas, introduzca el identificador de su tarea. 4. En Instancia de replicación, elija la instancia de replicación DMS que creó.	Administrador de la nube, Administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	5. En Punto de conexión de base de datos de origen, seleccione el punto de conexión de origen. 6. En Punto de conexión de base de datos de destino, seleccione la base de datos de destino Amazon RDS para Oracle. 7. En Tipo de migración, seleccione Replicar solo cambios de datos. Si recibe un mensaje que le indica que debe activar el registro suplementario, siga las instrucciones de la sección Solución de problemas. 8. En el cuadro Configuración de la tarea, seleccione Especificar el número de secuencia de registro. 9. En Número de cambio del sistema, introduzca el SCN de la base de datos de Oracle que generó en la base de datos de Oracle de origen. 10. Seleccione Activar validación. 11. Elija Habilitar registros. CloudWatch Al activar esta función, puede validar los datos y	

Tarea	Descripción	Habilidades requeridas
	los registros de Amazon para revisar CloudWatch los registros de las instancias de replicación de AWS DMS. 12. En Reglas de selección, complete lo siguiente: • Para Esquema, elija Introducir un esquema. • En el nombre del esquema, introduzca el nombre del esquema de JDE (por ejemplo: DV920). • En Nombre de la tabla, introduzca %. • En Acción, elija Incluir. 13. Seleccione Crear tarea. Tras crear la tarea, AWS DMS migra los cambios en curso a la instancia de base de datos de Amazon RDS para Oracle desde el SCN que proporcionó en el modo de inicio de CDC. También puede verificar la migración revisando los CloudWatch registros.	

Tarea	Descripción	Habilidades requeridas
Repita la tarea de replicación.	Repita los pasos anteriores para crear tareas de replicación para otros esquemas de JD Edwards que formen parte de la migración.	Administrador de la nube, Administrador de bases de datos, administrador de JDE CNC

Valide el esquema de la base de datos de Amazon RDS para Oracle

Tarea	Descripción	Habilidades requeridas
Valide la transferencia de datos.	Una vez iniciada la tarea de AWS DMS, puede consultar la pestaña Estadísticas de tabla en la página Tareas para ver los cambios realizados en los datos. Puede supervisar el estado de la replicación en curso desde la consola, en la página Tareas de migración de bases de datos. Para más información, consulte Validación de datos de AWS DMS	Administrador de la nube, Administrador de bases de datos

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Detención de la replicación.	Interrumpa el procedimiento de replicación y detenga los	Administrador de la nube, Administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	servicios de la aplicación de origen.	
Inicie la aplicación JD Edwards.	Inicie la aplicación de nivel lógico y de presentación JD Edwards de destino en AWS y diríjala a la base de datos Amazon RDS para Oracle. Cuando acceda a la aplicació n, verá que todas las conexiones se establecen ahora con la base de datos Amazon RDS para Oracle.	Administrador de base de datos, administrador de JDE CNC
Desactive la base de datos de origen.	Después de confirmar que no hay más conexiones, puede desactivar la base de datos de origen.	Administrador de base de datos

Resolución de problemas

Problema	Solución

Recibe un mensaje de advertencia para habilitar el registro adicional en la base de datos de origen para una replicación continua	Introduzca estos comandos para habilitar el registro suplementario:
	
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (ALL) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (FOREIGN KEY) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;`

Problema	Solución
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;`
AWS DMS tiene desactivado el registro suplementario.	El registro suplementario se encuentra desactivado de forma predeterminada en AWS DMS. Para activarlo en un punto de conexión de Oracle de origen: 1. Inicie sesión en la consola de administración de AWS y abra la consola de AWS DMS en la https://console.aws.amazon.com/dms/v2/. 2. Elija Puntos de conexión. 3. Elija el punto de conexión de origen de Oracle al que desee agregar el registro complementario. 4. Elija Modificar. 5. Elija Opciones avanzadas y agregue después el código siguiente en el cuadro de texto Atributos de conexión adicionales: `addSupplementalLogging=Y` 6. Elija Modificar.

El registro suplementario no está habilitado en el nivel de CDB.	1. Introduzca este comando:
	`SQL> alter session set container = CDB$ROOT;`
	`Session altered.`
	2. Repita los pasos para activar el registro suplementario.

Problema	Solución
Aparece el siguiente mensaje de error: «Falló el punto final de prueba: estado de la aplicació n: 1020912, mensaje de la aplicación: no es compatible con el entorno PDB de Oracle, no LogMiner se pudo inicializar el punto final».	Si aparece este mensaje de error, puede utilizar Binary Reader en lugar de. LogMiner En Configuración de puntos de conexión, añada esta línea a los atributos de conexión adicionales de la base de datos de origen: `useLogMinerReader=N;useBfile=Y;`

Recursos relacionados

- Introducción a AWS Database Migration Service (AWS DMS)
- Buenas prácticas de AWS Database Migration Service (AWS DMS)
- Migración de bases de datos de Oracle a la nube de AWS
- Referencia de tipo de recurso de AWS Database Migration Service para AWS CloudFormation
- Administre sus credenciales de punto de conexión de AWS DMS con AWS Secrets Manager
- Solución de problemas de las tareas de migración en AWS Database Migration Service (AWS DMS)
- Buenas prácticas de AWS Database Migration Service (AWS DMS)

Información adicional

Cómo transferir archivos con Amazon S3

Para transferir los archivos a Amazon S3, puede utilizar la CLI de AWS o la consola de Amazon S3. Tras transferir los archivos a Amazon S3, puede usar la instancia de Amazon RDS para Oracle para importar los archivos de Data Pump desde Amazon S3.

Si prefiere transferir el archivo de volcado usando la integración de Amazon S3 como método alternativo, siga estos pasos:

1. Cree un bucket de S3.
2. Exporte los datos de la base de datos de origen utilizando Oracle Data Pump.
3. Suba los archivos de Data Pump al bucket de S3.

4. Descargue los archivos de Data Pump desde el bucket de S3 en la base de datos de destino Amazon RDS para Oracle.
5. Realice la importación con los archivos de Data Pump.

> **Note**
>
> Para transferir archivos de datos de gran tamaño entre instancias de RDS y S3, le recomendamos que utilice la característica Aceleración de transferencias de Amazon S3.

Migre una PeopleSoft base de datos de Oracle a AWS mediante AWS DMS

Sampath Kathirvel, Amazon Web Services

Resumen

Oracle PeopleSoft es una solución de planificación de recursos empresariales (ERP) para procesos de toda la empresa. PeopleSoft tiene una arquitectura de tres niveles: cliente, aplicación y base de datos. PeopleSoft se puede ejecutar en Amazon Relational Database Service (Amazon RDS).

Si migra su base de datos de Oracle a Amazon RDS, Amazon Web Services (AWS) podrá encargarse de las tareas de backup y de la alta disponibilidad, lo que le permitirá concentrarse en el mantenimiento de PeopleSoft la aplicación y su funcionalidad. Para obtener una lista completa de los factores clave a tener en cuenta durante el proceso de migración, consulte Estrategias de migración de bases de datos de Oracle en Recomendaciones de AWS.

Este patrón proporciona una solución para migrar sus bases de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump con AWS Database Migration Service (AWS DMS) y su característica de captura de datos de cambios (CDC).

Al migrar aplicaciones ERP críticas, como Oracle PeopleSoft, es fundamental minimizar el tiempo de inactividad. AWS DMS minimiza el tiempo de inactividad gracias a su replicación, tanto continua como de carga completa, desde la base de datos de origen a la base de datos de destino. AWS DMS también proporciona supervisión y registro de la migración en tiempo real, lo que le ayudará a identificar y resolver cualquier problema que pueda provocar un tiempo de inactividad.

Al replicar los cambios con AWS DMS, debe especificar una hora o número de cambio de sistema (SCN) como punto de partida para que AWS DMS lea los cambios de los registros de la base de datos. Es fundamental mantener estos registros accesibles en el servidor durante un determinado período de tiempo para asegurar que AWS DMS tenga acceso a estos cambios.

Requisitos previos y limitaciones

Requisitos previos

- Base de datos Amazon RDS para Oracle aprovisionada en su entorno de nube de AWS como base de datos de destino.
- Una PeopleSoft base de datos de Oracle que se ejecuta en las instalaciones o en Amazon Elastic Compute Cloud (Amazon EC2) en la nube de AWS.

> **Note**
>
> Este patrón está diseñado para migrar de las instalaciones a AWS, pero se probó con Oracle Database en una EC2 instancia de Amazon. Para migrar desde una ubicación en las instalaciones, necesitará configurar la conectividad de red adecuada.

- Detalles del esquema. Al migrar una PeopleSoft aplicación de Oracle a Amazon RDS for Oracle, es necesario identificar qué esquema de base de datos de Oracle (por ejemplo`SYSADM`) se va a migrar. Antes de iniciar el proceso de migración, recopile los siguientes detalles sobre el esquema:
  - Tamaño
  - La cantidad de objetos por tipo de objeto
  - La cantidad de objetos no válidos.

  Esta información ayudará en el proceso de migración.

Limitaciones

- Este escenario se ha probado únicamente con la base de datos PeopleSoft DEMO. No se ha probado con un conjunto de datos grande.

Arquitectura

El siguiente diagrama muestra una instancia que ejecuta una base de datos de Oracle como base de datos de origen y una base de datos Amazon RDS para Oracle como base de datos de destino. Los datos se exportan e importan de la base de datos de Oracle de origen a la base de datos Amazon RDS para Oracle de destino mediante Oracle Data Pump, y los cambios de CDC se replican mediante AWS DMS.

1. El paso inicial consiste en extraer los datos de la base de datos de origen mediante Oracle Data Pump y, a continuación, enviarlos a la base de datos de destino Amazon RDS para Oracle.
2. Los datos se envían desde la base de datos de origen a un punto de conexión de origen en AWS DMS.
3. Desde el punto de conexión de origen, los datos se envían a la instancia de replicación de AWS DMS, donde se realiza la tarea de replicación.

4. Una vez completada la tarea de replicación, los datos se envían al punto de conexión de destino en AWS DMS.
5. Desde el punto de conexión de destino, los datos se envían a la instancia de base de datos Amazon RDS para Oracle.

Tools (Herramientas)

Servicios de AWS

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Amazon Relational Database Service (Amazon RDS) para Oracle le ayuda a configurar, utilizar y escalar una base de datos relacional de Oracle en la nube de AWS.

Otros servicios

- Oracle Data Pump le ayuda a trasladar datos y metadatos de una base de datos a otra a altas velocidades.

Prácticas recomendadas

Migrating LOBs

Si la base de datos de origen contiene objetos binarios de gran tamaño (LOBs) que deben migrarse a la base de datos de destino, AWS DMS ofrece las siguientes opciones:

- Modo LOB completo: AWS DMS migra todas las bases de datos LOBs de origen a la de destino, independientemente de su tamaño. Aunque la migración es más lenta, la ventaja es que los datos no se truncan. Para obtener un mejor rendimiento, puede crear una tarea independiente en la nueva instancia de replicación para migrar las tablas que tengan LOBs más de unos pocos megabytes.
- Modo LOB limitado: usted especifica el tamaño máximo de los datos de la columna LOB, lo que permite a AWS DMS preasignar los recursos y aplicarlos de forma masiva. LOBs Si el tamaño de las columnas LOB supera el tamaño especificado en la tarea, AWS DMS trunca los datos y envía advertencias al archivo de registro de AWS DMS. Puede mejorar el rendimiento usando el modo LOB limitado si el tamaño de los datos de LOB se encuentra dentro del tamaño de LOB limitado.

- Modo LOB en línea: puede migrar LOBs sin truncar los datos ni ralentizar el rendimiento de la tarea al replicar tanto los datos pequeños como los grandes. LOBs En primer lugar, especifique un valor para el InlineLobMaxSize parámetro, que solo estará disponible cuando el modo LOB completo esté establecido en true. La tarea de AWS DMS transfiere lo pequeño LOBs en línea, lo que es más eficiente. A continuación, AWS DMS migra el tamaño grande LOBs realizando una búsqueda en la tabla de origen. Sin embargo, el modo LOB en línea funciona únicamente en la fase de carga completa.

Generación de valores de secuencia

Tenga en cuenta que, durante el proceso de captura de datos de cambios con AWS DMS, los números de secuencia progresivos no se replican desde la base de datos de origen. Para evitar discrepancias en los valores de secuencia, debe generar el valor de secuencia más reciente del origen para todas las secuencias y aplicarlo a la base de datos Amazon RDS para Oracle de destino.

Administración de credenciales

Para ayudar a proteger sus recursos de AWS, le recomendamos seguir las prácticas recomendadas de AWS Identity and Access Management (IAM).

Epics

Aprovisione una instancia de replicación de AWS DMS con los puntos de conexión de origen y destino

Tarea	Descripción	Habilidades requeridas
Descargue la plantilla de .	Descargue la CloudFormation plantilla de AWS DMS_Instance.yaml para aprovisionar la instancia de replicación de AWS DMS y sus puntos de enlace de origen y destino.	Administrador de la nube, Administrador de bases de datos
Inicie la creación de la pila.	1. En la consola de administración de AWS, elija CloudFormation. 2. Seleccione Creación de pila.	Administrador de la nube, Administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	3. En Specify template (Especificar plantilla), elija Upload a template file (Cargar un archivo de plantilla). 4. Seleccione Elegir archivo. 5. Seleccione el archivo `DMS_instance.yaml` . 6. Elija Siguiente.	

Tarea	Descripción	Habilidades requeridas
Especifique los parámetros.	1. En Nombre de la pila, introduzca el nombre de la pila. 2. En Parámetros de instancia de AWS DMS, introduzca los siguientes parámetros: • DMSInstanceTipo: elija la instancia requerida para la instancia de replicación de AWS DMS, en función de las necesidades de su empresa. • DMSStorageTamaño: introduzca el tamaño de almacenamiento de la instancia de AWS DMS, en función del tamaño de la migración. 3. En Configuración de la base de datos de Oracle de origen, introduzca los siguientes parámetros: • SourceOracleEndpointID: el nombre del servidor de base de datos Oracle de origen • SourceOracleDatabaseName— El nombre del servicio de base de datos de origen o el ID de sesión (SID), según proceda	Administrador de la nube, Administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	• SourceOracleUserName— El nombre de usuario de la base de datos de origen (el predeterminado es sistema) • SourceOracleDBPassword— La contraseña del nombre de usuario de la base de datos fuente • SourceOracleDBPort— El puerto de la base de datos de origen 4. En Configuración de RDS para bases de datos de Oracle, introduzca los siguientes parámetros: • RDSOracleEndpointID de destino: el punto final de la base de datos RDS de destino • Destino RDSOracle DatabaseName: el nombre de la base de datos de RDS de destino • Destino RSOracle UserName: el nombre de usuario del RDS de destino • Destino RDSOracle DBPassword: la contraseña del RDS de destino	

Tarea	Descripción	Habilidades requeridas
	• TargetOracleDBPort— El puerto de la base de datos RDS de destino 5. En Configuración de VPC, subred y grupo de seguridad, introduzca los siguientes parámetros: • VPCID: la VPC de la instancia de replicación • VPCSecurityGroupId— El grupo de seguridad de VPC para la instancia de replicación • DMSSubnet1— La subred de la zona de disponibilidad 1 • DMSSubnet2— La subred de la zona de disponibilidad 2 6. Elija Siguiente.	

Tarea	Descripción	Habilidades requeridas
Cree la pila.	1. En la página Configura r opciones de pila, para Etiquetas, introduzca cualquier valor opcional. 2. Elija Siguiente. 3. En la página Revisar, verifique los detalles y, a continuación, seleccione Enviar. El aprovisionamiento debería completarse en un plazo aproximado de 5 a 10 minutos. Se completa cuando la página de AWS CloudFormation Stacks muestra CREATE_CO MPLETE.	Administrador de la nube, Administrador de bases de datos
Configure los puntos de conexión.	1. En la consola de administr ación de AWS, elija Database Migration Services. 2. En Administración de recursos, elija Instancias de replicación. 3. En Administración de recursos, elija Puntos de conexión.	Administrador de la nube, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Probar la conectividad.	Cuando los puntos de conexión de origen y destino muestren el estado Activo, pruebe la conectividad. Seleccione Ejecutar prueba en cada punto de conexión (origen y destino) para asegurarse de que el estado sea correcto.	Administrador de la nube, Administrador de bases de datos

Exporte el PeopleSoft esquema de la base de datos Oracle local mediante Oracle Data Pump

Tarea	Descripción	Habilidades requeridas
Genere el SCN.	Cuando la base de datos de origen esté activa y la aplicación la utilice, inicie la exportación de datos con Oracle Data Pump. En primer lugar, debe generar un número de cambio del sistema (SCN) de la base de datos de origen para garantizar la coherencia de datos durante la exportación con Oracle Data Pump. También servirá como punto de partida para la captura de datos de cambios en AWS DMS. Para generar el SCN actual de la base de datos de origen, introduzca la siguiente instrucción SQL.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	`SQL> select name from v $database;`
	`SQL> select name from v $database;`
	`NAME`
	`---------`
	`PSFTDMO`
	`SQL> SELECT current_s cn FROM v$database;`
	`CURRENT_SCN`
	`-----------`
	`23792008`
	
	Guarde el SCN generado. Lo usará para exportar los datos y crear la tarea de replicación de AWS DMS.	

Tarea	Descripción	Habilidades requeridas

Cree el archivo de parámetros.	Para crear un archivo de parámetros para exportar el esquema, puede usar el siguiente código.
	`$ cat exp_datapmp.par`
	`userid=system/*******`
	`directory=DATA_PUMP_DIR`
	`logfile=export_dms_sample_user.log`
	`dumpfile=export_dms_sample_data_%U.dmp`
	`schemas=SYSADM`
	`flashback_scn=23792008`
	Note
	También puede definir su propio `DATA_PUMP_DIR` mediante los siguientes comandos, en función de sus necesidades.
	`SQL> CREATE OR REPLACE DIRECTORY DATA_PUMP_DIR AS '/opt/oracle/product/19c/dbhome_1/dmsdump/';`
	`Directory created.`
	`SQL> GRANT READ, WRITE ON DIRECTORY DATA_PUMP_DIR TO system;`
	`Grant succeeded.`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	SQL> SQL> SELECT owner, directory_name, directory_path FROM dba_directories WHERE directory_name='DA TA_PUMP_DIR'; OWNER DIRECTORY_NAME DIRECTORY_PATH ---------- ---------- ---------- ---------- ---------- ---------- SYS DATA_PUMP_DIR /opt/ oracle/product/19c/dbh ome_1/dmsdump/	

Tarea	Descripción	Habilidades requeridas
Exporte el esquema.	Realice la exportación con la utilidad `expdp`. `$ expdp parfile=e xp_datapmp.par .... Transferring the dump file with DBMS_FILE _TRANSFER to Target: . . exported "SYSADM". "PS_XML_TEMPLT_LNG" 6.320 KB 0 rows . . exported "SYSADM". "PS_XML_TEMPLT_LNK" 6.328 KB 0 rows . . exported "SYSADM". "PS_XML_XLATDEF_LNG" 6.320 KB 0 rows . . exported "SYSADM". "PS_XML_XLATITM_LNG" 7.171 KB 0 rows . . exported "SYSADM". "PS_XPQRYRUNCNTL" 7.601 KB 0 rows . . exported "SYSADM". "PS_XPQRYRUNPARM" 7.210 KB 0 rows . . exported "SYSADM". "PS_YE_AMOUNTS" 9.351 KB 0 rows . . exported "SYSADM". "PS_YE_DATA" 16.58 KB 0 rows . . exported "SYSADM". "PS_YE_EE" 6.75 KB 0 rows . . exported "SYSADM". "PS_YE_W2CP_AMOUNTS" 9.414 KB 0 rows`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	. . exported "SYSADM". "PS_YE_W2CP_DATA" 20.94 KB 0 rows . . exported "SYSADM". "PS_YE_W2C_AMOUNTS" 10.27 KB 0 rows . . exported "SYSADM". "PS_YE_W2C_DATA" 20.95 KB 0 rows . . exported "SYSADM". "PS_ZBD_JOBCODE_TBL" 14.60 KB 0 rows . . exported "SYSADM". "PTGRANTTBL" 5.468 KB 0 rows Master table "SYSTEM". "SYS_EXPORT_SCHEMA _01" successfully loaded/unloaded ** Dump file set for SYSTEM.SYS_EXPORT_ SCHEMA_01 is: /opt/oracle/pr oduct/19c/dbhome_1 /dmsdump/export_dm s_sample_data_01.dmp Job "SYSTEM"."SYS_EXPO RT_SCHEMA_01" successfully completed at Mon Dec 19 20:13:57 2022 elapsed 0 00:38:22	

Importe el PeopleSoft esquema a la base de datos Amazon RDS for Oracle mediante Oracle Data Pump

Tarea	Descripción	Habilidades requeridas
Transfiera el archivo de volcado a la instancia de destino.	Para transferir sus archivos mediante `DBMS_FILE_TRANSFER`, debe crear un enlace de base de datos desde la base de datos de origen a la instancia de Amazon RDS para Oracle. Una vez establecido el enlace, la utilidad le permitirá transferir los archivos de Data Pump directamente a la instancia de RDS. Como alternativa, puede transferir los archivos de Data Pump a Amazon Simple Storage Service (Amazon S3) y, a continuación, importarlos a la instancia de Amazon RDS para Oracle. Para más información sobre esta opción, consulte la sección Información adicional. Para crear un enlace de base de datos `ORARDSDB` que conecte con el usuario principal de Amazon RDS en la instancia de base de datos de destino, ejecute los siguientes comandos en la base de datos de origen.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	`$sqlplus / as sysdba`
	`$ SQL> create database link orardsdb connect to admin identified by "*****" using '(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = testpsft.*******.us-west-2.rds.amazonaws.com)(PORT = 1521))(CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = orcl)))';`
	`Database link created.`	

Pruebe el enlace de la base de datos.	Pruebe el enlace de la base de datos para asegurarse de que puede conectarse mediante sqlplus a la base de datos de destino de Amazon RDS para Oracle.
	`SQL>`
	`SQL> select name from v$database@orardsdb;`
	`NAME`
	`---------`
	`ORCL`
	`SQL>`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

Transfiera el archivo de volcado a la base de datos de destino.	Para copiar el archivo de volcado a la base de datos de Amazon RDS para Oracle, puede usar el directorio predeterminado `DATA_PUMP_DIR` o bien crear su propio directorio con el siguiente código.
	`exec rdsadmin.rdsadmin_util.create_directory(p_directory_name => 'TARGET_PUMP_DIR') ;`
	El siguiente script copia un archivo de volcado denominado `export_dms_sample_data_01.dmp` desde la instancia de origen a una base de datos de Amazon RDS para Oracle usando el enlace de la base de datos denominado `orardsdb`.
	`$ sqlplus / as sysdba SQL> BEGIN DBMS_FILE_TRANSFER .PUT_FILE( source_directory_object => 'DATA_PUMP_DIR', source_file_name => 'export_dms_sample_data_01.dmp',`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`destination_directory _object => 'TARGET_P UMP_DIR'', destination_file_name => 'export_dms_sample _data_01.dmp', destination_database => 'orardsdb' ); END; / PL/SQL procedure successfully completed .`	
Incluya el archivo de volcado en la base de datos de destino.	Una vez finalizado el PL/SQL procedimiento, puede incluir el archivo de volcado de datos en la base de datos Amazon RDS for Oracle mediante el siguiente código. `SQL> select * from table (rdsadmin.rds_file _util.listdir(p_di rectory => 'TARGET_P UMP_DIR'));`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Inicie la importación en la base de datos de destino.	Antes de iniciar el proceso de importación, configure los roles, esquemas y espacios de tabla en la base de datos de destino Amazon RDS para Oracle mediante el archivo de volcado de datos. Para realizar la importación, acceda a la base de datos de destino con la cuenta de usuario maestra de Amazon RDS y use el nombre de la cadena de conexión del archivo `tnsnames.ora` , que incluye el `tns-entry` de la base de datos Amazon RDS para Oracle. Si es necesario , puede incluir una opción de reasignación para importar el archivo de volcado de datos a un espacio de tabla diferente o con un nombre de esquema diferente. Para iniciar la importación, utilice el siguiente código. `impdp admin@orardsdb directory=TARGET_PUMP_DIR logfile=import.log dumpfile=export_dms_sample_data_01.dmp`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Para garantizar una importación correcta, compruebe la ausencia de errores en el archivo de registro de importación y revise detalles como el número de objetos, el número de filas y los objetos no válidos. Si hay algún objeto no válido, repita la compilación. Compare también los objetos de la base de datos de origen y destino para confirmar que coinciden.	

Cree una tarea de replicación de AWS DMS usando CDC para realizar la replicación en vivo

Tarea	Descripción	Habilidades requeridas
Crear una tarea de replicación.	Cree la tarea de replicación de AWS DMS siguiendo estos pasos: 1. En la consola de AWS DMS, en Conversión y migración, seleccione Tarea de migración de base de datos. 2. En Configuración de tareas, en Identificador de tareas, introduzca su identificador de tarea. 3. En Instancia de replicación, elija la instancia de replicación DMS que creó.	Administrador de la nube, Administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	4. En Punto de conexión de base de datos de origen, seleccione el punto de conexión de origen. 5. En Punto de conexión de base de datos de destino, seleccione la base de datos de destino Amazon RDS para Oracle. 6. En Tipo de migración, seleccione Replicar solo cambios de datos. Si recibe un mensaje en el que se indica que es necesario activar el registro adicional , siga las instrucciones de la sección Información adicional. 7. En Configuración de tarea, seleccione Especificar número de secuencia de registro. 8. En Número de cambio del sistema, introduzca el SCN de la base de datos de Oracle que generó en la base de datos de Oracle de origen. 9. Seleccione Activar validació n. 10. Seleccione Activar registros . CloudWatch	

Tarea	Descripción	Habilidades requeridas
	Al activar esta función, puede validar los datos y los registros de Amazon para revisar CloudWatch los registros de las instancias de replicación de AWS DMS. 11. En Reglas de selección, complete lo siguiente: • Para Esquema, elija Introducir un esquema. • En Nombre del esquema, introduzca SYSADM. • En Nombre de la tabla, introduzca %. • En Acción, elija Incluir. 12. En Reglas de transformación, complete lo siguiente: • En Destino, elija Tabla. • Para Nombre de esquema, elija Introducir un esquema. • En Nombre del esquema, introduzca SYSADM. • En Acción, seleccione Cambiar nombre a. 13. Seleccione Crear tarea. Tras crear la tarea, se migra el CDC a la instancia de base de datos Amazon RDS para	

Tarea	Descripción	Habilidades requeridas
	Oracle desde el SCN que proporcionó en el modo de inicio de CDC. También puede verificarlos revisando los CloudWatch registros.	

Valide el esquema de la base de datos de Amazon RDS para Oracle

Tarea	Descripción	Habilidades requeridas
Valide la transferencia de datos.	Una vez iniciada la tarea de AWS DMS, puede consultar la pestaña Estadísticas de tabla en la página Tareas para ver los cambios realizados en los datos. Puede supervisar el estado de la replicación en curso desde la consola, en la página Tareas de migración de bases de datos. Para más información, consulte Validación de datos de AWS DMS	Administrador de la nube, Administrador de bases de datos

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Detención de la replicación.	Interrumpa el procedimiento de replicación y detenga los	Administrador de la nube, Administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	servicios de la aplicación de origen.	
Lanza el nivel PeopleSoft medio.	Lance la aplicación de nivel PeopleSoft medio de destino en AWS y diríjala a la base de datos Amazon RDS for Oracle migrada recientemente. Cuando acceda a la aplicación, verá que todas las conexiones de la aplicación se establecen ahora con la base de datos Amazon RDS para Oracle.	DBA, administrador PeopleSoft
Desactive la base de datos de origen.	Tras haber confirmado que no hay más conexiones a la base de datos de origen, puede desactivarla.	Administrador de base de datos

Recursos relacionados

- Introducción a AWS Database Migration Service (AWS DMS)
- Buenas prácticas de AWS Database Migration Service (AWS DMS)
- Migración de bases de datos de Oracle a la nube de AWS

Información adicional

Cómo transferir archivos con Amazon S3

Para transferir los archivos a Amazon S3, puede utilizar la CLI de AWS o la consola de Amazon S3. Tras transferir los archivos a Amazon S3, puede usar la instancia de Amazon RDS para Oracle para importar los archivos de Data Pump desde Amazon S3.

Si prefiere transferir el archivo de volcado usando la integración de Amazon S3 como método alternativo, siga estos pasos:

1. Cree un bucket de S3.
2. Exporte los datos de la base de datos de origen utilizando Oracle Data Pump.
3. Suba los archivos de Data Pump al bucket de S3.
4. Descargue los archivos de Data Pump desde el bucket de S3 en la base de datos de destino Amazon RDS para Oracle.
5. Realice la importación con los archivos de Data Pump.

> **Note**
>
> Para transferir archivos de datos de gran tamaño entre instancias de RDS y S3, se recomienda usar la característica Aceleración de transferencias de Amazon S3.

Active el registro adicional

Si recibe un mensaje de advertencia solicitando habilitar el registro adicional en la base de datos de origen para la replicación continua, siga estos pasos.

```
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (ALL) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (FOREIGN KEY) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;
```

Migración de una base de datos MySQL en las instalaciones a Amazon RDS para MySQL

Lorenzo Mota, Amazon Web Services

Resumen

Este patrón proporciona una guía para migrar una base de datos MySQL en las instalaciones a Amazon Relational Database Service (Amazon RDS) para MySQL. El patrón analiza el uso de AWS Database Migration Service (AWS DMS) o herramientas nativas de MySQL, como mysqldump, para una migración completa de bases de datos. Este patrón es principalmente para DBAs arquitectos de soluciones. Se puede usar en proyectos pequeños o grandes como un procedimiento de prueba (recomendamos al menos un ciclo de prueba) o como procedimiento de migración definitiva.

Requisitos previos y limitaciones

Requisitos previos

- Una AWS cuenta activa
- Una base de datos MySQL de origen en un centro de datos en las instalaciones

Limitaciones

- Límite de tamaño de la base de datos: 64 TB

Versiones de producto

- Versiones de MySQL 5.5, 5.6, 5.7, 8.0. Para ver la lista más reciente de versiones compatibles, consulte MySQL en Amazon RDS en la AWS documentación. Si está utilizando AWS DMS, consulte también Uso de una base de datos compatible con MySQL como destino para las versiones de AWS DMS MySQL compatibles actualmente con. AWS DMS

Arquitectura

Pila de tecnología de origen

- Una base de datos MySQL en las instalaciones

Pila de tecnología de destino

- Una instancia de base de datos de Amazon RDS que ejecute MySQL

Arquitectura de destino

En el diagrama siguiente se muestra la implementación de Amazon RDS para MySQL en el destino tras la migración.

AWS arquitectura de migración de datos

Uso de AWS DMS:

El siguiente diagrama muestra la arquitectura de migración de datos cuando se utiliza AWS DMS para enviar cambios completos e incrementales hasta la transición. La conexión de red local a otra AWS depende de sus requisitos y está fuera del alcance de este patrón.

Uso de herramientas MySQL nativas:

El diagrama siguiente muestra la arquitectura de migración de datos cuando se utilizan herramientas nativas de MySQL. Los archivos volcados de exportación se copian a Amazon Simple Storage Service (Amazon S3) y se importan a la base de datos Amazon RDS for MySQL antes de la transición. AWS La conexión de red local a otra AWS depende de sus requisitos y está fuera del alcance de este patrón.

Notas:

- Según los requisitos de tiempo de inactividad y el tamaño de la base de datos, el uso de una herramienta de captura de datos modificados (CDC) AWS DMS o una herramienta de captura de datos modificados (CDC) minimiza el tiempo de transición. AWS DMS puede ayudar a reducir al mínimo el tiempo de transición al nuevo objetivo (normalmente en minutos). Una estrategia offline con mysqldump puede ser suficiente si el tamaño de la base de datos y la latencia de la red permiten un período corto. (Recomendamos efectuar pruebas para obtener un tiempo aproximado).
- Por lo general, una estrategia de los CDC AWS DMS requiere más supervisión y complejidad que las opciones fuera de línea.

Tools (Herramientas)

- Servicios de AWS: AWS Database Migration Service (AWS DMS) le ayuda a migrar los almacenes de datos a una combinación de configuraciones en la nube y locales Nube de AWS o entre ellas. Para obtener información sobre las bases de datos de origen y destino de MySQL compatibles con AWS DMS, consulte Migración de bases de datos compatibles con MySQL a. AWS Si su base de datos de origen no es compatible con AWS DMS, debe elegir otro método para migrar los datos.
- Herramientas de MySQL nativas: mysqldump
- Herramientas de terceros: Percona XtraBackup

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos.	Valide las versiones de las bases de datos de origen y de destino.	Administrador de base de datos
Identifique los requisitos de hardware.	Identifique los requisitos de hardware del servidor de destino.	Administrador de base de datos, administrador de sistemas
Identifique los requisitos de almacenamiento.	Identifique los requisitos de almacenamiento (como el tipo y la capacidad de almacenamiento) de la base de datos de destino.	Administrador de base de datos, administrador de sistemas
Seleccione el tipo de instancia.	Seleccione el tipo de instancia de destino en función de la capacidad, las características de almacenamiento y las características de red.	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Identifique los requisitos de acceso a la red.	Identifique requisitos de seguridad para acceder a la red de las bases de datos de origen y destino.	Administrador de base de datos, administrador de sistemas
Identifique los objetos no compatibles.	Identifique los objetos no compatibles (si los hay) y determine el esfuerzo de migración.	Administrador de base de datos
Identifique las dependencias.	Identifique cualquier dependencia en las bases de datos remotas.	Administrador de base de datos
Determine la estrategia de migración de la aplicación.	Determine la estrategia para migrar las aplicaciones cliente.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).	Configure las tablas de enrutamiento, las puertas de enlace de Internet, las puertas de enlace NAT y las subredes. Para obtener más informaci ón, consulte VPCs Amazon RDS en la documentación de Amazon RDS.	Administrador de sistemas
Cree grupos de seguridad.	Configure puertos y rangos de CIDR o específicos en IPs función de sus requisito	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	s. El puerto predeterminado para MySQL es el 3306. Para obtener más información, consulte Controlling access with security groups (Control de acceso con grupos de seguridad) en la documentación de Amazon RDS.	
Configure e inicie una instancia de base de datos de Amazon RDS para MySQL.	Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS en la documentación de Amazon RDS. Compruebe si hay versiones compatibles.	Administrador de sistemas

Migración de datos: opción 1 (con herramientas nativas)

Tarea	Descripción	Habilidades requeridas
Utilice las herramientas nativas de MySQL o herramientas de terceros para migrar los objetos y datos de la base de datos.	Para obtener instrucciones, consulte la documentación de las herramientas de MySQL, como mysqldump y Percona XtraBackup (para la migración física). Para obtener más información sobre las opciones, consulte la entrada del blog Opciones de migración de MySQL a Amazon RDS para MySQL o Amazon Aurora MySQL.	Administrador de base de datos

Migrar datos: opción 2 (usar) AWS DMS

Tarea	Descripción	Habilidades requeridas
Migre datos con AWS DMS.	Para obtener instrucciones, consulte la documentación de AWS DMS.	Administrador de base de datos

Llevar a cabo las tareas preliminares antes de la transición

Tarea	Descripción	Habilidades requeridas
Corrija cualquier discrepancia en el recuento de objetos.	Recopile los recuentos de objetos de la base de datos de origen y de la nueva base de datos de destino. Corrija cualquier discrepancia en la base de datos objetivo.	Administrador de base de datos
Compruebe las dependencias.	Compruebe si las dependenc ias (los enlaces) con destino y origen en otras bases de datos son válidas y funcionan según lo previsto.	Administrador de base de datos
Efectúe pruebas.	Si se trata de un ciclo de pruebas, lleve a cabo pruebas de consulta, recopile métricas y solucione los problemas.	Administrador de base de datos

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Cambie a la base de datos de destino.	Cambie las aplicaciones cliente a la nueva infraestr uctura.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Proporcione soporte para las pruebas.	Proporcione soporte para las pruebas de aplicaciones funcionales.	Administrador de base de datos

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cierre los recursos.	Cierre los AWS recursos temporales que creó para la migración.	Administrador de base de datos, administrador de sistemas
Valide los documentos del proyecto.	Revise y valide los documento s del proyecto.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Recopile métricas.	Recopile métricas como el tiempo de migración, el porcentaje de esfuerzo manual en comparación con el automatizado, el ahorro de costos, etc.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Cerrar el proyecto.	Cerrar el proyecto y enviar comentarios.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Reitre de servicio la base de datos de origen.	Una vez completadas todas las tareas de migración y transición, retire la base de datos en las instalaciones.	Administrador de base de datos, administrador de sistemas

Recursos relacionados

Referencias

- Estrategia de migración para bases de datos relacionales
- AWS DMS sitio web
- AWS DMS documentación
- Documentación de Amazon RDS
- Precios de Amazon RDS
- Amazon VPC y Amazon RDS
- Implementaciones de Amazon RDS Multi-AZ
- Migre bases de datos MySQL locales a Aurora MySQL mediante Percona, XtraBackup Amazon EFS y Amazon S3
- Almacenamiento de instancias de base de datos de Amazon RDS

Tutoriales

- Cómo empezar con AWS DMS
- Introducción a Amazon RDS

Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server

Henrique Lobao, Jonathan Pereira Cruz y Vishal Singh, Amazon Web Services

Resumen

Este patrón proporciona una guía para migrar una base de datos de Microsoft SQL Server en las instalaciones a Amazon Relational Database Service (Amazon RDS) para SQL Server. Describe dos opciones de migración: utilizar AWS Data Migration Service (AWS DMS) o utilizar herramientas nativas de Microsoft SQL Server como Copy Database Wizard.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de origen Microsoft SQL Server en un centro de datos en las instalaciones

Limitaciones

- Límite de tamaño de la base de datos: 16 TB

Versiones de producto

- Para ver la lista actualizada de versiones y características compatibles, consulte Microsoft SQL Server en Amazon RDS en la documentación de AWS. Si utiliza AWS DMS, consulte también Uso de una base de datos de Microsoft SQL Server como destino para AWS DMS para conocer las versiones de SQL Server compatibles con AWS DMS.

Arquitectura

Pila de tecnología de origen

- Base de datos de Microsoft SQL Server en las instalaciones

Pila de tecnología de destino

- Instancia de base de datos de Amazon RDS para SQL Server

Arquitectura de origen y destino

Uso de AWS DMS:

Uso de herramientas nativas de SQL Server:

Tools (Herramientas)

- AWS DMS admite varios tipos de bases de datos de origen y destino. Para obtener más información, consulte los Step-by-Steptutoriales de AWS DMS. Si AWS DMS no es compatible con la base de datos de origen, seleccione otro método para migrar los datos.
- Las Herramientas nativas de Microsoft SQL Server incluyen copia de seguridad y restauración, Copy Database Wizard y la función de copiar y adjuntar bases de datos.

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Valide la versión y el motor de la base de datos de origen y de destino.		Administrador de base de datos
Identifique los requisitos de hardware de la instancia del servidor de destino.		Administrador de base de datos, administrador de sistemas
Identifique los requisitos de almacenamiento (el tipo y la capacidad de almacenam iento).		Administrador de base de datos, administrador de sistemas
Elija el tipo de instancia adecuado en función de la capacidad, las características		Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
de almacenamiento y las características de red.		
Identificar los requisitos de seguridad del acceso a la red para las bases de datos de origen y destino.		Administrador de base de datos, administrador de sistemas
Identificar la estrategia de migración de aplicaciones.		Administrador de base de datos, administrador de sistemas

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).		Administrador de sistemas
Cree grupos de seguridad.		Administrador de sistemas
Configure e inicie una instancia de base de datos de Amazon RDS.		Administrador de base de datos, administrador de sistemas

Migración de datos: opción 1

Tarea	Descripción	Habilidades requeridas
Utilice las herramientas nativas de SQL Server o herramientas de terceros para migrar los objetos y datos de la base de datos.		Administrador de base de datos

Migración de datos: opción 2

Tarea	Descripción	Habilidades requeridas
Migre datos con AWS DMS.		Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de migración de aplicaciones.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Cambie los clientes de la aplicación a la nueva infraestructura.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.		Administrador de base de datos, administrador de sistemas
Revise y valide los documentos del proyecto.		Administrador de base de datos, propietario de la

Tarea	Descripción	Habilidades requeridas
		aplicación, administrador de sistemas
Recopile métricas como el tiempo de migración, el porcentaje de esfuerzo manual en comparación con el automatizado y el ahorro de costos.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Cerrar el proyecto y enviar comentarios.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Recursos relacionados

Referencias

- Implementación de Microsoft SQL Server en Amazon Web Services
- Sitio web de AWS DMS
- Precios de Amazon RDS
- Productos de Microsoft en AWS
- Licencias de Microsoft en AWS
- Microsoft SQL Server en AWS
- Uso de la autenticación de Windows con una instancia de base de datos de Microsoft SQL Server
- Implementaciones Multi-AZ de Amazon RDS

Tutoriales y videos

- Introducción a AWS DMS
- Introducción a Amazon RDS
- AWS DMS (video)

- Amazon RDS (video)

Migración de datos de Microsoft Azure Blob a Amazon S3 mediante Rclone

Suhas Basavaraj, Aidan Keane y Corey Lane, Amazon Web Services

Resumen

Este patrón describe cómo usar Rclone para migrar datos del almacenamiento de objetos Blob de Microsoft Azure a un bucket de Amazon Simple Storage Service (Amazon S3). Puede usar este patrón para realizar una migración única o una sincronización continua de los datos. Rclone es un programa de línea de comandos escrito en Go. Se usa para mover datos a través de diversas tecnologías de almacenamiento de los proveedores de la nube.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Datos almacenados en el servicio de contenedor Blob de Azure

Arquitectura

Pila de tecnología de origen

- Contenedor de almacenamiento Blob de Azure

Pila de tecnología de destino

- Bucket de Amazon S3
- Instancia Linux de Amazon Elastic Compute Cloud (Amazon EC2)

Arquitectura

Tools (Herramientas)

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Rclone es un programa de línea de comandos de código abierto inspirado en rsync. Se usa para administrar archivos en numerosas plataformas de almacenamiento en la nube.

Prácticas recomendadas

Al migrar datos de Azure a Amazon S3, tenga en cuenta estas consideraciones para evitar costos innecesarios o lentitud en la velocidad de transferencia:

- Cree su infraestructura de AWS en la misma región geográfica que la cuenta de almacenamiento de Azure y el contenedor Blob, por ejemplo, en la región de AWS `us-east-1` (Virginia del Norte) y la región de Azure `East US`.
- Evite usar puerta de enlace NAT si es posible, ya que genera tarifas de transferencia de datos tanto para el ancho de banda de entrada como para el de salida.
- Use un punto de conexión de puerta de enlace VPC para Amazon S3 a fin de aumentar el rendimiento.
- Considere la posibilidad de utilizar una EC2 instancia basada en el procesador AWS Graviton2 (ARM) para reducir el coste y aumentar el rendimiento en comparación con las instancias x86 de Intel. Rclone presenta compilación cruzada y proporciona un binario ARM precompilado.

Epics

Prepare los recursos en la nube de AWS y Azure

Tarea	Descripción	Habilidades requeridas
Prepare un bucket de S3 de destino.	Cree un nuevo bucket de S3 en la región de AWS correspondiente, o bien elija un bucket existente como destino de los datos que desee migrar.	Administrador de AWS
Crea un rol de instancia de IAM para Amazon EC2.	Cree un nuevo rol de AWS Identity and Access Management (IAM) para Amazon EC2. Esta función le da a la EC2 instancia acceso de escritura al bucket S3 de destino.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Adjunte una política al rol de la instancia de IAM.	Utilice la consola de IAM o la interfaz de línea de comandos de AWS (AWS CLI) para crear una política en línea para EC2 el rol de instancia que permita permisos de acceso de escritura al bucket de S3 de destino. Para un ejemplo de política, consulte la sección Información adicional.	Administrador de AWS
Lance una instancia EC2 .	Lance una EC2 instancia de Amazon Linux configurada para usar el rol de servicio de IAM recién creado. Esta instancia también necesitar á acceder a los puntos de conexión de la API pública de Azure a través de Internet. **Note** Considere usar EC2 instancias basadas en AWS Graviton para reducir los costos. Rclone proporciona binarios compilados en ARM.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Cree una entidad principal de servicio de Azure AD.	Use la CLI de Azure para crear una entidad principal de servicio de Azure Active Directory (Azure AD) con acceso de solo lectura al contenedor de almacenamiento Blob de Azure de origen. Para obtener instrucciones, consulte la sección Información adicional. Guarde estas credenciales en la EC2 instancia en la ubicación. `~/azure-principal.json`	Administrador de la nube, Azure

Instalar y configurar Rclone

Tarea	Descripción	Habilidades requeridas
Descargar e instalar Rclone.	Descargue e instale el programa de línea de comandos Rclone. Para instrucciones sobre la instalación, consulte la documentación de instalación de Rclone.	AWS general, administrador de la nube
Configure Rclone.	Copie el siguiente archivo de ejemplo `rclone.conf` . Sustituya `AZStorageAccount` por el nombre de su cuenta de Azure Storage y `us-east-1` por la región de AWS en la que se encuentra su bucket de S3. Guarda este archivo en la ubicación	AWS general, administrador de la nube

Tarea	Descripción	Habilidades requeridas

	`~/.config/rclone/rclone.conf` de la EC2 instancia.
	
	`[AZStorageAccount]`
	`type = azureblob`
	`account = AZStorageAccount`
	`service_principal_file = azure-principal.json`
	
	`[s3]`
	`type = s3`
	`provider = AWS`
	`env_auth = true`
	`region = us-east-1`	

Tarea	Descripción	Habilidades requeridas

Verifique la configuración de Rclone.	Para confirmar que Rclone está configurado y que los permisos funcionan correctamente, compruebe que Rclone puede analizar el archivo de configuración y que los objetos del contenedor Blob de Azure y del bucket de S3 sean accesibles. Consulte a continuación algunos ejemplos de comandos de validación.
	• Enumere los controles remotos configurados en el archivo de configuración. Esto garantizará que el archivo de configuración se esté analizando correctamente. Revise el resultado para asegurarse de que coincide con su archivo `rclone.conf` .
	`rclone listremotes`
	`AZStorageAccount:`
	`s3:`
	• Enumere los contenedores Blob de Azure en la cuenta configurada. Sustituya `AZStorageAccount` por el nombre de la cuenta de almacenamiento que ha usado en el archivo `rclone.conf` .
		AWS general, administrador de la nube

Tarea	Descripción	Habilidades requeridas

	<pre>rclone lsd AZStorage Account:
	2020-04-29 08:29:26 docs</pre>
	• Enumere los archivos del contenedor Blob de Azure. Sustituya los documento s de este comando por un nombre de contenedor de Blob real en su cuenta de almacenamiento de Azure.
	<pre>rclone ls AZStorage Account:docs
	824884 administr ator-en.a4.pdf</pre>
	• Enumere los buckets en su cuenta de AWS.
	<pre>[root@ip-10-0-20-157 ~]# rclone lsd s3:
	2022-03-07 01:44:40 amzn-s3-demo-bucket1
	2022-03-07 01:45:16 amzn-s3-demo-bucket2
	2022-03-07 02:12:07 amzn-s3-demo-bucket3</pre>
	• Enumere los archivos en el bucket de S3.
	<pre>[root@ip-10-0-20-1 57 ~]# rclone ls</pre>	

Tarea	Descripción	Habilidades requeridas
	s3:amzn-s3-demo-bucket1 template0.yaml template1.yaml	

Migración de datos con Rclone

Tarea	Descripción	Habilidades requeridas

Migre los datos de sus contenedores.	Ejecute los comandos de Rclone copy o sync.
	
	Ejemplo: copy
	
	Este comando copia datos del contenedor Blob de Azure de origen al bucket de S3 de destino.
	
	`rclone copy AZStorageAccount:blob-container s3:amzn-s3-demo-bucket1`
	
	Ejemplo: sync
	
	Este comando sincroniza los datos entre el contenedor Blob de Azure de origen y el bucket de S3 de destino.
	
	`rclone sync AZStorageAccount:blob-container s3:amzn-s3-demo-bucket1`
		AWS general, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	Important Al usar el comando sync, los datos que no estén en el contenedor de origen se eliminará n del bucket de S3 de destino.	
Sincronice sus contenedores.	Una vez completada la copia inicial, ejecute el comando de Rclone sync para continuar con la migración. Solo se copiarán los archivos nuevos que no estén ya en el bucket de S3 de destino.	AWS general, administrador de la nube
Compruebe que los datos se hayan migrado correctamente.	Para comprobar que los datos se han copiado correctamente en el bucket de S3 de destino, ejecute los comandos lsd y ls de Rclone.	AWS general, administrador de la nube

Recursos relacionados

- Guía del usuario de Amazon S3 (documentación de AWS)
- Funciones de IAM para Amazon EC2 (documentación de AWS)
- Creación de un contenedor Blob de Microsoft Azure (documentación de Microsoft Azure)
- Comandos de Rclone (documentación de Rclone)

Información adicional

Ejemplo de política de roles para instancias EC2

Esta política otorga a tu EC2 instancia acceso de lectura y escritura a un segmento específico de tu cuenta. Si este bucket usa una clave administrada por el cliente para realizar el cifrado en el servidor, es posible que la política necesite obtener acceso adicional a AWS Key Management Service (AWS KMS).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
              "arn:aws:s3:::amzn-s3-demo-bucket/*",
              "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Crear una entidad principal de servicio de Azure AD de solo lectura

Una entidad principal de servicio de Azure es una identidad de seguridad que usan las aplicaciones, los servicios y las herramientas de automatización de los clientes para acceder a recursos específicos de Azure. Considérelo como una identidad de usuario (nombre de usuario y contraseña o certificado) con un rol específico, y con permisos estrictamente controlados para acceder a sus recursos. Para crear una entidad principal de servicio de solo lectura, con permisos de privilegio mínimo, y proteger los datos de Azure ante eliminaciones accidentales, siga estos pasos:

1. Inicia sesión en el portal de tu cuenta en la nube de Microsoft Azure e inicia Cloud Shell PowerShell o usa la interfaz de línea de comandos (CLI) de Azure en tu estación de trabajo.

2. Cree una entidad principal de servicio y configúrela con acceso de solo lectura a su cuenta de almacenamiento Blob de Azure. Guarde la salida JSON de este comando en un archivo local llamado `azure-principal.json`. El archivo se cargará en tu instancia. EC2 Sustituya las variables de marcador de posición que aparecen entre corchetes ({ y }) por el identificador de suscripción de Azure, el nombre del grupo de recursos y el nombre de la cuenta de almacenamiento.

```
az ad sp create-for-rbac `
--name AWS-Rclone-Reader `
--role "Storage Blob Data Reader" `
--scopes /subscriptions/{Subscription ID}/resourceGroups/{Resource Group Name}/
providers/Microsoft.Storage/storageAccounts/{Storage Account Name}
```

Migración de Couchbase Server a Couchbase Capella en AWS

Battulga Purevragchaa y Saurabh Shanbhag, Amazon Web Services

Mark Gamble, ninguno

Resumen

Couchbase Capella es una base de datos NoSQL como servicio (DBaaS) totalmente gestionada para aplicaciones de misión crítica (por ejemplo, perfiles de usuario o catálogos en línea y gestión de inventario). Couchbase Capella gestiona su carga de trabajo DBaa S en una cuenta de Amazon Web Services (AWS) gestionada por Couchbase. Capella facilita la ejecución y la administración de la replicación de múltiples clústeres, múltiples regiones de AWS, multinube y nube híbrida dentro de una sola interfaz.

Couchbase Capella le ayuda a escalar al instante sus aplicaciones de Couchbase Server, lo que le permite crear clústeres de varios nodos en cuestión de minutos. Couchbase Capella es compatible con todas las características de Couchbase Server, incluidas SQL++, Full Text Search, Eventing Service y Analytics Service. También elimina la necesidad de gestionar las instalaciones, las actualizaciones, las copias de seguridad y el mantenimiento general de las bases de datos.

Este patrón describe los pasos y las prácticas recomendadas para migrar un entorno de Couchbase Server autogestionado a la nube de AWS. El patrón proporciona un proceso repetible para migrar datos e índices desde los clústeres de Couchbase Server, que se ejecutan en las instalaciones o en la nube, a Couchbase Capella. El uso de estos pasos le ayuda a evitar problemas durante la migración y acelera el proceso general de migración.

Este patrón proporciona las dos opciones de migración siguientes:

- La opción 1 es adecuada si tiene que migrar menos de 50 índices.
- La opción 2 es adecuada si tiene que migrar más de 50 índices.

También puede configurar datos de muestra en su Couchbase Server autogestionado para seguir la guía de migración.

Si elije la opción de migración 2, o si utiliza ámbitos o colecciones distintos del valor predeterminado, debe utilizar el archivo de configuración de ejemplo, que se encuentra en la sección Información adicional.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de pago de Couchbase Capella existente. También puede crear una cuenta de Couchbase Capella en AWS y utilizar la prueba gratuita de Couchbase Capella y, a continuación, actualizar a una cuenta de pago para configurar el clúster para la migración. Para empezar con la versión de prueba, siga las instrucciones de Introducción a Couchbase Capella.
- Un entorno de Couchbase Server autogestionado existente, ya sea en las instalaciones o implementado en un proveedor de servicios en la nube.
- Para la opción de migración 2, Couchbase Shell y un archivo de configuración. Para crear el archivo de configuración, puede usar el archivo de ejemplo que se encuentra en la sección de Información adicional.
- Familiaridad con la administración de Couchbase Server y Couchbase Capella.
- Familiaridad con la apertura de puertos TCP y la ejecución de comandos en una interfaz de la línea de comandos (CLI).

El proceso de migración también requiere los roles y la experiencia que se describen en la siguiente tabla.

Rol	Experiencia	Responsabilidades
Administrador de Couchbase	• Familiaridad con Couchbase Server y Couchbase Capella • El conocimiento básico de la línea de comandos es útil pero no obligatorio	• Couchbase Server y Capella: tareas específicas
Administrador de sistemas; administrador de TI	• Familiaridad con el entorno y la administración del sistema Couchbase Server autogestionado	• Abrir puertos y determinar las direcciones IP en los nodos de clústeres de Couchbase Server autogestionados

Limitaciones

- Este patrón se utiliza para migrar datos, índices e índices de búsqueda de texto completo de Couchbase desde Couchbase Server a Couchbase Capella en AWS. El patrón no se aplica a la migración de Couchbase Eventing Service ni a Couchbase Analytics.
- Couchbase Capella se encuentra disponible en varias regiones de AWS. Para up-to-date obtener información sobre las regiones compatibles con Capella, consulte Amazon Web Services en la documentación de Couchbase.

Versiones de producto

- Couchbase Server (Community o Enterprise) Edition, versión 5.x o posterior

Arquitectura

Pila de tecnología de origen

- Couchbase Server

Pila de tecnología de destino

- Couchbase Capella

Arquitectura de destino

1. Para acceder a Couchbase Capella, utilice el plano de control de Capella. Puede utilizar el plano de control de Capella para hacer lo siguiente:
   - Controlar y supervisar su cuenta.
   - Gestionar clústeres y datos, índices, usuarios y grupos, permisos de acceso, supervisión y eventos.
2. Se han creado clústeres.
3. El plano de datos de Capella se encuentra en la cuenta de AWS gestionada por Couchbase. Tras crear un clúster nuevo, Couchbase Capella lo implementa en varias zonas de disponibilidad de la región de AWS seleccionada.
4. Puede desarrollar e implementar aplicaciones de Couchbase en una VPC de su cuenta de AWS. Normalmente, esta VPC accede al plano de datos de Capella a través del emparejamiento de VPC.

Tools (Herramientas)

- La replicación cruzada de centros de datos (XDCR) de Couchbase ayuda a replicar los datos en clústeres ubicados en diferentes proveedores de nube y diferentes centros de datos. Se utiliza para migrar datos a Couchbase Capella desde clústeres de servidores Couchbase autogestionados.

> **Note**
>
> XDCR no se puede usar con Couchbase Server Community Edition para migrar a Couchbase Capella. En su lugar, puede utilizar cbexport. Para obtener más información, consulte la épica sobre cómo migrar datos de Community Edition.

- Couchbase Shell es un intérprete de comandos de línea para que Couchbase Server y Couchbase Capella accedan a clústeres de Couchbase locales y remotos. En este patrón, Couchbase Shell se usa para migrar índices.
- cbexport es una utilidad de Couchbase para exportar datos del clúster de Couchbase. Incluido en las herramientas CLI de Couchbase Server.

Epics

Preparativos para la migración

Tarea	Descripción	Habilidades requeridas
Evaluar el tamaño del clúster de Couchbase Server autogestionado.	Inicie sesión en la consola web de Couchbase para Couchbase Server y evalúe los nodos y los buckets de su clúster autogestionado. 1. Para mostrar una lista de los nodos del clúster, seleccione la pestaña Servers (Servidores) en la barra de navegación.	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	2. Registre el número de nodos y, a continuación, seleccione cada nodo de la lista para ver sus propiedades. 3. Registre la memoria y el almacenamiento de cada nodo individual. 4. Seleccione la pestaña Buckets en la barra de navegación y, a continuación, elija cada bucket de la lista para ver sus propiedades. Registre la cuota de RAM y la configuración de resolución de conflictos de cada bucket. Utilizará las configuraciones de clúster de Couchbase Server autogestionadas como guía general para dimensionar y configurar el clúster de destino en Couchbase Capella. Si necesita ayuda con un ejercicio de dimensionamiento más detallado del Couchbase Capella, póngase en contacto con Couchbase.	

Tarea	Descripción	Habilidades requeridas
Registre la distribución del servicio Couchbase en el clúster de Couchbase Server autogestionado.	1. En la consola web de Couchbase, seleccione la pestaña Servers (Servidor es) para ver la lista de nodos del clúster. 2. Elija cada nodo para mostrar sus propiedades y, a continuación, registre la distribución del servicio de Couchbase para cada nodo (Data Service (Servicio de datos), Query Service (Servicio de consultas), Index Service (Servicio de índice), Search Service (Servicio de búsqueda), Analytics Service (Servicio de análisis) y Eventing Service (Servicio de eventos)).	Administrador de Couchbase
Registre las direcciones IP de los nodos del clúster de Couchbase Server autogesti onados.	(Ignore este paso si utiliza Community Edition). Registre la dirección IP de cada nodo del clúster. Se añadirán a la lista de permitidos de su clúster de Couchbase Capella más adelante.	Administrador de Couchbase, administrador de sistemas

Implemente y configure los recursos en Couchbase Capella

Tarea	Descripción	Habilidades requeridas
Elija una plantilla.	1. Inicie sesión en su plano de control Couchbase Capella, elija la pestaña Dashboard (Panel de control) o la pestaña Clusters (Clústeres) en la navegación principal y, a continuación, elija Create Cluster (Crear clúster). 2. Con la información que registró en la evaluación de su clúster de Couchbase Server autogestionado, elija la plantilla de clúster que cumpla con los requisito s de la configuración. Si no encuentra una plantilla adecuada, elija Custom Template (Plantilla personalizada) en el editor de Cluster Sizing (Tamaño de clústeres).	Administrador de Couchbase
Elija y configure los nodos.	Elija y configure los nodos para que se adapten a su entorno de clústeres de Couchbase Server autogesti onado, incluida la cantidad de nodos, la distribución, el procesamiento o la RAM de los servicios y el almacenam iento.	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	Couchbase Capella utiliza las prácticas recomendadas de escalado multidimensional. Los servicios y los nodos solo se pueden elegir de acuerdo con las prácticas recomenda das de implementación. Esto puede significar que no puede igualar exactamente las configuraciones de su clúster de Couchbase Server autogestionado.	

Tarea	Descripción	Habilidades requeridas
Implementación del clúster.	El conocimiento básico de la línea de comandos es útil pero no obligatorio Para obtener instrucciones y pasos detallados, consulte Create a cluster (Crear un clúster) en la documentación de Couchbase . **Important** Si utiliza la versión de prueba gratuita de Couchbase Capella, debe convertirla en una cuenta de pago antes de comenzar la migración. Para convertir su cuenta, abra la sección Billing (Facturación) del plano de control de Couchbase Capella y, a continuación, seleccione Add Activation ID (Añadir un ID de activación). El ID de activación se envía a su dirección de correo electróni co de contacto de facturación después de completar un acuerdo de compra con Couchbase Sales	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	o después de realizar una compra a través de AWS Marketplace.	

Tarea	Descripción	Habilidades requeridas
Crear un usuario con credenciales de base de datos.	Un usuario con credenciales de base de datos es específico de un clúster y consta de un nombre de usuario, una contraseña y un conjunto de privilegios de bucket. Este usuario es necesario para crear buckets y acceder a los datos del bucket. En el plano de control de Couchbase Capella, cree una credencial de base de datos para el nuevo clúster siguiendo las instrucciones de Configure database credentials (Configurar las credenciales de la base de datos) de la documentación de Couchbase Capella. **Note** Un usuario de la organización necesita que se le asignen credenciales de rol organizativo si quiere acceder a los datos del bucket en un clúster concreto, ya sea de forma remota o a través de la interfaz de usuario de Couchbase Capella.	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	Esto es independiente de las credenciales de la base de datos, que suelen utilizar las aplicaciones y las integraciones. La creación del usuario organizacional le permite crear y administrar los buckets de destino en su clúster de Couchbase Capella.	
Si utiliza la opción de migración 2, instale Couchbase Shell.	Puede instalar Couchbase Shell en cualquier sistema que tenga acceso de red tanto a su Couchbase Server autogestionado como a los clústeres de Couchbase Capella. Para obtener más información, consulte Instalar la versión 1.0.0-beta.5 de Couchbase Shell en la documentación de Couchbase Shell. Confirme que Couchbase Shell esté instalado probando una conexión a su clúster autogestionado en un terminal de línea de comandos.	Administrador de Couchbase, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Permitir direcciones IP.	1. En el plano de control de Couchbase Capella, elija Clústeres y, a continuación, elija su clúster de destino. 2. Elija la pestaña Connect (Conectar) del clúster y registre el punto de conexión del clúster que aparece en Manage Allowed IP (Administrar la IP permitida). 3. Para añadir la dirección IP del sistema en el que instaló Couchbase Shell y la dirección IP de las instancias de clúster de Couchbase Server autogestionadas como direcciones IP permitidas, haga lo siguiente: a. En Wide Area Network (Red de área amplia), elija Manage Allowed IP (Administrar la IP permitida). b. Seleccione Add Allowed IP (Añadir la IP permitida), introduzca la dirección IP del sistema en el que instaló Couchbase Shell y, a continuac ión, seleccione Add IP (Añadir IP).	Administrador de Couchbase, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	c. Repita el paso anterior para añadir la dirección IP de la instancia de clúster autogestionada de Couchbase Server. Para obtener más información sobre las direcciones IP permitidas, consulte Configurar las direcciones IP permitidas en la documentación de Couchbase.	

Tarea	Descripción	Habilidades requeridas
Configuración de los certificados.	1. Para descargar el certificado raíz de su clúster, en Root Certificate (Certificado raíz), seleccione Download (Descargar). 2. Guarde el certificado raíz con la extensión de archivo .pem en una carpeta del sistema en la que se ejecute Couchbase Shell. 3. A continuación, inicie sesión en la consola web autogestionada de Couchbase Server, seleccione Security (Seguridad) en la barra de navegación izquierda y, a continuación, seleccione la pestaña Certificates (Certificados). 4. Copie el certificado raíz de su clúster de Couchbase Server autogestionado y guárdelo como un archivo .pem en la misma carpeta en la que guardó el archivo de certificado raíz de su clúster de Couchbase Capella. Para obtener más información acerca del certificado raíz, consulte Certificado raíz	Administrador de Couchbase, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	en la documentación de Couchbase Server.	
Crear el archivo de configuración para Couchbase Shell.	Cree un archivo dotfile de configuración en el directorio principal de la instalación de Couchbase Shell (por ejemplo, `/<HOME_DIRECTORY>/.cbsh/config`). Para obtener más información, consulte Dotfiles de configuración en la documentación de Couchbase. Añada las propiedades de conexión de los clústeres de origen y destino al archivo de configuración. Puede usar el archivo de ejemplo de configuración que se encuentra en la sección de Información adicional y editar los ajustes de los clústeres. Guarde el archivo de configuración con los ajustes actualizados en la carpeta `.cbsh` (por ejemplo, `/<HOME_DIRECTORY>/.cbsh/config`).	Administrador de Couchbase, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Cree buckets de destino.	Para cada bucket de origen, cree un bucket de destino en su clúster de Couchbase Capella siguiendo las instrucciones de la documentación de Couchbase para crear un bucket. Las configuraciones de los buckets de destino deben coincidir con los nombres de los buckets, los ajustes de memoria y los ajustes de resolución de conflictos de los buckets de su clúster de Couchbase Server autogestionado.	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas

Crear ámbitos y colecciones.	Cada bucket contiene un ámbito y una colección predeterminados con el espacio de claves `_default._default` . Si utiliza otros espacios de clave para el ámbito y la colección, debe crear espacios de clave idénticos en el clúster de Capella de destino.
	1. Abra el terminal de línea de comandos del sistema en el que instaló Couchbase Shell.
	2. Para iniciar Couchbase Shell, ejecute el siguiente comando.
	`./cbsh`
	3. Para cada bucket que desee migrar, cree ámbitos y colecciones en el clúster de Capella ejecutando los siguientes comandos. Asegúrese de reemplaza r <BUCKET_NAME> por el nombre del bucket que desea migrar.
	`scopes --clusters "On-Prem-Cluster" --bucket <BUCKET_NAME> | select scope | where scope !`
		Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	`= "_default" | each { |it| scopes create $it.scope --clusters "Capella-Cluster" } collections --clusters "On-Prem-Cluster" --bucket <BUCKET_NAME> | select scope collection | where $it.scope != "_default" | where $it.collection != "_default" | each { |it| collections create $it.collection --clusters "Capella-Cluster" --bucket <BUCKET_NAME> --scope $it.scope }`	

Migración de los datos de Enterprise Edition

Tarea	Descripción	Habilidades requeridas
Abrir los puertos TCP en los nodos del clúster autogestionado de Couchbase Server.	Asegúrese de que los puertos adecuados estén abiertos para la comunicación XDCR en los nodos del clúster de Couchbase Server autogestionado. Para obtener más información, consulte la documentación sobre puertos de Couchbase Server.	Administrador de Couchbase, administrador de sistemas
Si utiliza Couchbase Server Enterprise Edition, configure Couchbase XDCR.	1. En el plano de control de navegación central de Couchbase Capella, elija Clústeres y, a continuación,	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	elija su clúster de destino para la migración. 2. En Root Certificate (Certificado raíz), seleccione Copy (Copiar). 3. Inicie sesión en la consola web autogestionada de Couchbase Server y, en la barra de navegación principal, seleccione XDCR. A continuación, seleccione Add remote (Agregar remoto). 4. Ingrese la siguiente configuración: • Nombre del clúster: un nombre para la conexión del clúster de Capella • IP/nombre de host: el punto de conexión de su clúster de Couchbase Capella • Nombre de usuario para el clúster remoto: el usuario de la base de datos de su clúster de Couchbase Capella • Contraseña: la contraseña de usuario de la base de datos para su clúster de Couchbase Capella • Habilitar conexión segura: seleccionado	

Tarea	Descripción	Habilidades requeridas
	• Completo (encripta la contraseña y los datos con TLS): seleccionado 5. Pegue el certificado raíz del clúster de Capella que copió anteriormente y, a continuación, seleccione Save (Guardar).	
Iniciar Couchbase XDCR.	1. En la consola web autogestionada de Couchbase Server, elija XDCR en la barra de navegación principal, y luego seleccione Agregar replicación. 2. Ingrese la siguiente configuración: • Replicar desde un bucket: seleccione el bucket de origen para la migración. • Bucket remoto: introduzca el nombre del bucket de destino. • Clúster remoto: seleccione el clúster de destino que creó anteriormente. 3. Elija Save Replication (Guardar replicación). El proceso de replicación debería comenzar en unos segundos.	Administrador de Couchbase

Migración de los índices mediante la opción 1

Tarea	Descripción	Habilidades requeridas
Migración de los índices de clústeres autogestionados a Couchbase Capella.	**⚠ Important** Recomendamos este proceso si tiene que migrar menos de 50 índices. Si tiene que migrar más de 50 índices, le recomendamos que utilice la opción de migración 2. 1. En la consola web de Couchbase, elija Indexes (Índices). 2. En la lista de índices, seleccione el primer índice que desea migrar. A continuación, se muestra la definición del índice. 3. Copie la definición del índice mediante la instrucción `CREATE`, pero no copie `WITH { "defer_build":true } .` Por ejemplo, del siguiente ejemplo de definición de índice, solo copiaría `CREATE INDEX` `` `cityindex` ON `travel-sample`(`city`) . ``	Administrador de Couchbase, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	<pre>CREATE INDEX `cityinde x` ON `travel-s ample`(`city`) WITH { "defer_bu ild":true }</pre> 4. En el plano de control de Couchbase Capella, elija Clústeres y, a continuación, elija el clúster de destino. 5. En la lista desplegable Herramientas, elija Query Workbench. Pegue la instrucción `CREATE` que copió anteriormente en el Query Editor (Editor de consultas) y, a continuación, seleccione Execute (Ejecutar). Esto crea y desarrolla el índice. 6. Para confirmar que se ha creado el índice, elija Indexes (Índices) en la lista desplegable Tools (Herramientas). La lista muestra que el índice se creó y se desarrolló. 7. Repita este proceso para cada índice que desee migrar.	

Migración de los índices mediante la opción 2

Tarea	Descripción	Habilidades requeridas

Migre las definiciones del índice.	**Important**
	Recomendamos este proceso si tiene que migrar más de 50 índices. Si tiene que migrar menos de 50 índices, le recomendamos que utilice la opción de migración 1.
	
	1. Abra el terminal de línea de comandos del sistema en el que instaló Couchbase Shell.
	2. Para iniciar Couchbase Shell, ejecute el siguiente comando.
	`./cbsh`
	3. Para conectarse al clúster de Couchbase Server autogestionado, ejecute el siguiente comando.
	`cb-env cluster On-Prem-Cluster`
	4. Para migrar las definiciones de índice del clúster de Couchbase Server
		Administrador de Couchbase, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	autogestionado al clúster de Couchbase Capella, ejecute el siguiente comando para cada bucket que desee migrar. Asegúrese de reemplazarlas por el nombre del bucket <BUCKET_NAME> que corresponda a los índices que desee migrar. Esta opción de migración requiere que los nombres de los buckets de destino sean idénticos a los nombres de los buckets de origen. `query indexes -- definitions | where bucket =~ <BUCKET_NAME>| get definition | each { |it| query $it --clusters Capella-Cluster }`	

Tarea	Descripción	Habilidades requeridas

Crear las definiciones del índice.	1. Para cambiar de contexto al clúster de Couchbase Capella, ejecute el siguiente comando:
	`cb-env cluster Capella-Cluster`
	2. Para crear las definiciones de índice que se migraron al clúster de Couchbase Capella, ejecute el siguiente comando y sustitúya <BUCKET_NAME> por el nombre del bucket que corresponda a los índices que desee crear.
	`query 'SELECT RAW CONCAT("BUILD INDEX ON ", k , "(['", CONCAT2 ("','", inames), "']);") FROM system:indexes AS s LET bid = CONCAT("` ",s.bucket_id, "`"), sid = CONCAT("`", s.scope_id, "`"), kid = CONCAT("` ", s.keyspace_id, "`"), k = NVL2(bid, CONCAT2(".", bid, sid, kid), kid) WHERE s.namespa ce_id = "default" AND s.bucket_id = "" GROUP BY k LETTING inames = ARRAY_AGG (s.name) FILTER`
		Administrador de Couchbase, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	(WHERE s.state = 'deferred') HAVING ARRAY_LENGTH(iname s) > 0;' | each { | it| query $it } 3. Repita este proceso para cada bucket.	

Migración de índices de búsqueda de texto completo

Tarea	Descripción	Habilidades requeridas
Migre los índices de búsqueda de texto completo de clústeres autogestionados a Couchbase Capella.	1. En la consola web de Couchbase, elija Search (Buscar). 2. En la lista de índices de búsqueda de texto completo (FTS), elija el primer índice de FTS que desee migrar, elija Show index definition JSON y, a continuación, Copy to Clipboard. Anote el nombre del índice y el bucket al que pertenece. 3. En el plano de control de Couchbase Capella, elija Clústeres y, a continuación, elija su clúster de destino. 4. En la lista desplegable de herramientas, seleccione Full Text Search (Búsqueda de texto completo).	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	5. Seleccione Import Index (Importar índice) y pegue la definición del índice FTS. 6. Introduzca el Index Name (Nombre del índice), seleccione el bucket correcto, tal y como se indica en el clúster autogestionado, y, a continuación, pulse Create (Crear). 7. Repita este proceso para cada índice FTS que desee migrar.	

Migración de los datos de Couchbase Community Edition

Tarea	Descripción	Habilidades requeridas
Exportar datos desde Couchbase Server Community Edition autogestionada.	El XDCR cifrado no está disponible en Couchbase Community Edition. Puede exportar los datos de Couchbase Community Edition y luego importarlos manualmente a Couchbase Capella. Para exportar datos del bucket de origen, utilice `cbexport` en la línea de comandos. Puede ver un ejemplo en el siguiente comando:	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas

	`cbexport json \`
	`--cluster localhost \`
	`--bucket <SOURCE BUCKET NAME> \`
	`--format lines \`
	`--username <USERNAME> \`
	`--password <PASSWORD> \`
	`--include-key cbkey \`
	`--scope-field cbscope \`
	`--collection-field cbcoll \`
	`--output cbexported_data.json`
	
	Tenga en cuenta que `cbkey`, `cbscope`, `cbcoll` y `cbexported_data.json` son etiquetas arbitrarias. Se hará referencia a ellas más adelante en el proceso, así que si decide asignarles un nombre diferente, anótelo.	

Tarea	Descripción	Habilidades requeridas
Importar datos a Couchbase Capella.	1. En el plano de control de Couchbase Capella, elija Clústeres y, a continuación, elija el clúster de destino. 2. En la lista desplegable Tools (Herramientas), seleccione Import (Importar). Se abrirá un asistente con los seis pasos siguientes: a. Bucket: elija el bucket de destino. b. File (Archivo): elija JSON, elija Lines (Líneas) y, a continuac ión, elija Using your web browser (Usar su navegador web). Si tiene una gran cantidad de datos, puede explorar la opción Manually (Manualmente). Seleccione el archivo creado por `cbexport`. c. Colecciones: elija un Custom Collection Mapping (asignación de colecciones personali zado). Si su base de datos de Community Edition no usa ámbitos ni coleccion es, o solo usa _default, puede elegir la opción	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	Select Single Collection (Seleccionar colección única) en su lugar. Para Collection Mapping Expression (Expresión de asignación de colección), introduzca `%cbscope%.%cbcoll%` . Para comprobar que esta expresión funciona correctamente, puede pegar datos de ejemplo, como los siguientes. `{ "cbscope" :"inventory", "cbcoll":"landmark", "cbkey":" landmark_3991" }` d. Clave: elija Customer Generation (Generación de clientes). (Si no le importa conservar las claves de los datos que va a importar, puede seleccionar el Automatically Generated UUID (UUID generado automáticamente) en su lugar y continuar con el paso 5). En Key Name Generator Expression (Expresión del generador de nombres de clave),	

Tarea	Descripción	Habilidades requeridas
	introduzca %cbkey%. Para comprobar que esta expresión funciona correctamente, pegue datos de ejemplo. e. Configuraciones: elija Ignore fields (Ignorar campos) e introduzca cbscope, cbcoll o cbkey. Estos campos contienen información transitor ia que no necesita estar en el bucket de destino después de una importación. No cambie los valores predeterm inados de los demás ajustes. f. Importar: revise y seleccione Import (Importar) cuando esté listo. Espere a que se carguen y se importen los datos. Para archivos grandes, Couchbase Capella admite la importación por línea de comandos mediante cURL. Puede explorar las opciones de importación con más detalle en Import data (Importar datos) en la	

Tarea	Descripción	Habilidades requeridas
	documentación de Couchbase Capella.	

Probar y verificar la migración

Tarea	Descripción	Habilidades requeridas
Comprobación de la migración de datos.	1. En el plano de control de Couchbase Capella, elija Clústeres y, a continuación, elija el clúster de destino de su lista de clústeres. 2. Seleccione la pestaña Buckets para el clúster de destino. Compruebe que el número de elementos (documentos) del bucket de destino coincide con el número de elementos del bucket de origen. 3. En el clúster de destino, en la lista desplegable Tools (Herramientas), seleccione Documents (Documentos). Compruebe que se hayan migrado todos los documentos. 4. (Opcional) Una vez migrados todos los datos, puede cerrar la replicación eliminándola. Para obtener más información, consulte Delete a replication (Eliminación	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	de una replicación) en la documentación de Couchbase.	
Verificar la migración del índice.	En el plano de control de Couchbase Capella, en la lista desplegable Tools (Herramientas) del clúster de destino, seleccione Indexes (Índices). Compruebe que los índices se hayan migrado y creado.	Administrador de Couchbase
Verificar los resultados de consulta.	1. En el plano de control de Couchbase Capella, en la lista desplegable Tools (Herramientas) del clúster de destino, seleccione Query Workbench. 2. Ejecute un ejemplo de consulta de N1QL o una consulta utilizada en su aplicación. Asegúrese de recibir los mismos resultados que cuando ejecutó la consulta en su clúster de Couchbase Server autogestionado.	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
Verificar los resultados de la búsqueda de texto completo (aplicable si migró los índices FTS).	1. En el plano de control de Couchbase Capella, en la lista desplegable Herramientas del clúster de destino, seleccione Full Text Search (Búsqueda de texto completo). 2. Seleccione un índice FTS eligiendo su nombre. 3. Elija Buscar. 4. Introduzca un ejemplo de consulta de búsqueda y seleccione Search (Buscar). 5. Compruebe que los resultados sean los mismos que cuando ejecutó la búsqueda en el clúster autogestionado.	Administrador de Couchbase

Recursos relacionados

Preparativos para la migración

- Comience con la prueba gratuita de Couchbase Capella
- Requisitos de proveedor de servicios en la nube para Couchbase Capella
- Pautas de tamaños de Couchbase Capella

Migración de datos e índices

- Couchbase XDCR
- Documentación de Couchbase Shell

Couchbase, Capella y su soporte SLAs

- Acuerdos de nivel de servicio de Couchbase Capella () SLAs
- Política de soporte del servicio Couchbase Capella

Información adicional

El siguiente código es un ejemplo de archivo de configuración para Couchbase Shelll.

```
Version = 1

[[clusters]]
identifier = "On-Prem-Cluster"
hostnames = ["<SELF_MANAGED_COUCHBASE_CLUSTER>"]
default-bucket = "travel-sample"
username = "<SELF_MANAGED_ADMIN>"
password = "<SELF_MANAGED_ADMIN_PWD>"
tls-cert-path = "/<ABSOLUTE_PATH_TO_SELF_MANAGED_ROOT_CERT>"
data-timeout = "2500ms"
connect-timeout = "7500ms"
query-timeout = "75s"

[[clusters]]
identifier = "Capella-Cluster"
hostnames = ["<COUCHBASE_CAPELLA_ENDPOINT>"]
default-bucket = "travel-sample"
username = "<CAPELLA_DATABASE_USER>"
password = "<CAPELLA_DATABASE_USER_PWD>"
tls-cert-path = "/<ABSOLUTE_PATH_TO_COUCHBASE_CAPELLA_ROOT_CERT>"
data-timeout = "2500ms"
connect-timeout = "7500ms"
query-timeout = "75s"
```

Antes de guardar el archivo de configuración, utilice la siguiente tabla para asegurarse de haber agregado su propia información de clúster de origen y destino.

<SELF_MANAGED_COUCHBASE_CLUSTER>	Use las direcciones IP para su clúster de Couchbase Server autogestionado.

<SELF_MANAGED_ADMIN>	Use el usuario administrador para su clúster de Couchbase Server autogestionado.
<ABSOLUTE_PATH_TO_SELF_MANAGED_ROOT_CERT>	Use la ruta absoluta al archivo de certificado raíz guardado para su clúster de Couchbase Server autogestionado.
<COUCHBASE_CAPELLA_ENDPOINT>	Use el punto de conexión de su clúster de Couchbase Capella.
<CAPELLA_DATABASE_USER>	Use el usuario de la base de datos para su clúster de Couchbase Capella.
<CAPELLA_DATABASE_USER_PWD>	Use la contraseña de usuario de la base de datos para su clúster de Couchbase Capella.
<ABSOLUTE_PATH_TO_COUCHBASE_CAPELLA_ROOT_CERT>	Use la ruta absoluta al archivo de certificado raíz guardado para su clúster de Couchbase Capella.

Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2

Neal Ardeljan y Afroz Khan, Amazon Web Services

Resumen

Este patrón le guía por los pasos para migrar de un sistema Red Hat Enterprise Linux (RHEL) 6.9 o posterior local que ejecute IBM WebSphere Application Server (WAS) a RHEL 8 con Apache Tomcat en una instancia de Amazon Elastic Compute Cloud (Amazon). EC2

Este patrón se puede aplicar a las siguientes versiones de origen y destino:

- WebSphere Application Server 7.x a Apache Tomcat 8 (con Java 7 o posterior)
- WebSphere Del servidor de aplicaciones 8.x a Apache Tomcat 8 (con Java 7 o posterior)
- WebSphere Del servidor de aplicaciones 8.5.5.x a Apache Tomcat 9 (con Java 8 o posterior)
- WebSphere Del servidor de aplicaciones 8.5.5.x a Apache Tomcat 10 (con Java 8 o posterior)

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Código fuente de Java, con las siguientes suposiciones:
  - Emplea la versión de Java Development Kit (JDK) de Java 7 o posterior
  - Emplea el marco Spring o Apache Struts
  - No utiliza el framework Enterprise Java Beans (EJB) ni ninguna otra funcionalidad de WebSphere servidor que no esté fácilmente disponible para Tomcat
  - Utiliza principalmente servlets o Java Server Pages () JSPs
  - Emplea conectores de Java Database Connectivity (JDBC) para conectar a las bases de datos
- Fuente: IBM WebSphere Application Server versión 7.x o superior
- Destino: Apache Tomcat, versión 8.5 o superior

Arquitectura

Pila de tecnología de origen

- Una aplicación web creada con el marco Apache Struts Model-View-Controller (MVC)
- Una aplicación web que se ejecuta en las versiones 7.x u 8.x de IBM WebSphere Application Server
- Una aplicación web que emplea un conector Lightweight Directory Access Protocol (LDAP) para conectar a un directorio LDAP (iPlanet/eTrust)
- Una aplicación que emplea la conectividad de IBM Tivoli Access Manager (TAM) para actualizar la contraseña del usuario de TAM (en la presente implementación, las aplicaciones usan PD.jar)

Bases de datos en las instalaciones

- Oracle Database 21c (21.0.0.0)
- Oracle Database 19c (19.0.0.0)
- Oracle Database 12c Versión 2 (12.2.0.1)
- Oracle Database 12c Release 1 (12.1.0.2)

Pila de tecnología de destino

- Apache Tomcat versión 8 (o posterior) que se ejecuta en RHEL en una instancia EC2
- Amazon Relational Database Service (Amazon RDS) para Oracle

Para obtener más información sobre las versiones de Oracle compatibles con Amazon RDS, consulte el sitio web de Amazon RDS para Oracle.

Arquitectura de destino

Tools (Herramientas)

- Nivel de aplicación: reconstrucción de una aplicación Java en un archivo WAR.
- Nivel de base de datos: copia de seguridad y restauración nativas de Oracle.
- Herramienta de migración de Apache Tomcat para Jakarta EE. Esta herramienta toma una aplicación web escrita para Java EE 8 y ejecutada en Apache Tomcat 9 y la convierte automáticamente para ejecutarla en Apache Tomcat 10, que implementa Jakarta EE 9.

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Complete el descubrimiento de las aplicaciones, el estado actual y la línea base de rendimiento.		BA, líder de migración
Valide las versiones de las bases de datos de origen y de destino.		Administrador de base de datos
Identifique los requisitos de hardware para la instancia del servidor EC2 de destino.		DBA, SysAdmin
Identifique los requisitos de almacenamiento (como el tipo y la capacidad de almacenamiento).		DBA, SysAdmin
Elija el tipo de EC2 instancia adecuado en función de la capacidad, las características de almacenamiento y las características de la red.		DBA, SysAdmin
Identifique los requisitos de seguridad de acceso a la red para las bases de datos de origen y destino.		DBA, SysAdmin
Identifique la estrategia y las herramientas de migración de aplicaciones.		Administrador de base de datos, líder de migración

Tarea	Descripción	Habilidades requeridas
Complete el diseño de la migración y la guía de migración de la aplicación.		Responsable de compilación, líder de migración
Complete el manual de procedimientos de migración de aplicaciones.		Responsable de compilación, líder de transición, líder de pruebas, líder de migración

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).		SysAdmin
Creación de grupos de seguridad.		SysAdmin
Configure e inicie Amazon RDS para Oracle.		DBA, SysAdmin

Migración de datos

Tarea	Descripción	Habilidades requeridas
Cree o acceda a los puntos de conexión para recuperar los archivos de copia de seguridad de la base de datos.		Administrador de base de datos
Utilice el motor de base de datos nativo o una herramien ta de terceros para migrar los	Para obtener más información, consulte “Migración de objetos y datos de bases de datos”	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
objetos y datos de la base de datos.	en la sección de Información adicional.	

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Presente la solicitud de cambio (CR) para la migración .		Líder de transición
Obtenga la aprobación de la CR para la migración.		Líder de transición
Siga la estrategia de migración de aplicaciones según el manual de procedimi entos de migración de aplicaciones.	Para obtener más información, consulte “Configurar el nivel de aplicación” en la sección de Información adicional.	Administrador de base de datos, ingeniero de migracion es, propietario de la aplicación
Actualice la aplicación (si es necesario).		Administrador de base de datos, ingeniero de migracion es, propietario de la aplicación
Complete las pruebas funcionales y no funcionales, de validación de datos, de acuerdo de nivel de servicio y de rendimiento.		Líder de pruebas, propietario de la aplicación, usuarios de la aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Obtenga la aprobación del propietario de la aplicación o del propietario de la empresa.		Líder de transición
Cambie los clientes de aplicaciones a la nueva infraestructura.		Administrador de base de datos, ingeniero de migracion es, propietario de la aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporale s de AWS.		DBA, ingeniero de migración, SysAdmin
Revise y valide los documento s del proyecto.		Líder de migración
Recopile métricas como el tiempo de migración, el porcentaje de esfuerzo manual en comparación con el automatizado y el ahorro de costos.		Líder de migración
Cerrar el proyecto y enviar comentarios.		Líder de migración, propietario de la aplicación

Recursos relacionados

Referencias

- Documentación de Apache Tomcat 10.0

- Documentación de Apache Tomcat 9.0
- Documentación de Apache Tomcat 8.0
- Guía de instalación de Apache Tomcat 8.0
- Documentación de JNDI de Apache Tomcat
- Sitio web de Amazon RDS para Oracle
- Precios de Amazon RDS
- Oracle y Amazon Web Services
- Oracle en Amazon RDS
- Implementaciones de Amazon RDS Multi-AZ

Tutoriales y videos

- Introducción a Amazon RDS

Información adicional

Migración de objetos y datos de bases de datos

Por ejemplo, si utiliza backup/restore utilidades nativas de Oracle:

1. Cree la copia de seguridad de Amazon Simple Storage Service (Amazon S3) para los archivos de copia de seguridad de la base de datos (opcional).
2. Haga una copia de seguridad de los datos de la base de datos de Oracle en la carpeta compartida de la red.
3. Inicie sesión en el servidor transitorio de migración para mapear la carpeta compartida de la red.
4. Copie los datos de la carpeta de recursos compartidos de la red al bucket de S3.
5. Solicite una implementación de Amazon RDS Multi-AZ para Oracle.
6. Restaure la copia de seguridad de la base de datos en las instalaciones en Amazon RDS para Oracle.

Configurar el nivel de aplicación

1. Instale Tomcat 8 (o 9/10) desde el sitio web de Apache Tomcat.
2. Empaquete la aplicación y las bibliotecas compartidas en un archivo WAR.

3. Implemente el archivo WAR en Tomcat.
4. Supervise el registro de inicio para `Linux cat` ver si hay alguna biblioteca compartida que falte WebSphere.
5. Observe el registro de inicio de `Linux cat` cualquier WebSphere extensión descriptora de despliegue específica.
6. Recopile del servidor las bibliotecas Java dependientes que falten. WebSphere
7. Modifique los elementos descriptores de despliegue WebSphere específicos con equivalentes compatibles con Tomcat.
8. Reconstruya el archivo WAR con las bibliotecas Java dependientes y los descriptores de implementación actualizados.
9. Actualice la configuración de LDAP y la configuración de la base de datos y pruebe las conexiones (consulte las instrucciones de configuración de Realm y las instrucciones de JNDI Datasource en la documentación de Apache Tomcat).
10. Pruebe la aplicación instalada con la base de datos de Amazon RDS para Oracle restaurada.
11. Cree una Amazon Machine Image (AMI) para Linux a partir de la EC2 instancia.
12. Inicie la arquitectura completa con el equilibrador de carga de aplicación y el grupo de escalado automático.
13. Actualice URLs (mediante la unión WebSeal) para que apunte al Application Load Balancer.
14. Actualice la base de datos de administración de configuración (CMDB).

Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2 con Auto Scaling

Kevin Yung y Afroz Khan, Amazon Web Services

Resumen

Este patrón proporciona orientación para migrar una aplicación Java de IBM WebSphere Application Server a Apache Tomcat en una instancia de Amazon Elastic Compute Cloud EC2 (Amazon) con Amazon EC2 Auto Scaling activado.

Con el uso de este patrón, puede lograr lo siguiente:

- Una reducción de los costos de licencias de IBM
- Alta disponibilidad mediante la Implementación multi-AZ
- Resiliencia de aplicaciones mejorada con Amazon EC2 Auto Scaling

Requisitos previos y limitaciones

Requisitos previos

- Las aplicaciones Java (versión 7.x o 8.x) deben desarrollarse en pilas LAMP.
- El estado de destino es alojar aplicaciones Java en hosts Linux. Este patrón se ha implementado con éxito en un entorno de Red Hat Enterprise Linux (RHEL) 7. Otras distribuciones de Linux pueden seguir este patrón, pero consultando siempre la configuración de la distribución de Apache Tomcat.
- Debe comprender las dependencias de la aplicación Java.
- Debe tener acceso al código fuente de la aplicación Java para poder realizar cambios.

Limitaciones y redefiniciones de plataforma

- Debe comprender los componentes del archivo empresarial (EAR) y comprobar que todas las bibliotecas estén empaquetadas en archivos WAR de componentes web. Debe configurar el complemento WAR de Apache Maven y producir artefactos en los archivos WAR.
- Al usar Apache Tomcat 8, existe un conflicto conocido entre servlet-api.jar y los archivos jar integrados en el paquete de la aplicación. Para resolver este problema, elimine servlet-api.jar del paquete de la aplicación.

- Debe configurar WEB-INF/Resources, ubicado en classpath de la Configuración de Apache Tomcat. De forma predeterminada, las bibliotecas JAR no se cargan en el directorio. Como alternativa, puede implementar todos los recursos que se indican a continuación. src/main/resources
- Compruebe si hay alguna raíz de contexto con codificación rígida en la aplicación Java y actualice la nueva raíz de contexto de Apache Tomcat.
- Para configurar las opciones de tiempo de ejecución de JVM, puede crear el archivo de configuración setenv.sh en la carpeta bin de Apache Tomcat; por ejemplo, JAVA_OPTS, JAVA_HOME, etc.
- La autenticación se configura a nivel de contenedor, como un dominio en las configuraciones de Apache Tomcat. La autenticación se establece para cualquiera de los tres dominios siguientes:
  - JDBC Database Realm busca los usuarios en una base de datos relacional a la que se accede mediante el controlador JDBC.
  - DataSource Database Realm busca usuarios en una base de datos a la que accede JNDI.
  - JNDI Directory Realm busca a los usuarios en el directorio de Lightweight Directory Access Protocol (LDAP) al que accede el proveedor de JNDI. Las búsquedas requieren:
    - Detalles de la conexión LDAP: base de búsqueda de usuarios, filtro de búsqueda, base de roles, filtro de roles
    - Dominio clave del directorio JNDI: se conecta a LDAP, autentica a los usuarios y recupera todos los grupos de los que un usuario es miembro
- Autorización: en el caso de un contenedor con una autorización basada en roles que compruebe las restricciones de autorización en web.xml, los recursos web deben definirse y compararse con los roles indicados en las restricciones. Si LDAP no tiene un mapeo de roles de grupo, debe establecer el atributo < security-role-ref > en web.xml para lograr el mapeo de roles de grupo. Para ver un ejemplo de un documento de configuración, consulte la documentación de Oracle.
- Conexión de base de datos: cree una definición de recurso en Apache Tomcat con una URL y detalles de conexión de un punto de conexión Amazon Relational Database Service (Amazon RDS). Actualice el código de la aplicación para que haga referencia a mediante la búsqueda JNDI. DataSource Una conexión de base de datos existente definida en no WebSphere funcionaría, ya que utiliza sus nombres WebSphere JNDI. Puede añadir una <resource-ref>entrada en el archivo web.xml con el nombre y la definición del DataSource tipo del JNDI. Para ver un ejemplo de documento de configuración, consulte la documentación de Apache Tomcat.
- Registro: de forma predeterminada, Apache Tomcat inicia sesión en la consola o en un archivo de registro. Puede habilitar el rastreo a nivel de dominio actualizando logging.properties (consulte

Registros en Tomcat). Si usa Apache Log4j para añadir registros a un archivo, debe descargar tomcat-juli y añadirlo al classpath.

- Gestión de sesiones: si va a usar IBM WebSeal como equilibrador de carga de aplicación y gestión de sesiones, no es necesario realizar ningún cambio. Si utiliza un Application Load Balancer o Network Load Balancer en AWS para reemplazar el componente IBM WebSeal, debe configurar la administración de sesiones mediante una instancia de ElastiCache Amazon con un clúster de Memcached y configurar Apache Tomcat para que utilice la administración de sesiones de código abierto.
- Si usa el proxy de reenvío WebSeal de IBM, debe configurar un nuevo equilibrador de carga de red en AWS. Utilice lo que IPs proporciona el Network Load Balancer para las configuraciones de empalmes WebSeal.
- Configuración SSL: le recomendamos que utilice Secure Sockets Layer (SSL) para end-to-end las comunicaciones. Para configurar un servidor SSL en Apache Tomcat, siga las instrucciones de la documentación de Apache Tomcat.

Arquitectura

Pila de tecnología de origen

- Servidor WebSphere de aplicaciones IBM

Pila de tecnología de destino

- La arquitectura usa Elastic Load Balancing (versión 2). Si usa IBM WebSeal para la gestión de identidades y el equilibrio de carga, puede seleccionar un equilibrador de carga de red en AWS para integrarlo con el proxy inverso IBM WebSeal.
- Las aplicaciones Java se implementan en un servidor de aplicaciones Apache Tomcat, que se ejecuta en una EC2 instancia de un grupo de Amazon EC2 Auto Scaling. Puedes configurar una política de escalado basada en CloudWatch las métricas de Amazon, como el uso de la CPU.
- Si va a dejar de utilizar IBM WebSeal para el equilibrio de carga, puede utilizar Amazon for Memcached ElastiCache para la gestión de sesiones.
- En la base de datos de backend, puede implementar alta disponibilidad (Multi-AZ) para Amazon RDS y seleccionar un tipo de motor de base de datos.

Arquitectura de destino

Tools (Herramientas)

- AWS CloudFormation
- Interfaz de la línea de comandos de AWS (AWS CLI)
- Apache Tomcat (versión 7.x o 8.x)
- RHEL 7 o Centos 7
- Implementación de Amazon RDS Multi-AZ
- Amazon ElastiCache para Memcached (opcional)

Epics

Configure el VPC

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).		
Cree subredes.		
Cree tablas de enrutamiento si es necesario.		
Cree listas de control de acceso a la red (). ACLs		
Configure AWS Direct Connect o una conexión VPN corporativa.		

Redefina la plataforma de la aplicación

Tarea	Descripción	Habilidades requeridas
Refactorice la configuración de Maven en compilación de la aplicación para generar los artefactos de WAR.		
Refactorice los orígenes de datos de dependencia de las aplicaciones en Apache Tomcat.		
Refactorice los códigos fuente de las aplicaciones para que usen nombres JNDI en Apache Tomcat.		
Implemente los artefactos WAR en Apache Tomcat.		
Complete las validaciones y pruebas de las aplicaciones.		

Configurar la red

Tarea	Descripción	Habilidades requeridas
Configure el firewall corporativo para permitir la conexión a los servicios de dependencia.		
Configure el firewall corporativo para permitir el acceso de los usuarios finales a Elastic Load Balancing en AWS.		

Cree la infraestructura de aplicaciones

Tarea	Descripción	Habilidades requeridas
Cree e implemente la aplicación en una EC2 instancia.		
Cree un clúster de Amazon ElastiCache for Memcached para la administración de sesiones.		
Cree una instancia de Amazon RDS Multi-AZ para la base de datos de backend.		
Cree certificados SSL e impórtelos a AWS Certificate Manager (ACM).		
Instale certificados SSL en los equilibradores de carga.		
Instale certificados SSL para los servidores Apache Tomcat.		
Complete las validaciones y pruebas de las aplicaciones.		

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Desactive la infraestructura existente.		

Tarea	Descripción	Habilidades requeridas
Restaure la base de datos de producción a Amazon RDS.		
Realice cambios en el DNS para interrumpir la aplicación.		

Recursos relacionados

Referencias

- Documentación de Apache Tomcat 7.0
- Guía de instalación de Apache Tomcat 7.0
- Documentación de JNDI de Apache Tomcat
- Implementaciones Multi-AZ de Amazon RDS
- Amazon ElastiCache para Memcached

Tutoriales y videos

- Introducción a Amazon RDS

Migración de una aplicación .NET de Microsoft Azure App Service a AWS Elastic Beanstalk

Raghavender Madamshitti, Amazon Web Services

Resumen

Este patrón describe cómo migrar una aplicación web .NET alojada en Microsoft Azure App Service a AWS Elastic Beanstalk. Hay dos formas de migrar aplicaciones a Elastic Beanstalk:

- Mediante AWS Toolkit para Visual Studio: este complemento para el IDE de Microsoft Visual Studio proporciona la forma más fácil y sencilla de implementar aplicaciones .NET personalizadas en AWS. Puede utilizar este enfoque para implementar código .NET directamente en AWS y crear recursos de apoyo, como Amazon Relational Database Service (Amazon RDS) para bases de datos de SQL Server, directamente desde Visual Studio.
- Mediante carga e implementación en Elastic Beanstalk: cada Azure App Service incluye un servicio en segundo plano llamado Kudu que resulta útil para capturar los volcados de memoria y los registros de implementación, ver los parámetros de configuración y acceder a los paquetes de implementación. Puede usar la consola Kudu para acceder al contenido de Azure App Service, extraer el paquete de implementación y, a continuación, cargar el paquete en Elastic Beanstalk mediante la opción de carga e implementación de la consola de Elastic Beanstalk.

Este patrón describe el segundo enfoque (cargar la aplicación en Elastic Beanstalk a través de Kudu). El patrón también utiliza los siguientes servicios de AWS: AWS Elastic Beanstalk, Amazon Virtual Private Cloud (Amazon VPC), Amazon, Amazon Elastic Compute Cloud (Amazon) Auto Scaling, CloudWatch Amazon Simple Storage Service (Amazon S3 EC2) Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) y Amazon Route 53.

La aplicación web.NET se implementa en AWS Elastic Beanstalk, que se ejecuta en un grupo de Amazon EC2 Auto Scaling. Puedes configurar una política de escalado basada en CloudWatch las métricas de Amazon, como el uso de la CPU. Para una base de datos, puede utilizar Amazon RDS en un entorno Multi-AZ o Amazon DynamoDB, según los requisitos empresariales y de la aplicación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa

- Una aplicación web .NET que se ejecute en Azure App Service
- Permiso para usar la consola Kudu de Azure App Service

Versiones de producto

- .NET Core (x64) 1.0.1, 2.0.0 o posterior, o .NET Framework 4.x, 3.5 (consulte el historial de la plataforma .NET en Windows Server)
- Internet Information Services (IIS) versión 8.0 o posterior que se ejecute en Windows Server 2012 o posterior
- .NET 2.0 o 4.0 Runtime.

Arquitectura

Pila de tecnología de origen

- Aplicación desarrollada con .NET Framework 3.5 o posterior, o .NET Core 1.0.1, 2.0.0 o posterior, y alojada en Azure App Service (aplicación web o aplicación API)

Pila de tecnología de destino

- AWS Elastic Beanstalk ejecutándose en un grupo de Amazon EC2 Auto Scaling

Arquitectura de migración

Flujo de trabajo de una implementación

Tools (Herramientas)

Herramientas

- .NET Core o .NET Framework
- C#
- IIS
- Consola Kudu

Servicios y características de AWS

- AWS Elastic Beanstalk: Elastic Beanstalk es un servicio para implementar y easy-to-use escalar aplicaciones web.NET. Elastic Beanstalk administra automáticamente el aprovisionamiento de capacidad, el equilibrio de carga y el escalado automático.
- Grupo Amazon EC2 Auto Scaling: Elastic Beanstalk incluye un grupo de Auto Scaling que administra las instancias de Amazon en EC2 el entorno. En un entorno de una sola instancia, el grupo de escalado automático garantiza que siempre haya una instancia en ejecución. En un entorno con equilibrio de carga, puede configurar el grupo con un rango de instancias para su ejecución, y Amazon EC2 Auto Scaling añade o elimina instancias según sea necesario, en función de la carga.
- Elastic Load Balancing: cuando habilita el equilibrio de carga en AWS Elastic Beanstalk, se crea un balanceador de carga que distribuye el tráfico entre las instancias del entorno. EC2
- Amazon CloudWatch: Elastic Beanstalk CloudWatch utiliza Amazon automáticamente para proporcionar información sobre los recursos de su aplicación y entorno. Amazon CloudWatch admite métricas estándar, métricas personalizadas y alarmas.
- Amazon Route 53: Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad. Puede usar los registros de alias de Route 53 para asignar nombres de dominio personalizados a los entornos de AWS Elastic Beanstalk.

Epics

Configurar una VPC

Tarea	Descripción	Habilidades requeridas
Configure una nube privada virtual (VPC).	En su cuenta de AWS, cree una VPC con la información requerida.	Administrador de sistemas
Cree subredes.	Cree dos o más subredes en la VPC.	Administrador de sistemas
Cree una tabla de enrutamie nto.	Cree una tabla de enrutamie nto según sus necesidades.	Administrador de sistemas

Configurar Elastic Beanstalk

Tarea	Descripción	Habilidades requeridas
Acceda a la consola Kudu de Azure App Service.	Para acceder a Kudu a través del portal de Azure, diríjase al panel de control de App Service y, a continuación, seleccione Advanced Tools (Herramientas avanzadas) y Go (Ir). O bien, puede modificar la URL del servicio de aplicaciones de Azure de la siguiente manera: `https://<appservicename>.scm.azurewebsites.net` .	Desarrollador de aplicaciones, administrador de sistemas
Descargue el paquete de implementación de Kudu.	Navegue a Windows PowerShell seleccionando la DebugConsoleopción. De esta forma se abrirá la consola Kudo. Vaya a la carpeta `wwwroot` y descárguela. Se descargará el paquete de implementación de Azure App Service como un archivo zip. Para ver un ejemplo, consulte el archivo adjunto.	Desarrollador de aplicaciones, administrador de sistemas
Cree un paquete para Elastic Beanstalk.	Descomprima el paquete de implementación que descargó de Azure App Service. Cree un archivo JSON llamado `aws-windows-deployment-manifest.json` (este archivo solo es necesario para las	Desarrollador de aplicaciones, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	aplicaciones .NET Core). Cree un archivo zip que incluya el archivo `aws-windows-deployment-manifest.json` del paquete de implementación de Azure App Service. Para ver un ejemplo, consulte el archivo adjunto.	
Cree una nueva aplicación de Elastic Beanstalk.	Abra la consola de Elastic Beanstalk. Seleccione una aplicación existente o cree una nueva.	Desarrollador de aplicaciones, administrador de sistemas
Cree el entorno.	En el menú Actions (Acciones) de la consola de Elastic Beanstalk, seleccione Create environment (Crear entorno). Seleccione el entorno del servidor web y la plataforma .NET/IIS. En código de aplicación, seleccione Cargar. Cargue el archivo zip que preparó para Elastic Beanstalk y, a continuación, seleccione Create Environment (Crear entorno).	Desarrollador de aplicaciones, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Configura Amazon CloudWatch.	De forma predeterminada, la CloudWatch supervisión básica está habilitada. Si desea cambiar la configuración, en el asistente de Elastic Beanstalk, seleccione la aplicación publicada y, a continuación, Monitoring (Supervisión).	Administrador de sistemas
Compruebe que el paquete de implementación se encuentre en Amazon S3.	Una vez creado el entorno de la aplicación, encontrará el paquete de implementación en el bucket de S3.	Desarrollador de aplicaciones, administrador de sistemas
Probar la aplicación.	Una vez creado el entorno, utilice la URL proporcionada en la consola de Elastic Beanstalk para probar la aplicación.	Administrador de sistemas

Recursos relacionados

- Conceptos AWS Elastic Beanstack (documentación de Elastic Beanstalk)
- Getting Started with .NET on Elastic Beanstalk (Introducción a .NET en Elastic Beanstalk (documentación de Elastic Beanstalk)
- Consola Kudu () GitHub
- Using "Kudu" to Manage Azure Web Apps (artículo de GS Lab)
- Custom ASP.NET Core Elastic Beanstalk Deployments (Guía del usuario del Kit de herramientas de AWS para Visual Studio)
- Documentación de Elastic Load Balancing
- AWS Elastic Beanstalk Supported Platforms (Plataformas compatibles con AWS Elastic Beanstalk (documentación de Elastic Beanstalk)

- Deploy a Web Application to AWS (Implementación de una aplicación web en AWS) (artículo de C# Corner)
- Cómo escalar el tamaño de su grupo de Auto Scaling (EC2 documentación de Amazon)
- High Availability (Multi-AZ) for Amazon RDS (Alta disponibilidad (Multi-AZ) para Amazon RDS) (documentación de Amazon RDS)

Información adicional

Notas

- Si va a migrar una base de datos en las instalaciones o de Azure SQL Server a Amazon RDS, también debe actualizar los detalles de conexión a la base de datos.
- Para realizar las pruebas, se adjunta un ejemplo de aplicación de demostración.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migre de Oracle WebLogic a Apache Tomcat (ToMEE) en Amazon ECS

Anya Epishcheva y Harshad Gohil, Amazon Web Services

Resumen

Este patrón describe los pasos para migrar un sistema Oracle Solaris SPARC local que ejecuta Oracle WebLogic a una instalación basada en contenedores Docker que ejecuta Apache ToMEE (Apache Tomcat con soporte adicional para contenedores) con Amazon Elastic Container Service (Amazon ECS).

Para obtener información sobre la migración de las bases de datos asociadas a las aplicaciones que va a migrar de Oracle a Tomcat, consulte los patrones de migración de bases de datos de este WebLogic catálogo.

Prácticas recomendadas

Los pasos para migrar las aplicaciones web de Java y Java Enterprise Edition (Java EE) varían según la cantidad de recursos específicos del contenedor que utilice la aplicación. Las aplicaciones basadas en Spring suelen ser más fáciles de migrar, ya que tienen un número reducido de dependencias en el contenedor de implementación. Por el contrario, las aplicaciones Java EE que utilizan recursos empresariales JavaBeans (EJBs) y de contenedores gestionados, como los grupos de subprocesos, el Servicio de autenticación y autorización de Java (JAAS) y la persistencia gestionada por contenedores (CMP), requieren más esfuerzo.

Las aplicaciones desarrolladas para Oracle Application Server utilizan con frecuencia la suite Oracle Identity Management. Los clientes que migran a servidores de aplicaciones de código abierto suelen optar por volver a implementar la gestión de identidades y accesos mediante una federación basada en SAML. Otros utilizan Oracle HTTP Server Webgate en casos en los que la migración desde la suite Oracle Identity Management no es una opción.

Las aplicaciones web Java y Java EE son excelentes candidatas para su implementación en los servicios de AWS basados en Docker, como AWS Fargate y Amazon ECS. Los clientes suelen elegir una imagen de Docker con la última versión del servidor de aplicaciones de destino (como ToMEE) y el kit de desarrollo de Java (JDK) preinstalados. Instalan sus aplicaciones sobre la imagen de Docker base, la publican en su registro Amazon Elastic Container Registry (Amazon ECR) y la utilizan para la implementación escalable de sus aplicaciones en AWS Fargate o Amazon ECS.

Lo ideal es que la implementación de aplicaciones sea elástico, es decir, que el número de instancias de aplicaciones se amplíe o disminuya en función del tráfico o la carga de trabajo. Esto significa

que las instancias de aplicaciones deben estar en línea o cancelarse para ajustar la capacidad a la demanda.

Cuando traslade una aplicación Java a AWS, considere convertirla en apátrida. Este es un principio arquitectónico clave del Marco de AWS Well-Architected que permitirá el escalado horizontal mediante el almacenaje en contenedores. Por ejemplo, la mayoría de las aplicaciones web basadas en Java almacenan la información de las sesiones de los usuarios de forma en las instalaciones. Para sobrevivir a la finalización de la instancia de la aplicación debido al escalado automático en Amazon Elastic Compute Cloud (Amazon EC2) o por otros motivos, la información de las sesiones de los usuarios debe almacenarse de forma global para que los usuarios de aplicaciones web puedan seguir trabajando sin problemas y de forma transparente sin tener que volver a conectarse a una aplicación web ni volver a iniciar sesión en ella. Existen varias opciones de arquitectura para este enfoque, como Amazon ElastiCache for Redis o el almacenamiento del estado de la sesión en una base de datos global. Los servidores de aplicaciones, como ToMEE, tienen complementos que permiten almacenar y administrar las sesiones a través de Redis, bases de datos y otros almacenes de datos globales.

Utilice una herramienta común y centralizada de registro y depuración que se integre fácilmente con Amazon CloudWatch y AWS X-Ray. La migración brinda la oportunidad de mejorar las capacidades del ciclo de vida de las aplicaciones. Por ejemplo, es posible que desee automatizar el proceso de creación para que los cambios se puedan realizar fácilmente mediante una canalización de integración y entrega continuas (CI/CD). Esto puede requerir cambios en la aplicación para que pueda implementarse sin tiempo de inactividad.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Código fuente de Java y JDK
- Aplicación de origen creada con Oracle WebLogic
- Solución definida para Identity and Access Management (SAML u Oracle Webgate)
- Solución definida para la gestión de las sesiones de la aplicación (like-for-liketrasladarla o con Amazon ElastiCache, o hacer que la aplicación quede sin estado si es necesario)
- Sepa si el equipo necesita refactorizar las bibliotecas específicas de J2EE para poder transferirlas a Apache ToMEE (consulte el estado de implementación de Java EE 7 en el sitio web de Apache)
- Imagen reforzada de ToMEE en función de sus requisitos de seguridad

- Imagen de contenedor con el objetivo ToMee preinstalado
- Se acuerda e implementa la corrección de la aplicación si es necesaria (por ejemplo, registro, depuración, compilación o autenticación)

Versiones de producto

- Oracle WebLogic OC4 J, 9i, 10 g
- Tomcat 7 (con Java 1.6 o versiones posteriores)

Arquitectura

Pila de tecnología de origen

- Aplicación web creada con Oracle WebLogic
- Aplicación web que utiliza la autenticación Oracle Webgate o SAML
- Aplicaciones web conectadas a la versión 10g y posteriores de Oracle Database

Pila de tecnología de destino

- ToMEE (Apache Tomcat con soporte adicional para contenedores) que se ejecuta en Amazon ECS (consulte también Implementación de aplicaciones web Java y microservicios Java en Amazon ECS)
- Amazon Relational Database Service (Amazon RDS) para Oracle; para ver las versiones de Oracle compatibles con Amazon RDS, consulte Amazon RDS para Oracle

Arquitectura de destino

Tools (Herramientas)

Para funcionar en ToMEE, una aplicación Java debe reconstruirse en un archivo.war. En algunos casos, es posible que sea necesario realizar cambios en la aplicación para que funcione en ToMee; debe comprobar que las opciones de configuración y las propiedades del entorno necesarias estén definidas correctamente.

Además, las búsquedas de la interfaz de nombres y directorios de Java (JNDI) y los espacios de nombres de JavaServer páginas (JSP) deben definirse correctamente. Considere la posibilidad de comprobar los nombres de los archivos utilizados por la aplicación para evitar colisiones de nombres con las bibliotecas T integradas. Por ejemplo, persistence.xml es un nombre de archivo utilizado por el marco Apache OpenJPA (que se incluye con OpenEJB en ToMEE) con fines de configuración. El archivo persistence.xml de PUI contiene las declaraciones Bean de Spring Framework.

La versión 7.0.3 y posteriores de ToMee (Tomcat 8.5.7 y posteriores) devuelve una respuesta HTTP 400 (solicitud incorrecta) en formato RAW (sin codificar) con caracteres especiales. URLs La respuesta del servidor aparece como una página en blanco para el usuario final. Las versiones anteriores de ToMee y Tomcat permitían el uso de ciertos caracteres especiales no codificados URLs; sin embargo, se considera inseguro, como se indica en el sitio web CVE-2016-6816. Para resolver el problema de codificación de las URL, las que URLs se pasen directamente al navegador a través de ellas JavaScript deben codificarse con el método encodeURI () en lugar de utilizarse como cadenas sin procesar.

Tras implementar el archivo.war en ToMEE, supervise el registro de inicio de Linux cat para ver si faltan bibliotecas compartidas y extensiones específicas de Oracle para añadir los componentes que falten de las bibliotecas de Tomcat.

Procedimiento general

- Configure la aplicación en ToMee.
- Identifique y reconfigure los archivos y recursos de configuración específicos del servidor de aplicaciones desde el formato de origen al formato de destino.
- Identifique y reconfigure los recursos de JNDI.
- Ajuste el espacio de nombres y las búsquedas de EJB al formato requerido por el servidor de aplicaciones de destino (si corresponde).
- Reconfigure las funciones de seguridad y las asignaciones principales específicas del contenedor de aplicaciones de JAAS (si corresponde).
- Empaquete la aplicación y las bibliotecas compartidas en un archivo.war.
- Implemente el archivo.war en ToMEE mediante el contenedor de Docker proporcionado.
- Supervise el registro de inicio para identificar cualquier biblioteca compartida o extensión descriptora de implementación que falte. Si encuentra alguna, vuelva a la primera tarea.
- Pruebe la aplicación instalada con la base de datos de Amazon RDS restaurada.

- Inicie la arquitectura completa con un equilibrador de carga y un clúster de Amazon ECS siguiendo las instrucciones de Implementación de contenedores de Docker.
- Actualiza el punto URLs para que apunte al balanceador de cargas.
- Actualice la base de datos de administración de configuración (CMDB).

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Realice el descubrimiento de aplicaciones (estado actual del entorno y punto de referencia de rendimiento).		BA, líder de migración
Validar versiones y motores de las bases de datos de origen y destino.		Administrador de base de datos
Valide el diseño de la aplicación de origen y destino (gestión de identidades y sesiones).		Administrador de base de datos, ingeniero de migraciones, propietario de la aplicación
Identifique los requisitos de hardware y almacenamiento para la instancia del servidor de destino.		DBA, SysAdmin
Elija el tipo de instancia adecuado en función de la capacidad, las características de almacenamiento y las características de red.		DBA, SysAdmin
Identifique los requisitos de seguridad de acceso a la		DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
red de las bases de datos de origen y destino.		
Identifique la estrategia y las herramientas de migración de aplicaciones.		Administrador de base de datos, líder de migración
Complete el diseño de la migración y la guía de migración de la aplicación.		Responsable de compilación, líder de migración
Complete el manual de procedimientos de migración de aplicaciones.		Responsable de compilación, líder de transición, líder de pruebas, líder de migración

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).		SysAdmin
Cree grupos de seguridad.		SysAdmin
Configure e inicie la instancia de base de datos de Amazon RDS.		DBA, SysAdmin
Configure la implementación de Amazon ECS.		SysAdmin
Empaquete su aplicación como una imagen de Docker.		SysAdmin
Inserte la imagen en el registro de Amazon ECR (u		SysAdmin

Tarea	Descripción	Habilidades requeridas
omita este paso y envíela al clúster de Amazon ECS).		
Configure la definición de tareas para la aplicación y las opciones de servicio de Amazon ECS.		SysAdmin
Configure su clúster, revise los ajustes de seguridad y establezca los roles de AWS Identity and Access Management (IAM).		SysAdmin
Inicie la configuración y ejecute las pruebas de acuerdo con el manual de procedimientos de migración de aplicaciones.		SysAdmin

Migración de datos

Tarea	Descripción	Habilidades requeridas
Obtenga el permiso de su equipo de control de seguridad para trasladar los datos de producción a AWS.		Administrador de base de datos, ingeniero de migracion es, propietario de la aplicación
Cree puntos de conexión y obtenga acceso a ellos para recuperar los archivos de copia de seguridad de la base de datos.		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Utilice el motor de base de datos nativo o herramientas de terceros para migrar los objetos y datos de la base de datos.		Administrador de base de datos
Ejecute las pruebas necesarias del manual de procedimientos de migración de aplicaciones para confirmar que la migración de datos se realizó correctamente.		Administrador de base de datos, ingeniero de migraciones, propietario de la aplicación

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Cree una solicitud de cambio (CR) para la migración.		Líder de transición
Obtenga la aprobación de CR para la migración.		Líder de transición
Siga la estrategia de migración de aplicaciones del manual de procedimientos de migración de aplicaciones.		Administrador de base de datos, ingeniero de migraciones, propietario de la aplicación
Actualice la aplicación (si es necesario).		Administrador de base de datos, ingeniero de migraciones, propietario de la aplicación
Realice pruebas funcionales y no funcionales, de validación		Líder de pruebas, propietario de la aplicación, usuarios de la aplicación

Tarea	Descripción	Habilidades requeridas
de datos, de acuerdo de nivel de servicio y de rendimiento.		

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Obtenga la aprobación del propietario de la aplicación o de la empresa.		Líder de transición
Realiza un ejercicio sobre un tema de mesa para repasar todos los pasos del manual de procedimientos de transición.		Administrador de base de datos, ingeniero de migracion es, propietario de la aplicación
Cambie los clientes de aplicaciones a la nueva infraestructura.		Administrador de base de datos, ingeniero de migracion es, propietario de la aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporale s de AWS.		DBA, ingeniero de migración, SysAdmin
Revise y valide los documento s del proyecto.		Líder de migración
Recopile métricas sobre el tiempo de migración, el porcentaje de migraciones manuales en comparación con		Líder de migración

Tarea	Descripción	Habilidades requeridas
las realizadas con herramien tas, el ahorro de costos, etc.		
Cerrar el proyecto y enviar comentarios.		Líder de migración, propietario de la aplicación

Recursos relacionados

Referencias

- Documentación de Apache Tomcat 7.0
- Guía de instalación de Apache Tomcat 7.0
- Documentación de JNDI de Apache Tomcat
- Documentación de Apache ToMee
- Amazon RDS para Oracle
- Precios de Amazon RDS
- Oracle y AWS
- Documentación de Oracle en Amazon RDS
- Implementaciones de Amazon RDS Multi-AZ
- Introducción a Amazon ECS
- Introducción a Amazon RDS

Tutoriales y videos

- Prácticas recomendadas para ejecutar las bases de datos de Oracle en Amazon RDS (re:Invent 2018 presentation)

Migre una base de datos Oracle de Amazon EC2 a Amazon RDS for Oracle mediante AWS DMS

Chethan Gangadharaiah y Brian Motzer, Amazon Web Services

Resumen

Este patrón describe los pasos para migrar una base de datos Oracle en Amazon Elastic Compute Cloud (Amazon EC2) a Amazon Relational Database Service (Amazon RDS) para Oracle mediante AWS Database Migration Service (AWS DMS). El patrón también utiliza Oracle SQL Developer o SQL *Plus para conectarse a la instancia de base de datos de Oracle e incluye una CloudFormation plantilla de AWS que automatiza algunas de las tareas.

La migración a Amazon RDS para Oracle le permite centrarse en su empresa y en sus aplicaciones, mientras que Amazon RDS se encarga de las tareas de administración de bases de datos, como el aprovisionamiento de bases de datos, las copias de seguridad y la recuperación, los parches de seguridad, las actualizaciones de versiones y la administración del almacenamiento.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una imagen de máquina de Amazon (AMI) para Oracle Database en Amazon EC2

Versiones de producto

- AWS DMS es compatible con las versiones de Oracle 11g (versiones 11.2.0.3.v1 y posteriores), 12c y 18c para bases de datos de instancias de Amazon RDS para las ediciones Enterprise, Standard, Standard One y Standard Two. Para obtener la información más reciente sobre las versiones compatibles, consulte Uso de una base de datos de Oracle como origen para AWS DMS en la documentación de AWS. (Las CloudFormation plantillas de AWS adjuntas utilizan la versión 12c de Oracle como base de datos de origen).
- Desarrollador SQL de Oracle 4.0.3

Arquitectura

Arquitectura de origen

- Base de datos Oracle en Amazon EC2

Arquitectura de destino

- Amazon RDS para Oracle

Arquitectura de migración

Tools (Herramientas)

- AWS DMS: AWS Database Migration Service (AWS DMS) le ayuda a migrar los datos de forma rápida y segura a AWS. Admite migraciones homogéneas y heterogéneas. Para obtener información sobre las versiones y ediciones de bases de datos de Oracle compatibles, consulte Uso de una base de datos de Oracle como origen para AWS DMS y Uso de una base de datos de Oracle como destino para AWS DMS en la documentación de AWS.
- Oracle SQL Developer o SQL *Plus: estas herramientas le permiten conectarse a la instancia de base de datos de Amazon RDS para Oracle.

Epics

Configurar la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Crear una instancia de base de datos de Amazon RDS para Oracle.	Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/. Cree una instancia de base de datos de Oracle seleccionando el motor, la plantilla, la configuración de credenciales de base de datos, el tipo de instancia, el almacenamiento, la configuración de multi-AZ,	Desarrollador

Tarea	Descripción	Habilidades requeridas
	la nube privada virtual (VPC) y la configuración, las credencia les de inicio de sesión y las configuraciones adicional es para la base de datos de Oracle. Para obtener instrucci ones, consulte los enlaces de la sección "Recursos relacionados". O utilice la CloudFormation plantilla de AWS (Create_RDS.yaml) del archivo adjunto para crear la instancia de base de datos Amazon RDS for Oracle.	

Tarea	Descripción	Habilidades requeridas
Conéctese a Amazon RDS y conceda privilegios al usuario de Oracle.	Modifique el grupo de seguridad para abrir los puertos adecuados para conectarse desde la máquina local y la instancia de replicación de AWS DMS. Al configurar la conectividad, asegúrese de que la opción «Accesible públicamente» esté seleccionada para poder conectarse a la base de datos desde fuera de la VPC. Conéctese a Amazon RDS con Oracle SQL Developer o SQL *Plus mediante las credenciales de inicio de sesión, cree un usuario de AWS DMS y proporcione los privilegios necesarios al usuario de AWS DMS para modificar la base de datos.	Desarrollador

Configure el grupo de seguridad de la instancia de origen EC2

Tarea	Descripción	Habilidades requeridas
Compruebe si la base de datos de Oracle está en funcionamiento.	Utilice Secure Shell (SSH) para conectarse a la EC2 instancia e intente conectarse a la base de datos de Oracle mediante SQL *Plus.	Desarrollador
Modifique el grupo de seguridad.	Modifique el grupo de seguridad de la EC2 instancia	Desarrollador

Tarea	Descripción	Habilidades requeridas
	para abrir los puertos correspondientes, de modo que pueda conectarse desde su máquina local y la instancia de replicación de AWS DMS.	

Configure AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación de AWS DMS.	En AWS DMS, cree una instancia de replicación en la misma VPC que su instancia de base de datos Amazon RDS para Oracle. Especifique el nombre y la descripción de la instancia de replicación, elija la clase de instancia y la versión del motor de replicación (utilice la predeterminada), elija la VPC en la que creó la instancia de base de datos de Amazon RDS, establezca la configuración de multi-AZ en caso necesario, asigne almacenamiento, especifique la zona de disponibilidad y configure ajustes adicionales. Como alternativa, puede usar la CloudFormation plantilla de AWS (DMS.yaml) del archivo adjunto para implementar este paso.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Conéctese a los puntos de conexión de las bases de datos de origen y destino.	Cree los puntos de conexión de la base de datos de origen y destino especificando el identificador del punto de conexión, el motor, el servidor, el puerto, las credenciales de inicio de sesión y los atributos de conexión adicionales. Para el servidor de origen, utilice el DNS público de la EC2 instancia que aloja la base de datos de Oracle. Para el servidor de destino, utilice el punto de conexión de Amazon RDS para Oracle. Realice una prueba para comprobar que las conexiones de origen y destino funcionan. Como alternativa, puede usar la CloudFormation plantilla de AWS (DMS.yaml) del archivo adjunto para implementar este paso.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree una tarea de AWS DMS.	Cree una tarea de AWS DMS para migrar los datos del punto de conexión de origen al punto de conexión de destino, para configurar la replicación entre el punto de conexión de origen y destino, o ambos. Al crear la tarea de AWS DMS, especifique la instancia de replicación, el punto de conexión de origen, el punto de conexión de destino, el tipo de migración (solo datos, solo replicación o ambos), el mapeo de tablas y el filtro. Ejecute la tarea de AWS DMS, supervise la tarea, compruebe las estadísticas de la tabla y compruebe los registros en Amazon CloudWatch. Como alternativa, puede usar la CloudFormation plantilla de AWS (DMS.yaml) del archivo adjunto para implementar este paso.	Administrador de base de datos

Recursos relacionados

- Creación de una instancia de base de datos de Amazon RDS
- Conexión a una instancia de base de datos que ejecuta el motor de base de datos de Oracle
- Documentación de AWS DMS
- Tutoriales de AWS DMS Step-by-Step
- Migración de bases de datos de Oracle a la nube de AWS

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migre una base de datos Oracle local a Amazon OpenSearch Service mediante Logstash

Aditya Goteti, Amazon Web Services

Resumen

Este patrón describe cómo mover datos de una base de datos Oracle local a Amazon OpenSearch Service mediante Logstash. Incluye consideraciones arquitectónicas y algunos conjuntos de habilidades necesarias y recomendaciones. Los datos pueden proceder de una sola tabla o de varias tablas en las que será necesario realizar una búsqueda de texto completo.

OpenSearch El servicio se puede configurar dentro de una nube privada virtual (VPC) o se puede colocar públicamente con restricciones basadas en IP. Este patrón describe un escenario en el que el OpenSearch servicio se configura dentro de una VPC. Logstash se utiliza para recopilar los datos de la base de datos de Oracle, analizarlos en formato JSON y, a continuación, introducir los datos en Service. OpenSearch

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Java 8 (requerido por Logstash 6.4.3)
- Conectividad entre los servidores de bases de datos locales y las instancias de Amazon Elastic Compute Cloud (Amazon EC2) en una VPC, establecida mediante la red privada virtual de AWS (AWS VPN)
- Una consulta para recuperar los datos necesarios para enviarlos a OpenSearch Service desde la base de datos
- Controladores de Oracle Java Database Connectivity (JDBC)

Limitaciones

- Logstash no puede identificar los registros que se han eliminado definitivamente de la base de datos

Versiones de producto

- Oracle Database 12c
- OpenSearch Servicio 6.3
- Logstash 6.4.3

Arquitectura

Pila de tecnología de origen

- Base de datos de Oracle en las instalaciones
- AWS VPN en las instalaciones

Pila de tecnología de destino

- VPC
- EC2 instancia
- OpenSearch Servicio
- Logstash
- NAT Gateway (para actualizar el sistema operativo en las EC2 instancias e instalar Java 8, Logstash y complementos)

Arquitectura de migración de datos

Tools (Herramientas)

- Logstash 6.4.3
- Complemento de entrada JDBC (descarga y más información)
- Complemento de salida de Logstash (_es) logstash-output-amazon
- Controladores JDBC de Oracle

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Identificar el tamaño de la base de datos de origen.	El tamaño de los datos de origen es uno de los parámetros que se utilizan para determinar el número de particiones que se van a configurar en un índice.	Administrador de base de datos, Desarrollador de base de datos
Analizar los tipos de datos de cada columna y los datos correspondientes.	OpenSearch El servicio mapea dinámicamente el tipo de datos cuando encuentra en el documento un campo que no se había visto anteriorm ente. Si hay algún tipo o formato de datos específic o (por ejemplo, campos de fecha) que deba declararse de forma explícita, identifique los campos y defina la asignació n de esos campos durante la creación del índice.	Propietario de la aplicación, desarrollador, desarrollador de bases de datos
Determinar si hay columnas con claves principales o únicas.	Para evitar la duplicación de registros en Amazon OpenSearch Service durante las actualizaciones o insercion es, debes configurar el `document_id` ajuste en la sección de resultados del `amazon_es` complemento (por ejemplo, `document_id => "%{customer_id}"`	Propietario de la aplicación, desarrollador

Tarea	Descripción	Habilidades requeridas
	dónde `customer_id` está la clave principal).	
Analizar el número y la frecuencia de los nuevos registros que se agregan; comprobar la frecuencia con la que se eliminan los registros.	Esta tarea es necesaria para comprender la tasa de crecimiento de los datos de origen. Si los datos se leen de forma intensiva y las insercion es son poco frecuentes, puede tener un índice único. Si se insertan nuevos registros con frecuencia y no hay eliminaci ones, el tamaño de la partición puede superar fácilmente el tamaño máximo recomenda do de 50 GB. En este caso, se puede crear un índice de forma dinámica configura ndo los patrones de índice en Logstash y en el código al que se puede acceder mediante un alias.	Propietario de la aplicación, desarrollador
Determinar cuántas réplicas se necesitan.		Propietario de la aplicación, desarrollador
Determinar la cantidad de particiones que se van a configurar en el índice.		Propietario de la aplicación, desarrollador
Identifique los tipos de instancias para los nodos maestros dedicados, los nodos de datos y la EC2 instancia.	Para obtener más información, consulte la sección Recursos relacionados.	Propietario de la aplicación, desarrollador

Tarea	Descripción	Habilidades requeridas
Determinar el número de nodos maestros dedicados y nodos de datos necesarios.	Para obtener más información, consulte la sección Recursos relacionados.	

Migración de datos

Tarea	Descripción	Habilidades requeridas
Lanza una EC2 instancia.	Lance una EC2 instancia dentro de la VPC a la que está conectada la VPN de AWS.	Constructos de Amazon VPC, VPN de AWS
Instale Logstash en la instancia. EC2		Desarrollador
Instalar los complementos de Logstash.	Instalar los complementos de Logstash necesarios `jdbc-input` y `logstash-output-amazon_es` .	Desarrollador
Configurar Logstash.	Crear el almacén de claves de Logstash para almacenar información confidencial, como las claves de AWS Secrets Manager y las credenciales de las bases de datos, y, a continuación, colocar las referencias en un archivo de configuración de Logstash.	Desarrollador
Configurar la cola de mensajes fallidos y la cola persistente.	De forma predeterminada, cuando Logstash detecta un evento que no puede procesar porque los datos	Desarrollador

Tarea	Descripción	Habilidades requeridas
	contienen un error de mapeo o algún otro problema, la canalización de Logstash bloquea o descarta el evento fallido. Para protegerse de la pérdida de datos en esta situación, puede configurar Logstash para que escriba los eventos fallidos en una cola de mensajes fallidos en lugar de descartarlos. Para evitar la pérdida de datos durante una interrupción anómala, Logstash tiene una caracterí stica de cola persistente que almacenará la cola de mensajes en el disco. Las colas persistentes proporcio nan la durabilidad de los datos en Logstash.	

Tarea	Descripción	Habilidades requeridas
Crea el dominio OpenSearch de Amazon Service.	Cree el dominio de Amazon OpenSearch Service con una política de acceso que no requiera firmar las solicitud es con las credenciales de AWS Identity and Access Management (IAM). El dominio OpenSearch de Amazon Service debe crearse en la misma VPC. También debe seleccionar los tipos de instancias y establecer el número de nodos dedicados y maestros en función de su análisis.	Desarrollador
Configura los registros de Amazon OpenSearch Service necesarios.	Para obtener más información, consulta la documentación del OpenSearch servicio.	
Cree el índice.		Desarrollador
Iniciar Logstash.	Ejecutar Logstash como un servicio en segundo plano. Logstash ejecuta la consulta SQL configurada, extrae los datos, los convierte al formato JSON y los envía a Service. OpenSearch Para la carga inicial, no configure el programador en el archivo de configuración de Logstash.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Consulte los documentos.	Compruebe el número de documentos del índice y si todos los documentos están presentes en la base de datos de origen. Durante la carga inicial, se añaden al índice y se utilizan para detener Logstash. Cambie la configuración de Logstash para agregar un programador que se ejecute en un intervalo fijo según los requisitos del cliente y reinicie Logstash. Logstash seleccion ará solo los registros que se hayan actualizado o agregado después de la última ejecución , y la marca temporal de la última ejecución se almacenar á en el archivo que está configurado con la propiedad `last_run_metadata_ path => "/usr/sha re/logstash/.logst ash_jdbc_last_run"` en el archivo de configuración de Logstash.	Desarrollador

Recursos relacionados

- Alarmas recomendadas CloudWatch
- Nodos maestros OpenSearch de Amazon Service dedicados
- Dimensionamiento de los dominios de Amazon OpenSearch Service

- Documentación de Logstash
- Complemento de entrada JDBC
- Complemento de salida Logstash
- Sitio web OpenSearch de Amazon Service

Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle

Baji Shaik y Pavan Pusuluri, Amazon Web Services

Resumen

Este patrón describe los pasos para migrar bases de datos de Oracle en las instalaciones a Amazon Relational Database Service (Amazon RDS) para Oracle. Como parte del proceso de migración, debe crear un plan de migración y tener en cuenta los factores importantes de la infraestructura de la base de datos de destino en función de la base de datos de origen. Puede elegir una de las dos opciones de migración según los requisitos empresariales y el caso de uso:

- AWS Database Migration Service (AWS DMS): puede usar AWS DMS para migrar bases de datos a la nube de AWS de forma rápida y segura. Su base de datos de origen permanece totalmente operativa durante la migración, lo que minimiza el tiempo de inactividad de las aplicaciones que dependen de ella. Puede reducir el tiempo de migración mediante AWS DMS para crear una tarea que capture los cambios continuos después de completar una migración inicial a carga completa mediante un proceso denominado captura de datos de cambios (CDC).
- Herramientas nativas de Oracle: puede migrar bases de datos mediante herramientas nativas de Oracle, como Oracle y Data Pump Export y Data Pump Import con Oracle GoldenGate for CDC. También puede utilizar herramientas nativas de Oracle, como la utilidad de exportación original y la utilidad de importación original, para reducir el tiempo de carga total.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de Oracle en las instalaciones
- Una instancia de base de datos (DB) Oracle de Amazon RDS

Limitaciones

- Límite de tamaño de la base de datos: 64 TB

Versiones de producto

- Oracle, versiones 11g (versiones 11.2.0.3.v1 y posteriores) y hasta la 12.2 y la 18c. Para obtener la lista más reciente de versiones y ediciones compatibles, consulte Amazon RDS para Oracle en la documentación de AWS. Para ver las versiones de Oracle compatibles con AWS DMS, consulte Uso de una base de datos de Oracle como origen de AWS DMS en la documentación de AWS DMS.

Arquitectura

Pila de tecnología de origen

- Bases de datos de Oracle en las instalaciones

Pila de tecnología de destino

- Amazon RDS para Oracle

Arquitectura de origen y destino

En el siguiente diagrama se muestra cómo migrar una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante AWS DMS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Cree o utilice un usuario de base de datos existente, conceda los permisos de AWS DMS necesarios para ese usuario, active el modo ARCHIVELOG y, a continuación, configure el registro adicional.
2. Configure la puerta de enlace de Internet entre la red en las instalaciones y la red de AWS.
3. Configure los puntos de conexión de origen y destino para AWS DMS.
4. Configure las tareas de replicación de AWS DMS para migrar los datos de la base de datos de origen a la base de datos de destino.
5. Complete las actividades posteriores a la migración en la base de datos de destino.

En el siguiente diagrama se muestra cómo migrar una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante herramientas nativas de Oracle.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Cree o utilice un usuario de base de datos existente y otorgue los permisos necesarios para realizar una copia de seguridad de la base de datos de Oracle mediante las utilidades Export (`exp`) e Import (`imp`) de Oracle.
2. Configure la puerta de enlace de Internet entre la red en las instalaciones y la red de AWS.
3. Configure el cliente de Oracle en el host bastión para que tome la base de datos de copias de seguridad.
4. Cargue la copia de seguridad de la base de datos en un bucket de Amazon Simple Storage Service (Amazon S3).
5. Restaure la copia de seguridad de la base de datos de Amazon S3 en una base de datos de Amazon RDS para Oracle.
6. Configure Oracle GoldenGate para CDC.
7. Complete las actividades posteriores a la migración en la base de datos de destino.

Tools (Herramientas)

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Las herramientas nativas de Oracle lo ayudan a llevar a cabo una migración homogénea. Puede utilizar Oracle Data Pump para migrar datos entre las bases de datos de origen y destino. Este patrón utiliza Oracle Data Pump para realizar la carga completa desde la base de datos de origen a la base de datos de destino.
- Oracle le GoldenGate ayuda a realizar la replicación lógica entre dos o más bases de datos. Este patrón se utiliza GoldenGate para replicar los cambios delta después de la carga inicial mediante Oracle Data Pump.

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Cree documentos del proyecto y registre los detalles de la base de datos.	1. Documente sus objetivos de migración, los requisitos de migración, las principales partes interesadas del proyecto, los hitos del proyecto, los plazos del proyecto, las métricas clave, los riesgos de migración y los planes de mitigación de riesgos. 2. Documente la información crítica sobre su base de datos de origen, incluida la RAM, las IOPS y CPUs. Más adelante, utilizará esta información para determinar la instancia de base de datos de destino adecuada. 3. Valide las versiones de sus bases de datos de origen y destino.	Administrador de base de datos
Identifique los requisitos de almacenamiento.	Identifique y documente sus requisitos de almacenamiento, incluidos los siguientes: 1. Calcule el almacenamiento asignado para la instancia de la base de datos de origen.	DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
	2. Recopile las métricas de crecimiento históricas de la instancia de la base de datos de origen. 3. Pronostique el crecimiento futuro para la instancia de la base de datos objetivo. **Note** En el caso de los volúmenes SSD de uso general (gp2), se obtienen tres IOPS por cada 1 GB de almacenamiento. Para asignar el almacenamiento, calcule el número total de IOPS de lectura y escritura en la base de datos de origen.	

Tarea	Descripción	Habilidades requeridas
Elija el tipo de instancia adecuado en función de los requisitos de procesamiento.	1. Determine los requisitos de procesamiento de la instancia de base de datos de destino. 2. Identifique problemas de rendimiento. 3. Tenga en cuenta los factores para determinar el tipo de instancia adecuado: • Utilización de la CPU de la instancia de base de datos de origen • IOPS (lectura y escritura) para la instancia de base de datos de origen • Huella de memoria en la instancia de la base de datos de origen	SysAdmin
Identifique los requisitos de seguridad de acceso a la red.	1. Identifique y documente los requisitos de seguridad de acceso a la red para sus bases de datos de origen y destino. 2. Configure los grupos de seguridad adecuados para permitir que la aplicación se comunique con la base de datos.	DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
Identificar la estrategia de migración de aplicaciones.	1. Determine y documente la estrategia de transición a la migración. 2. Determine y documente el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO) y, a continuación, planifique la transición en consecuencia.	DBA, propietario de la SysAdmin aplicación

Tarea	Descripción	Habilidades requeridas
Identifique los riesgos de migración.	Evalúe la base de datos y documente los riesgos y mitigaciones específicos de la migración. Por ejemplo: • Identifique tablas sin registro y destaque el riesgo de pérdida de datos en caso de recuperación. • Extraiga los usuarios y privilegios de la base de datos de origen y destaque los conflictos con los privilegios de Amazon RDS. • Revise el registro de alertas para ver si hay errores o advertencias específicos de Oracle. • Identifique las caracterí sticas compatibles y no compatibles de la instancia de base de datos de destino. • Revise las características obsoletas del motor de la versión de base de datos de destino.	Administrador de base de datos

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	Cree una nueva Amazon Virtual Private Cloud (Amazon VPC) para la instancia de base de datos de destino.	SysAdmin
Cree grupos de seguridad.	Cree un grupo de seguridad en la nueva VPC para permitir las conexiones entrantes a la instancia de base de datos.	SysAdmin
Crear una instancia de base de datos de Amazon RDS para Oracle.	Cree la instancia de base de datos de destino con la nueva VPC y el nuevo grupo de seguridad y, a continuación, inicie la instancia.	SysAdmin

Opción 1: uso de herramientas nativas de Oracle o de terceros para migrar los datos

Tarea	Descripción	Habilidades requeridas
Prepare la base de datos de origen.	1. Cree un directorio de Data Pump o utilice uno existente. 2. Cree un usuario de migración y conceda permisos para realizar la extracción de Data Pump. 3. Extraiga los roles, los usuarios y los espacios de tabla de la base de datos de origen como un script SQL.	DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
	4. Transfiera el volcado de Data Pump extraído al directorio `data pump` de la instancia de la base de datos de destino.	

Tarea	Descripción	Habilidades requeridas
Prepare la base de datos de destino.	1. Confirme que todas las opciones de base de datos (por ejemplo, texto y Java) estén instaladas o habilitadas en la instancia de base de datos de Amazon RDS para Oracle. 2. Cree un directorio de Data Pump o utilice uno existente. 3. Cree un usuario de migración y conceda permisos para realizar la importación de Data Pump. 4. Cree los espacios de tabla, los usuarios y los roles necesarios en la instancia de base de datos de destino. 5. Importe el volcado de exportación de Data Pump transferido a la base de datos de destino. 6. Cree los índices excluidos durante la importación o la creación del objeto. 7. Cree cualquier restricción excluida durante la importación. 8. Valide o vuelva a compilar los objetos no válidos. 9. Reconstruya los índices no válidos.	DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
	10. Valide los recuentos de objetos de la base de datos entre las bases de datos de origen y destino. 11. Resuelva cualquier discrepancia que se encuentre entre los recuentos de objetos.	

Opción 2: uso de AWS DMS para migrar datos

Tarea	Descripción	Habilidades requeridas
Prepare los datos.	1. Limpie los datos de la base de datos de origen. 2. Cree una instancia de replicación. 3. Cree un punto de conexión de origen y un punto de conexión de destino. 4. Identifique el número de tablas y objetos que se van a migrar.	Administrador de base de datos
Migre los datos.	1. Elimine las restricciones y los disparadores de clave externa en la base de datos de destino. 2. Elimine los índices secundarios en la base de datos de destino. 3. Configure los ajustes de tareas de carga completa	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de AWS DMS desde la base de datos de origen a la base de datos de destino. 4. Habilite claves externas. 5. Permita que AWS DMS CDC replique los cambios en curso. 6. Active los desencade nadores. 7. Actualice las secuencias. 8. Valide los datos de origen y destino.	

Realizar la transición a la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Cambie los clientes de aplicaciones a la nueva infraestructura.	1. Detenga todos los servicios de aplicaciones y las conexiones de clientes que apunten a Oracle. 2. Ejecute las tareas de AWS DMS. 3. Configure una tarea de reversión (por ejemplo, revierta el CDC de la base de datos de Amazon RDS a la base de datos de Oracle en las instalaciones). 4. Valide los datos. 5. Inicie los servicios de la aplicación en la nueva	DBA, propietario de la SysAdmin aplicación

Tarea	Descripción	Habilidades requeridas
	base de datos de destino configurando Amazon Route 53 en la nueva instancia de base de datos de Amazon RDS para Oracle. 6. Añada la CloudWatch monitorización de Amazon a su nueva instancia de base de datos de Amazon RDS for Oracle.	
Implemente su plan de reversión.	1. Detenga todos los servicios de aplicaciones que apunten a la instancia de base de datos de Amazon RDS para Oracle. 2. Revierta los cambios en la base de datos de Oracle en las instalaciones de origen mediante una tarea de AWS DMS. 3. Detenga la ejecución de las tareas de AWS DMS desde la base de datos de Oracle en las instalaciones a la base de datos Amazon RDS para Oracle. 4. Vuelva a configurar las aplicaciones en la base de datos de Oracle de origen. 5. Confirme que se ha completado la implement ación de la reversión.	Administrador de base de datos, propietario de la aplicación

Cerrar el proyecto de migración

Tarea	Descripción	Habilidades requeridas
Limpiar recursos.	Cierre o elimine los recursos temporales de AWS, como la instancia de replicación de AWS DMS y el bucket de S3.	DBA, SysAdmin
Revise los documentos del proyecto.	Revise los documentos y objetivos de planificación de la migración y, a continuación, confirme que ha completado todos los pasos de migración necesarios.	DBA, propietario de la SysAdmin aplicación
Recopile métricas.	Registre las métricas clave de la migración, como el tiempo que se tardó en completar la migración, el porcentaje de tareas manuales en comparación con las tareas basadas en herramientas, el ahorro de costos y otras métricas relevantes.	DBA, propietario de la SysAdmin aplicación
Cerrar el proyecto.	Cierre el proyecto de migración y obtenga comentarios sobre el esfuerzo.	DBA, propietario de la SysAdmin aplicación

Recursos relacionados

Referencias

- Migrating Oracle databases to the AWS Cloud (Recomendaciones de AWS)
- AWS Database Migration Service (AWS DMS) (documentación de AWS DMS)
- Precios de Amazon RDS (documentación de Amazon RDS)

Tutoriales y videos

- Introducción a AWS Database Migration Service (AWS DMS) (documentación de AWS DMS)
- Recursos de Amazon RDS (documentación de Amazon RDS)
- AWS Database Migration Service (DMS) (YouTube)

Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump

Mohan Annam y Brian Motzer, Amazon Web Services

Resumen

Este patrón describe cómo migrar una base de datos de Oracle de un centro de datos en las instalaciones a una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para Oracle mediante Oracle Data Pump.

El patrón implica crear un archivo de volcado de datos a partir de la base de datos de origen, almacenar el archivo en un bucket de Amazon Simple Storage Service (Amazon S3) y, a continuación, restaurar los datos en una instancia de base de datos de Amazon RDS para Oracle. Este patrón resulta útil cuando se encuentra con limitaciones al utilizar AWS Database Migration Service (AWS DMS) para la migración.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Los permisos necesarios para crear roles en AWS Identity and Access Management (IAM) y para la carga multiparte a Amazon S3
- Los permisos necesarios para exportar datos desde la base de datos de origen
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada

Versiones de producto

- Oracle Data Pump solo está disponible para Oracle Database 10g, versión 1 (10.1) y versiones posteriores.

Arquitectura

Pila de tecnología de origen

- Bases de datos de Oracle en las instalaciones

Pila de tecnología de destino

- Amazon RDS para Oracle
- Cliente SQL (desarrollador de Oracle SQL)
- Un bucket de S3

Arquitectura de origen y destino

Tools (Herramientas)

Servicios de AWS

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos. En este patrón, la IAM se utiliza para crear los roles y políticas necesarios para migrar datos de Amazon S3 a Amazon RDS para Oracle.
- Amazon Relational Database Service (Amazon RDS) para Oracle le ayuda a configurar, utilizar y escalar una base de datos relacional de Oracle en la nube de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

- Oracle Data Pump le ayuda a trasladar datos y metadatos de una base de datos a otra a altas velocidades. En este patrón, Oracle Data Pump se utiliza para exportar el archivo de volcado de datos (.dmp) al servidor de Oracle e importarlo a Amazon RDS para Oracle. Para obtener más información, consulte Importación de datos a Oracle en Amazon RDS en la documentación de Amazon RDS.
- Oracle SQL Developer es un entorno de desarrollo integrado que simplifica el desarrollo y la administración de bases de datos de Oracle, tanto en implementaciones tradicionales como en implementaciones basadas en la nube. Interactúa con la base de datos de Oracle en las instalaciones y con Amazon RDS para Oracle para ejecutar los comandos SQL necesarios para exportar e importar datos.

Epics

Creación de un bucket de S3

Tarea	Descripción	Habilidades requeridas
Crear el bucket.	Para crear el bucket de S3, siga las instrucciones que figuran en la Documentación de AWS.	Administrador de sistemas de AWS

Crear el rol de IAM y asignar políticas

Tarea	Descripción	Habilidades requeridas
Configurar los permisos de IAM.	Para configurar los permisos, siga las instrucciones que figuran en la Documentación de AWS.	Administrador de sistemas de AWS

Crear la instancia de base de datos de Amazon RDS para Oracle y asociar el rol de integración de Amazon S3

Tarea	Descripción	Habilidades requeridas
Crear la instancia de la base de datos de destino de Amazon RDS para Oracle.	Para crear la instancia de Amazon RDS para Oracle, siga las instrucciones que figuran en la Documentación de AWS.	Administrador de sistemas de AWS
Asociar el rol con la instancia de base de datos.	Para asociar el rol a la instancia, siga las instrucciones que figuran en la Documentación de AWS.	Administrador de base de datos

Crear el usuario de la base de datos en la base de datos de destino

Tarea	Descripción	Habilidades requeridas

Cree el usuario.	Conectarse a la base de datos de destino de Amazon RDS para Oracle desde Oracle SQL Developer o SQL*Plus y ejecutar el siguiente comando SQL para crear el usuario al que importar el esquema.
	`create user SAMPLE_SCHEMA identified by <PASSWORD>;`
	`grant create session, resource to <USER NAME>;`
	`alter user <USER NAME> quota 100M on users;`
		Administrador de base de datos

Crear el archivo de exportación a partir de la base de datos de Oracle de origen

Tarea	Descripción	Habilidades requeridas

Crear un archivo de volcado de datos.	Para crear un archivo de volcado con el nombre `sample.dmp` indicado en el directorio `DATA_PUMP_DIR` para exportar al usuario `SAMPLE_SCHEMA` , utilice el siguiente script.
	`DECLARE`
	`  hdnl NUMBER;`
	`BEGIN`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	<pre> hdnl := dbms_data
	pump.open(operation
	 => 'EXPORT',
	
	          job_mode =>
	 'SCHEMA',
	
	          job_name =>
	 NULL);
	
	    dbms_datapump.add_
	file(handle => hdnl,
	
	         filename =>
	 'sample.dmp',
	
	       directory =>
	 'DATA_PUMP_DIR',
	
	         filetype =>
	 dbms_datapump.ku$_
	file_type_dump_file);
	
	    dbms_datapump.add_
	file(handle => hdnl,
	
	         filename =>
	 'export.log',
	
	       directory =>
	 'DATA_PUMP_DIR',
	
	         filetype =>
	 dbms_datapump.ku$_
	file_type_log_file);
	
	    dbms_datapump.meta
	data_filter(hdnl,
	 'SCHEMA_EXPR', 'IN
	 (''SAMPLE_SCHEMA''
	)');</pre>	

Tarea	Descripción	Habilidades requeridas

	`dbms_datapump.start_job(hdnl);`
	`END;`
	`/`
	
	Revise los detalles de la exportación revisando el archivo `export.log` en su directorio `DATA_PUMP_DIR` local.	

Cargue el archivo de volcado en el bucket de S3

Tarea	Descripción	Habilidades requeridas
Cargar el archivo de volcado de datos desde el origen hasta el bucket de S3.	Ejecute el siguiente comando utilizando AWS CLI. `aws s3 cp sample.dmp s3://<bucket_created_epic_1>/`	Administrador de base de datos

Descargar el archivo de exportación del bucket de S3 en la instancia de RDS

Tarea	Descripción	Habilidades requeridas
Descargar el archivo de volcado de datos en Amazon RDS	Para copiar el archivo de volcado `sample.dmp` desde el bucket de S3 hasta la base de datos de Amazon RDS para Oracle, ejecute el siguiente comando SQL. En este ejemplo, el archivo `sample.dmp` se descarga	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas

	del bucket de S3 `my-s3-integration1` al directorio de Oracle `DATA_PUMP_DIR`. Asegúrese de tener suficiente espacio en el disco asignado a la instancia de RDS para alojar tanto la base de datos como el archivo de exportación.
	
	`-- If you want to download all the files in the S3 bucket remove the p_s3_prefix line.`
	
	`SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(`
	`p_bucket_name => 'my-s3-integration',`
	`p_s3_prefix => 'sample.dmp',`
	`p_directory_name => 'DATA_PUMP_DIR')`
	`AS TASK_ID FROM DUAL;`
	
	El comando anterior genera un ID de tarea. Para revisar el estado de la descarga mediante la revisión de los datos en el ID de tarea, ejecute el siguiente comando.
	
	`SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','d`	

Tarea	Descripción	Habilidades requeridas

	`btask-<task_id>.log'));`
	
	Para ver los archivos en el directorio `DATA_PUMP_DIR`, ejecute el comando siguiente en el directorio.
	
	`SELECT filename, type,filesize/1024/1024 size_megs ,to_char(mtime,'DD-MON-YY HH24:MI:SS') timestamp FROM TABLE(rdsadmin.rds_file_util.listdir(p_directory => upper('DATA_PUMP_DIR'))) order by 4;`	

Importar el archivo de volcado a la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Restaurar el esquema y los datos en Amazon RDS.	Para importar el archivo de volcado al esquema de la base de datos `sample_schema`, ejecute el siguiente comando SQL desde SQL Developer o SQL*Plus. `DECLARE hdnl NUMBER; BEGIN`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	``
	hdnl := DBMS_DATA
	PUMP.OPEN(operation
	 => 'IMPORT', job_mode
	 => 'SCHEMA', job_name=
	>null);
	
	DBMS_DATAPUMP.ADD_
	FILE(handle => hdnl,
	 filename => 'sample.d
	mp', directory =>
	 'DATA_PUMP_DIR',
	 filetype => dbms_data
	pump.ku$_file_type
	_dump_file);
	
	DBMS_DATAPUMP.ADD_FILE
	(handle => hdnl,
	 filename => 'import.l
	og', directory =>
	 'DATA_PUMP_DIR',
	 filetype => dbms_data
	pump.ku$_file_type
	_log_file);
	
	DBMS_DATAPUMP.
	METADATA_FILTER(hd
	nl,'SCHEMA_EXPR','
	IN (''SAMPLE_SCHEMA''
	)');
	
	DBMS_DATAPUMP.START_J
	OB(hdnl);
	
	END;
	/
	``
	
	Para ver el archivo de registro de la importación, ejecute el siguiente comando.	

Tarea	Descripción	Habilidades requeridas
	`SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('DATA_PUMP_DIR','import.log'));`	

Eliminar el archivo de volcado del directorio DATA_PUMP_DIR

Tarea	Descripción	Habilidades requeridas

Enumerar y limpiar los archivos de exportación.	Para enumerar y eliminar los archivos de exportación en el directorio `DATA_PUMP_DIR` , ejecute los siguientes comandos.
	`-- List the files SELECT filename, type,filesize/1024/1024 size_megs ,to_char(mtime,'DD-MON-YY HH24:MI:SS') timestamp FROM TABLE(rdsadmin.rds_file_util.listdir(p_directory => upper('DATA_PUMP_DIR'))) order by 4;`
	`-- Remove the files EXEC UTL_FILE.FREMOVE('DATA_PUMP_DIR','sample.dmp'); EXEC UTL_FILE.FREMOVE('DATA_PUMP_DIR','import.log');`
		Administrador de sistemas de AWS

Recursos relacionados

- Integración de Amazon S3
- Crear una instancia de base de datos
- Importación de datos a Oracle en Amazon RDS
- Documentación de Amazon S3
- documentación de IAM
- Documentación de Amazon RDS
- Documentación de Oracle Data Pump
- Oracle SQL Developer

Migre de PostgreSQL en EC2 Amazon a Amazon RDS para PostgreSQL mediante pglogical

Rajesh Madiwale, Amazon Web Services

Resumen

Este patrón describe los pasos para migrar una base de datos PostgreSQL (versión 9.5 y posteriores) de Amazon Elastic Compute Cloud (Amazon) a Amazon Relational Database Service (EC2Amazon RDS) para PostgreSQL mediante la extensión pglogical de PostgreSQL. Amazon RDS ahora admite la extensión pglogical en la extensión para PostgreSQL versión 10.

Requisitos previos y limitaciones

Requisitos previos

- Elija el tipo correcto de instancia de Amazon RDS. Para obtener más información, consulte Tipos de instancia Amazon RDS.
- Asegúrese de que las versiones de origen y destino de PostgreSQL sean las mismas.
- Instale e integre la extensión pglogical con PostgreSQL en Amazon. EC2

Versiones de producto

- PostgreSQL versión 10 y posteriores en Amazon RDS, con las funciones compatibles con Amazon RDS (consulte PostgreSQL en Amazon RDS en la documentación de AWS). Este patrón se probó migrando PostgreSQL 9.5 a la versión 10 de PostgreSQL en Amazon RDS, pero también se aplica a versiones posteriores de PostgreSQL en Amazon RDS.

Arquitectura

Arquitectura de migración de datos

Tools (Herramientas)

- extensión pglogic
- Utilidades nativas de PostgreSQL: pg_dump y pg_restore

Epics

Migración de datos mediante la extensión pglogical

Tarea	Descripción	Habilidades requeridas
Crear una instancia de base de datos PostgreSQL en Amazon RDS.	Configurar una instancia de base de datos de Amazon RDS. Para obtener instrucciones, consulte la documentación de Amazon RDS para PostgreSQL.	Administrador de base de datos
Obtenga un volcado de esquema de la base de datos PostgreSQL de origen y restaúrelo en la base de datos PostgreSQL de destino.	1. Utilice la utilidad pg_dump con la opción `-s` de generar un archivo de esquema a partir de la base de datos de origen. 2. Utilice la utilidad psql con la opción `-f` de cargar el esquema en la base de datos de destino.	Administrador de base de datos
Habilita la decodificación lógica.	En el grupo de parámetros de base de datos de Amazon RDS, defina el parámetro estático `rds.logical_replication` como 1. Para obtener instrucciones, consulte la Documentación de Amazon RDS.	Administrador de base de datos
Cree la extensión pglogical en las bases de datos de origen y destino.	1. Cree la extensión `pglogical` en la base de datos PostgreSQL de origen:	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

	`psql -h <amazon-ec2-endpoint> -d target-dbname -U target-dbuser -c "create extension pglogical ;"`
	2. Cree la extensión `pglogical` en la base de datos PostgreSQL de destino:
	`psql -h <amazon-rds-endpoint> -d source-dbname -U source-dbuser -c "create extension pglogical ;"`	

Cree un publicador en la base de datos PostgreSQL de origen.	Para crear un publicador, ejecute: `psql -d dbname -p 5432 <<EOF SELECT pglogical .create_n ode( node_name := 'provider1', dsn := 'host=<ec2-endpoint> port=5432 dbname=source-dbname user=source-dbuser' ); EOF`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

Cree un conjunto de réplicas, añada tablas y secuencias.	Para crear un conjunto de réplicas en la base de datos PostgreSQL de origen y añadir tablas y secuencias al conjunto de réplicas, ejecute:
	`psql -d dbname -p 5432 <<EOF`
	`SELECT pglogical.replication_set_add_all_tables('default', '{public}'::text[],synchronize_data := true);`
	`EOF`
		Administrador de base de datos

Cree un suscriptor.	Para crear un suscriptor en la base de datos PostgreSQL de destino, ejecute:
	`psql -h <rds-endpoint> -d target-dbname -U target-dbuser <<EOF`
	`SELECT pglogical.create_node(`
	`node_name := 'subscriber1',`
	`dsn := 'host=<rds-endpoint> port=5432 dbname=target-dbname password=postgres user=target-dbuser'`
	`);`
	`EOF`
		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree una suscripción.	Para crear una suscripción en la base de datos PostgreSQL de destino, ejecute: `psql -h <rds-endpoint> -d target -U postgres <<EOF SELECT pglogical.create_subscription( subscription_name := 'subscription1', replication_sets := array['default'], provider_dsn := 'host=<ec2-endpoint> port=5432 dbname=<source-dbname> password=<password> user=source-dbuser' );`	Administrador de base de datos

Validación de sus datos

Tarea	Descripción	Habilidades requeridas
Compruebe las bases de datos de origen y destino.	Compruebe las bases de datos de origen y destino para confirmar que los datos se están replicando correctamente. Puede realizar una validación básica utilizando las tablas `select count(1)` de origen y destino.	Administrador de base de datos

Recursos relacionados

- Amazon RDS
- Replicación lógica para PostgreSQL en Amazon RDS (documentación de Amazon RDS)
- pglogical (repositorio) GitHub
- Limitaciones de pglogical (archivo README del repositorio) GitHub
- Migración de PostgreSQL de un entorno local o de Amazon EC2 a Amazon RDS mediante la replicación lógica (blog de AWS Database)

Migración de una base de datos PostgreSQL en las instalaciones a Aurora PostgreSQL

Baji Shaik y Jitender Kumar, Amazon Web Services

Resumen

La edición Amazon Aurora compatible con PostgreSQL que combina el rendimiento y la disponibilidad de las bases de datos comerciales de gama alta con la simplicidad y la rentabilidad de las bases de datos de código abierto. Aurora ofrece estos beneficios al escalar el almacenamiento en tres zonas de disponibilidad en la misma región de AWS y admite hasta 15 instancias de réplica de lectura para escalar horizontalmente las cargas de trabajo de lectura y proporcionar alta disponibilidad en una sola región. Al utilizar una base de datos global Aurora, puede replicar las bases de datos PostgreSQL en hasta cinco regiones para el acceso remoto de lectura y la recuperación de desastres en caso de que se produzca un error en una región. Este patrón describe los pasos para migrar una base de datos de origen de PostgreSQL en las instalaciones a una base de datos de Aurora compatible con PostgreSQL. El patrón incluye dos opciones de migración: usar AWS Data Migration Service (AWS DMS) o usar herramientas nativas de PostgreSQL (como pg_dump, pg_restore y psql) o herramientas de terceros.

Los pasos descritos en este patrón también se aplican a las bases de datos PostgreSQL de destino en instancias de Amazon Relational Database Service (Amazon RDS) y Amazon Elastic Compute Cloud (Amazon). EC2

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Base de datos de origen de PostgreSQL en un centro de datos en las instalaciones.
- Una instancia de base de datos Aurora compatible con PostgreSQL o una instancia de base de datos de Amazon RDS para PostgreSQL.

Limitaciones

- Los límites de tamaño de la base de datos son 64 TB para Amazon RDS para PostgreSQL y 128 TB para Aurora compatible con PostgreSQL.
- Si utiliza la opción de migración a AWS DMS, consulte las Limitaciones del uso de una base de datos PostgreSQL como fuente de DMS.

Versiones de producto

- Para obtener información sobre el soporte de las versiones principal y secundaria de PostgreSQL en Amazon RDS, consulte Actualizaciones de Amazon RDS para PostgreSQL en la documentación de Amazon RDS.
- Para obtener información sobre la compatibilidad con PostgreSQL en Aurora, consulte Amazon Aurora PostgreSQL updates en la documentación de Aurora.
- Si utiliza la opción de migración a AWS DMS, consulte las versiones de PostgreSQL compatibles en la documentación de AWS DMS.

Arquitectura

Pila de tecnología de origen

- Base de datos PostgreSQL en las instalaciones

Pila de tecnología de destino

- Instancia de base de datos de Aurora compatible con PostgreSQL

Arquitectura de origen

Arquitectura de destino

Arquitectura de migración de datos

Uso de AWS DMS

Uso de herramientas nativas de PostgreSQL

Tools (Herramientas)

- AWS Database Migration Service (AWS DMS) le ayuda a migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en las instalaciones y en la nube. Este

servicio admite diferentes bases de datos de origen y destino. Para obtener información sobre cómo validar las versiones y ediciones de las bases de datos de origen y destino de PostgreSQL compatibles para su uso con AWS DMS, consulte Using a PostgreSQL database as an AWS DMS source. Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características.

- Entre las herramientas nativas de PostgreSQL, se incluyen pg_dump, pg_restore y psql.

Epics

Analice la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.	Si utiliza AWS DMS, asegúrese de que esté utilizando una versión compatible de PostgreSQL.	Administrador de base de datos
Identifique el tipo de almacenamiento y los requisitos de capacidad.	1. Calcule el almacenamiento asignado para la instancia de base de datos de origen. 2. Recopile las métricas de crecimiento históricas de la instancia de base de datos de origen. 3. Anticipe la previsión de crecimiento futuro de la instancia de base de datos de destino. 4. Calcule el número total de IOPS de lectura y escritura en la base de datos de origen para asignar el almacenamiento. Un volumen SSD de uso general (gp2) proporciona	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	3 IOPS por cada 1 GB de almacenamiento.	
Elija el tipo de instancia, la capacidad, las caracterí sticas de almacenamiento y las características de red adecuadas.	Determine los requisitos de procesamiento de la instancia de base de datos de destino. Revise los problemas de rendimiento conocidos que puedan necesitar más atención. Tenga en cuenta los siguientes factores para determinar el tipo de instancia adecuado: • Utilización de la CPU de la instancia de base de datos de origen • IOPS (operaciones de lectura y escritura) para la instancia de base de datos de origen • Huella de memoria en la instancia de base de datos de origen Para obtener más información, consulte Clases de instancia de base de datos de Aurora en la documentación de Aurora.	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Identifique los requisitos de seguridad de acceso a la red para las bases de datos de origen y destino.	Determine los grupos de seguridad adecuados que permitirían a la aplicación comunicarse con la base de datos.	Administrador de base de datos, administrador de sistemas
Identificar la estrategia de migración de aplicaciones.	• Determine la estrategia de transición de la migración en función de la complejidad de su aplicación. • Determine el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO) para la aplicación, y planifique la transición según correspon da.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	Cree una nueva nube privada virtual (VPC) para la instancia de base de datos de destino.	Administrador de sistemas
Cree grupos de seguridad.	Cree un grupo de seguridad dentro de la VPC (como se determinó en la epopeya anterior) para permitir las conexiones entrantes a la instancia de base de datos.	Administrador de sistemas
Configure e inicie el clúster de base de datos Aurora.	Cree la instancia de base de datos de destino con la nueva	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	VPC y el nuevo grupo de seguridad, e inicie la instancia.	

Migración de datos: opción 1 (con AWS DMS)

Tarea	Descripción	Habilidades requeridas
Complete los pasos previos a la migración.	1. Limpie los datos de la base de datos de origen. 2. Cree una instancia de replicación. 3. Cree puntos de conexión de origen y destino. 4. Identifique el número de tablas y objetos disponibles que se van a migrar.	Administrador de base de datos
Complete los pasos de migración.	1. Elimine las restricciones y los disparadores de clave externa en la base de datos de destino. 2. Elimine los índices secundarios en la base de datos de destino. 3. Utilice una tarea de carga completa para migrar los datos de la base de datos de origen a la de destino. 4. Habilite claves externas. 5. Si utiliza una migración instantánea y su aplicación requiere un tiempo de inactividad mínimo,	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	habilite la captura de datos de cambios (CDC) para replicar los cambios en curso 6. Active los desencade nadores. 7. Actualice las secuencias. 8. Valide los datos de origen y destino.	
Valide los datos.	Para asegurarse de que los datos se migraron con precisión del origen al destino, siga los pasos de validación de datos de la documentación de AWS DMS.	Administrador de base de datos

Migración de datos: opción 2 (con pg_dump y pg_restore)

Tarea	Descripción	Habilidades requeridas
Prepare la base de datos de origen.	1. Cree un directorio para almacenar la copia de seguridad de pg_dump si aún no existe. 2. Cree un usuario de migración que tenga permisos para ejecutar pg_dump en los objetos de la base de datos. 3. Conéctese a la EC2 instancia y ejecute pg_dump backup.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte la documentación de pg_dump y el tutorial en la documentación de AWS DMS.	
Prepare la base de datos de destino.	1. Cree un usuario de migración que tenga permisos para usar pg_restore en los objetos de la base de datos. 2. Importe el volcado de la base de datos mediante pg_restore. Para obtener más información, consulte la documentación de pg_restore y el tutorial en la documentación de AWS DMS.	Administrador de base de datos
Valide los datos.	1. Compare los recuentos de objetos de la base de datos entre las bases de datos de origen y destino. 2. Resuelva cualquier discrepancia que se encuentre entre los recuentos de objetos.	Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de migración de aplicaciones.	Implemente la estrategia de migración de aplicaciones que creó en la primera epopeya.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Realizar la transición a la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Cambie los clientes de la aplicación a la nueva infraestructura.	1. Detenga todos los servicios de aplicaciones y las conexiones de cliente que apunten a la base de datos PostgreSQL en las instalaciones. 2. Ejecute las tareas de AWS DMS. 3. Configure una tarea de reversión (cambie el CDC de la base de datos de Aurora compatible con PostgreSQL a la base de datos PostgreSQL en las instalaciones) si es necesario. 4. Valide los datos. 5. Para iniciar los servicios de la aplicación en el nuevo destino, configure Amazon Route 53 en la nueva instancia de base de datos	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	de Aurora compatible con PostgreSQL. 6. Añada la supervisión de Amazon CloudWatch y Performance Insights a su nueva instancia de base de datos Aurora compatible con PostgreSQL.	

Tarea	Descripción	Habilidades requeridas
Si necesita revertir la migración, haga lo siguiente.	1. Detenga todos los servicios de aplicaciones que apuntan a la base de datos de Aurora compatible con PostgreSQL. 2. Revierta los cambios en la base de datos PostgreSQL en las instalaciones de origen mediante la tarea de AWS DMS que creó en la historia anterior. 3. Detenga la ejecución de las tareas de AWS DMS desde la base de datos PostgreSQL en las instalaciones a la base de datos de Aurora compatible con PostgreSQL. 4. Configure la aplicación para que apunte de nuevo a la base de datos PostgreSQL en las instalaciones de origen. 5. Confirme que se haya completado toda la implementación de la reversión.	Administrador de base de datos, propietario de la aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cierre los recursos.	Cerrar los recursos temporales de AWS.	Administrador de base de datos, administrador de sistemas
Valide los documentos.	Revise y valide los documentos del proyecto.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Recopile métricas.	Recopile métricas sobre el tiempo de migración, el porcentaje de ahorro de costos manuales en comparación con los de herramientas, etc.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Cierre el proyecto.	Cierre el proyecto y envíe sus comentarios.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Recursos relacionados

Referencias

- AWS Data Migration Service
- VPCs y Amazon Aurora
- Precios de Amazon Aurora
- Using a PostgreSQL database as an AWS DMS source
- How to create an AWS DMS replication instance
- How to create source and target endpoints using AWS DMS

Recursos adicionales

- Introducción a AWS DMS
- step-by-stepTutoriales sobre la migración de datos
- Recursos de Amazon Aurora

Migre una base de datos local de Microsoft SQL Server a Microsoft SQL Server en Amazon EC2 con Linux

Tirumala Dasari, Amazon Web Services

Resumen

Este patrón describe cómo migrar de una base de datos local de Microsoft SQL Server que se ejecuta en Microsoft Windows a Microsoft SQL Server en una instancia Linux de Amazon Elastic Compute Cloud (Amazon EC2) mediante utilidades de copia de seguridad y restauración.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- AMI de Amazon EC2 Linux (Amazon Machine Image) con Microsoft SQL Server
- AWS Direct Connect entre Windows local y Microsoft SQL Server en la instancia de Linux EC2

Arquitectura

Pila de tecnología de origen

- Base de datos de Microsoft SQL Server en las instalaciones

Pila de tecnología de destino

- EC2 Instancia de Linux con una base de datos de Microsoft SQL Server

Arquitectura de migración de base de datos

Tools (Herramientas)

- WinSCP: esta herramienta permite a los usuarios de Windows compartir archivos fácilmente con los usuarios de Linux.
- Sqlcmd: esta utilidad de línea de comandos le permite enviar expresiones o lotes de T-SQL a instancias locales y remotas de SQL Server. La utilidad es extremadamente útil para tareas repetitivas de bases de datos, como el procesamiento por lotes o las pruebas unitarias.

Epics

Prepare la instancia de EC2 Linux con SQL Server

Tarea	Descripción	Habilidades requeridas
Seleccione una AMI que proporcione el sistema operativo Linux e incluya Microsoft SQL Server.		Sysadmin
Configure la AMI para crear una EC2 instancia.		Sysadmin
Cree reglas de entrada y de salida para los grupos de seguridad.		Sysadmin
Configure la EC2 instancia de Linux para una base de datos de Microsoft SQL Server.		Administrador de base de datos
Cree usuarios y proporcione permisos como en la base de datos de origen.		Appowner, Administrador de base de datos
Instale las herramientas de SQL Server y la utilidad sqlcmd en la instancia de Linux. EC2		Administrador de base de datos

Haga una copia de seguridad de la base de datos y mueva el archivo de copia de seguridad a la instancia de Linux EC2

Tarea	Descripción	Habilidades requeridas
Realice una copia de seguridad de la base de datos		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
de SQL Server en las instalaciones.		
Instale WinSCP en Microsoft SQL Server.		Administrador de base de datos
Mueva el archivo de respaldo a la EC2 instancia de Linux que ejecuta Microsoft SQL Server.		Administrador de base de datos

Restaure la base de datos en una EC2 instancia de Linux que ejecute SQL Server

Tarea	Descripción	Habilidades requeridas
Restaure la base de datos desde el archivo de copia de seguridad de la base de datos mediante la utilidad sqlcmd.		Administrador de base de datos
Valide los objetos y datos de la base de datos.		Desarrollador, ingeniero de pruebas

Cambie de una instancia de Windows SQL Server a una EC2 instancia de Windows SQL Server en Linux

Tarea	Descripción	Habilidades requeridas
Valide los objetos y datos de la base de datos.		Desarrollador, ingeniero de pruebas
Pase de la base de datos local de Microsoft SQL Server a la EC2 instancia de Linux que ejecuta Microsoft SQL Server.		Administrador de base de datos

Recursos relacionados

- Cómo configurar SQL Server 2017 en Amazon Linux y Ubuntu AMIs
- Instalación de herramientas SQL en una instancia de Linux
- Backup y restauración desde una base de datos de Microsoft SQL Server local a Microsoft SQL Server en una instancia de Linux EC2

Migración de bases de datos en las instalaciones de Microsoft SQL Server a Amazon RDS para SQL Server mediante servidores vinculados

Kevin Yung, Viqash Adwani y Vishal Singh, Amazon Web Services

Resumen

Los servidores vinculados permiten a Microsoft SQL Server ejecutar expresiones SQL en otras instancias de servidores de bases de datos. Este patrón describe cómo puede migrar su base de datos en las instalaciones de Microsoft SQL Server a Amazon Relational Database Service (Amazon RDS) para Microsoft SQL Server a fin de reducir los costos y aumentar la disponibilidad. En la actualidad, Amazon RDS para Microsoft SQL Server no admite conexiones fuera de una red de Amazon Virtual Private Cloud (Amazon VPC).

Puede utilizar este patrón para lograr los siguientes objetivos:

- Migrar Microsoft SQL Server a Amazon RDS para Microsoft SQL Server sin interrumpir las capacidades del servidor vinculado.
- Priorizar y migrar Microsoft SQL Server vinculado en diferentes oleadas.

Requisitos previos y limitaciones

Requisitos previos

- Compruebe si Microsoft SQL Server en Amazon RDS admite las características que necesita.
- Asegúrese de que puede utilizar Amazon RDS para Microsoft SQL Server con las intercalaciones predeterminadas o las intercalaciones configuradas en los niveles de la base de datos.

Arquitectura

Pila de tecnología de origen

- Base de datos en las instalaciones (Microsoft SQL Server)

Pila de tecnología de destino

- Amazon RDS para SQL Server

Arquitectura de estado de origen

Arquitectura de estado de destino

En el estado de destino, se migra Microsoft SQL Server a Amazon RDS para Microsoft SQL Server mediante servidores vinculados. Esta arquitectura utiliza un Equilibrador de carga de red para enviar por proxy el tráfico de Amazon RDS para Microsoft SQL Server a los servidores en las instalaciones que ejecutan Microsoft SQL Server. El siguiente diagrama muestra la capacidad de proxy inverso del Equilibrador de carga de red.

Tools (Herramientas)

- AWS CloudFormation
- Equilibrador de carga de red
- Amazon RDS for SQL Server en varias zonas de disponibilidad (múltiplesAZs)
- AWS Database Migration Service (AWS DMS)

Epics

Crear una VPC de zona de aterrizaje

Tarea	Descripción	Habilidades requeridas
Cree la asignación del CIDR.		AWS SysAdmin
Cree una nube privada virtual (VPC).		AWS SysAdmin

Tarea	Descripción	Habilidades requeridas
Cree las redes de la VPC.		AWS SysAdmin
Cree las listas de control de acceso a la subred (ACLs).		AWS SysAdmin
Cree las rutas de enrutamie nto de subred.		AWS SysAdmin
Cree una conexión con AWS Direct Connect o una red privada virtual (VPN) de AWS.		AWS SysAdmin

Migración de una base de datos a Amazon RDS

Tarea	Descripción	Habilidades requeridas
Cree una instancia de base de datos de Amazon RDS para Microsoft SQL Server.		AWS SysAdmin
Cree una instancia de replicaci ón de AWS DMS.		AWS SysAdmin
Cree puntos de conexión de bases de datos de origen y de destino en AWS DMS.		AWS SysAdmin
Cree la tarea de migración y active la replicación continua después de una carga completa.		AWS SysAdmin
Solicite un cambio de firewall para permitir que Amazon RDS para Microsoft SQL Server acceda a las bases de		AWS SysAdmin

Tarea	Descripción	Habilidades requeridas
datos de SQL Server en las instalaciones.		
Crear un equilibrador de carga de red.		AWS SysAdmin
Cree un grupo de destino que se dirija a los servidores de bases de datos de su centro de datos	Le recomendamos que utilice nombres de host en la configuración de destino para incorporar los eventos de conmutación por error del centro de datos (DC).	AWS SysAdmin
Ejecute la expresión SQL para la configuración del servidor vinculado.	Ejecute las expresiones SQL para añadir un servidor vinculado mediante la herramienta de administr ación de Microsoft SQL en la instancia de base de datos Amazon RDS para Microsoft SQL Server. En la expresión SQL, configure @datasrc para que utilice el nombre de host de Equilibrador de carga de red. Añada credencia les de inicio de sesión de servidor vinculado mediante la herramienta de administr ación de Microsoft SQL en la instancia de base de datos Amazon RDS para Microsoft SQL Server.	AWS SysAdmin
Pruebe y valide las funciones de SQL Server.		AWS SysAdmin

Tarea	Descripción	Habilidades requeridas
Cree una transición.		AWS SysAdmin

Recursos relacionados

- Tareas de administración frecuentes para Microsoft SQL Server en Amazon RDS
- Intercalaciones y conjuntos de caracteres para Microsoft SQL Server
- Documentación del Equilibrador de carga de red
- Implementación de servidores vinculados con Amazon RDS para Microsoft SQL Server (entrada del blog)

Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server mediante métodos nativos de copia de seguridad y restauración

Tirumala Dasari, David Queiroz y Vishal Singh, Amazon Web Services

Resumen

Este patrón describe cómo migrar una base de datos de Microsoft SQL Server en las instalaciones a una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para SQL Server (migración homogénea). El proceso de migración se basa en los métodos nativos de copia de seguridad y restauración de SQL Server. Utiliza SQL Server Management Studio (SSMS) para crear un archivo de copia de seguridad de la base de datos y un bucket de Amazon Simple Storage Service (Amazon S3) para almacenar el archivo de copia de seguridad antes de restaurarlo en Amazon RDS para SQL Server.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Políticas de rol de AWS Identity and Access Management (IAM) para el acceso al bucket de S3 y a la instancia de base de datos de Amazon RDS para SQL Server.

Limitaciones

- El proceso descrito en este patrón migra solo la base de datos. Los inicios de sesión de SQL o los usuarios de bases de datos, incluidos los trabajos de SQL Server Agent, no se migran porque requieren pasos adicionales.

Versiones de producto

- SQL Server 2012-2017. Para ver la lista actualizada de versiones compatibles, consulte MySQL en Amazon RDS en la documentación de AWS.

Arquitectura

Pila de tecnología de origen

- Base de datos de Microsoft SQL Server en las instalaciones

Pila de tecnología de destino

- Instancia de base de datos de Amazon RDS para SQL Server

Arquitectura de migración de datos

Tools (Herramientas)

- Microsoft SQL Server Management Studio (SSMS) es un entorno integrado para administrar infraestructuras de SQL Server. Proporciona una interfaz de usuario y un grupo de herramientas con editores de scripts enriquecidos que interactúan con SQL Server.

Epics

Cree una instancia de base de datos de Amazon RDS para SQL Server

Tarea	Descripción	Habilidades requeridas
Seleccione SQL Server como motor de base de datos en Amazon RDS para SQL Server.		Administrador de base de datos
Seleccione SQL Server Express Edition.		Administrador de base de datos
Especifique los detalles de la base de datos.	Para obtener más informaci ón acerca de cómo crear una instancia de base de datos, consulte la documentación de Amazon RDS.	Administrador de base de datos, propietario de la aplicación

Cree un archivo de copia de seguridad a partir de la base de datos de SQL Server en las instalaciones

Tarea	Descripción	Habilidades requeridas
Conéctese a la base de datos de SQL Server en las instalaciones mediante SSMS.		Administrador de base de datos
Cree una copia de seguridad de la base de datos.	Para obtener instrucciones, consulte la documentación de SSMS.	Administrador de base de datos, propietario de la aplicación

Cargue el archivo de copia de seguridad en Amazon S3

Tarea	Descripción	Habilidades requeridas
Cree un bucket de Amazon S3.	Para obtener más información, consulte la documentación de Amazon S3.	Administrador de base de datos
Cargue el archivo de copia de seguridad en el bucket de S3.	Para obtener más información, consulte la documentación de Amazon S3.	SysOps administrador

Restaure la base de datos en Amazon RDS para SQL Server

Tarea	Descripción	Habilidades requeridas
Añada el grupo de opciones a Amazon RDS.	1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/. 2. En el panel de navegación, elija Option grupos (Grupos de opciones), Create gropu (Crear grupo).	SysOps administrador

Tarea	Descripción	Habilidades requeridas
	3. Complete la información del grupo de opciones y, a continuación, seleccione Create (Crear). 4. Añada la opción `SQLSERVER_BACKUP_RESTORE` al grupo de opciones y, a continuación, elija Add option (Añadir opción). Para obtener más información, consulte la documentación de Amazon RDS.	
Restaure la base de datos.	1. Conéctese a Amazon RDS para SQL Server mediante SSMS. 2. Para restaurar la base de datos, llame al procedimiento almacenado `msdb.dbo.rds_restore_database` .	Administrador de base de datos

Valide la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Valide los objetos y los datos.	Valide los objetos y los datos entre la base de datos de origen y Amazon RDS para SQL Server.	Administrador de base de datos, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	Note Esta tarea solo migra la base de datos. Los inicios de sesión y los trabajos no se migrarán.	

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Redirija el tráfico de la aplicación.	Tras la validación, redirija el tráfico de la aplicación a la instancia de base de datos Amazon RDS para SQL Server.	Administrador de base de datos, propietario de la aplicación

Recursos relacionados

- Documentación de Amazon S3
- Documentación de Amazon RDS para SQL Server
- Opciones para el motor de base de datos de Microsoft SQL Server

Migración de una base de datos de Microsoft SQL Server a Aurora MySQL mediante AWS DMS y AWS SCT

Mark Szalkiewicz y Pavan Pusuluri, Amazon Web Services

Resumen

Este patrón describe cómo migrar una base de datos de Microsoft SQL Server que se encuentra en las instalaciones o en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) a Amazon Aurora MySQL. Este patrón utiliza AWS Database Migration Service (AWS DMS) y Herramienta de conversión de esquemas de AWS (AWS SCT) para la migración de datos y la conversión de esquemas.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de origen de Microsoft SQL Server en un centro de datos local o en una instancia EC2
- Controladores de conectividad de bases de datos Java (JDBC) para conectores SCT de AWS, instalados en una máquina local o en una instancia en la EC2 que esté instalado AWS SCT

Limitaciones

- Límite de tamaño de la base de datos: 64 TB

Versiones de producto

- Versiones de Microsoft SQL Server 2008, 2008R2, 2012, 2014, 2016 y 2017 para las ediciones Enterprise, Standard, Workgroup y Developer. Las ediciones Web y Express no son compatibles con AWS DMS. Para ver la lista actualizada de versiones compatibles, consulte Using a Microsoft SQL Server Database as a Source for AWS DMS (Usar una base de datos de Microsoft SQL Server como fuente de AWS DMS). Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características. Para obtener información sobre las versiones de Microsoft SQL Server compatibles con AWS SCT, consulte la documentación de AWS SCT.

- Versiones de MySQL 5.5, 5.6 y 5.7. Para ver la lista actualizada de versiones compatibles, consulte Using a MySQL-Compatible Database as a Target for AWS DMS (Usar una base de datos compatible con MySQL como destino para AWS DMS).

Arquitectura

Pila de tecnología de origen

Uno de los siguientes:

- Base de datos de Microsoft SQL Server en las instalaciones
- Una base de datos de Microsoft SQL Server en una EC2 instancia

Pila de tecnología de destino

- Aurora MySQL

Arquitectura de migración de datos

- Desde una base de datos de Microsoft SQL Server que se ejecute en la nube de AWS

- Una base de datos de Microsoft SQL Server que se ejecute en un centro de datos en las instalaciones

Tools (Herramientas)

- AWS DMS: AWS Data Migration Service (AWS DMS) le permite migrar datos hacia y desde bases de datos comerciales y de código abierto muy utilizadas, incluidas Oracle, SQL Server, MySQL y PostgreSQL. Puede utilizar AWS DMS para migrar datos a la nube de AWS, entre instancias en las instalaciones (a través de una configuración de nube de AWS) o entre combinaciones de configuraciones en las instalaciones y en la nube.
- AWS SCT: La Herramienta de conversión de esquemas de AWS (AWS SCT) gestiona las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base

de datos de origen y la mayor parte del código personalizado a un formato compatible con la base de datos de destino.

Epics

Preparación para la migración

Tarea	Descripción	Habilidades requeridas
Valide la versión y el motor de la base de datos de origen y de destino.		Administrador de base de datos
Cree un grupo de seguridad saliente para las bases de datos de origen y destino.		SysAdmin
Cree y configure una EC2 instancia para AWS SCT, si es necesario.		Administrador de base de datos
Descargue la versión más reciente de AWS SCT y los controladores asociados.		Administrador de base de datos
Agregue y valide los usuarios y permisos de los requisitos previos en la base de datos de origen.		Administrador de base de datos
Cree un proyecto de AWS SCT para la carga de trabajo y conéctese a la base de datos de origen.		Administrador de base de datos
Genere un informe de evaluación y evalúe la viabilidad.		Administrador de base de datos

Prepare la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Cree una instancia de base de datos de Amazon RDS de destino con Amazon Aurora como motor de base de datos.		Administrador de base de datos
Extraiga la lista de usuarios, roles y permisos del origen.		Administrador de base de datos
Asigne los usuarios existente s de la base de datos a los nuevos usuarios de la base de datos.		Propietario de la aplicación
Cree usuarios en la base de datos de destino.		Administrador de base de datos
Aplique los roles del paso anterior a la base de datos de destino.		Administrador de base de datos
Revise las opciones, los parámetros, los archivos de red y los enlaces de la base de datos de origen y, a continuación, evalúe su aplicabilidad a la base de datos de destino.		Administrador de base de datos
Aplique cualquier configura ción pertinente al destino.		Administrador de base de datos

Transferir objetos

Tarea	Descripción	Habilidades requeridas
Configure la conectividad de AWS SCT con la base de datos de destino.		Administrador de base de datos
Convierta el esquema con AWS SCT.	AWS SCT convierte automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado a un formato compatible con la base de datos de destino. Cualquier código que la herramienta no pueda convertir automáticamente está claramente marcado para que pueda convertirlo usted mismo.	Administrador de base de datos
Revise el informe SQL generado y guarde los errores y advertencias.		Administrador de base de datos
Aplique los cambios de esquema automatizados al destino o guárdelos como un archivo .sql.		Administrador de base de datos
Valide que AWS SCT haya creado los objetos en el destino.		Administrador de base de datos
Reescriba, rechace o rediseñe manualmente cualquier elemento que no se haya		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
podido convertir automátic amente.		
Aplique los permisos de rol y de usuario generados y revise cualquier excepción.		Administrador de base de datos

Migración de datos

Tarea	Descripción	Habilidades requeridas
Determine el método de migración.		Administrador de base de datos
Cree una instancia de replicaci ón desde la consola de AWS DMS.	Para obtener más informaci ón sobre el uso de AWS DMS, consulte los enlaces de la sección “Recursos relaciona dos”.	Administrador de base de datos
Cree los puntos de conexión de origen y de destino.		Administrador de base de datos
Cree una tarea de replicación.		Administrador de base de datos
Inicie la tarea de replicación y supervise los registros.		Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Utilice AWS SCT para analizar y convertir los elementos de	Al convertir su esquema de base de datos de un	Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
SQL del código de la aplicación.	motor a otro, también deberá actualizar el código SQL de las aplicaciones para interactuar con el nuevo motor de base de datos en lugar del antiguo. Puede ver, analizar, editar y guardar el código SQL convertido. Para obtener más información sobre el uso de AWS SCT, consulte los enlaces de la sección “Recursos relacionados”.	
Cree los nuevos servidores de aplicaciones en AWS.		Propietario de la aplicación
Migre el código de la aplicación a los nuevos servidores.		Propietario de la aplicación
Configure el servidor de aplicaciones para los controladores y la base de datos de destino.		Propietario de la aplicación
Corrija cualquier código específico del motor de base de datos de origen de la aplicación.		Propietario de la aplicación
Optimice el código de la aplicación para el motor de destino.		Propietario de la aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Aplique al destino los nuevos usuarios, los permisos y los cambios de código.		Administrador de base de datos
Bloquee la aplicación para cualquier cambio.		Propietario de la aplicación
Valide que todos los cambios se hayan propagado a la base de datos de destino.		Administrador de base de datos
Apunte el nuevo servidor de la aplicación hacia la base de datos de destino.		Propietario de la aplicación
Vuelva a comprobar todo.		Propietario de la aplicación
Realice la puesta en marcha.		Propietario de la aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cierre los recursos temporales de AWS (la instancia de replicación de AWS DMS y la EC2 instancia utilizada para AWS SCT).		Administrador de base de datos, propietario de la aplicación
Actualice los comentarios sobre el proceso de AWS DMS para los equipos internos.		Administrador de base de datos, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Revise el proceso de AWS DMS y mejore la plantilla si es necesario.		Administrador de base de datos, propietario de la aplicación
Revise y valide los documento s del proyecto.		Administrador de base de datos, propietario de la aplicación
Recopile métricas sobre el tiempo de migración , el porcentaje de ahorro de costos manuales en comparación con los de herramientas, etc.		Administrador de base de datos, propietario de la aplicación
Cierre el proyecto y envíe sus comentarios.		Administrador de base de datos, propietario de la aplicación

Recursos relacionados

Referencias

- Guía del usuario de AWS DMS
- Guía del usuario de AWS SCT
- Precios de Amazon Aurora

Tutoriales y videos

- Getting Started with AWS Database Migration Service (AWS DMS) (Introducción a AWS Database Migration Service (AWS DMS))
- Introducción a la Herramienta de conversión de esquemas de AWS
- Recursos de Amazon RDS
- Tutoriales de AWS DMS Step-by-Step

Migración de una base de datos de MariaDB en las instalaciones hasta Amazon RDS para MariaDB mediante herramientas nativas

Shyam Sunder Rakhecha, Amazon Web Services

Resumen

Este patrón proporciona una guía para migrar una base de datos de MariaDB en las instalaciones a Amazon Relational Database Service (Amazon RDS) para MariaDB mediante herramientas nativas. Si tiene instaladas las herramientas de MySQL, puede utilizar mysql y mysqldump. Si tiene instaladas todas las herramientas de MariaDB, puede utilizar mariadb y mariadb-dump. Las herramientas MySQL y MariaDB tienen el mismo origen, pero hay pequeñas diferencias en la versión 10.6 de MariaDB y las posteriores.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de origen MariaDB en un centro de datos en las instalaciones

Limitaciones

- Límite de tamaño de la base de datos: 64 TB

Versiones de producto

- MariaDB, versiones 10.0-10.6 (para ver la lista actualizada de versiones compatibles, consulte MariaDB en Amazon RDS en la documentación de AWS)

Arquitectura

Pila de tecnología de origen

- Base de datos MariaDB en un centro de datos en las instalaciones

Pila de tecnología de destino

- Instancia de base de datos Amazon RDS para MariaDB

Arquitectura de destino

Arquitectura de migración de datos

Tools (Herramientas)

- Herramientas nativas de MySQL: mysql y mysqldump
- Herramientas nativas de MariaDB: mariadb y mariadb-dump

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Validar versiones y motores de las bases de datos de origen y destino.		Administrador de base de datos
Identifique los requisitos de hardware de la instancia del servidor de destino.		Administrador de base de datos, administrador de sistemas
Identifique los requisitos de almacenamiento (como el tipo y la capacidad de almacenamiento).		Administrador de base de datos, administrador de sistemas
Elija el tipo de instancia adecuado en función de la capacidad, las características de almacenamiento y las características de red.		Administrador de base de datos, administrador de sistemas
Identificar los requisitos de seguridad del acceso a la red		Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
para las bases de datos de origen y destino.		
Identificar la estrategia de migración de aplicaciones.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).		Administrador de sistemas
Cree grupos de seguridad.		Administrador de sistemas
Configurar e iniciar una instancia de base de datos de Amazon RDS que ejecute MariaDB.		Administrador de sistemas

Migración de datos

Tarea	Descripción	Habilidades requeridas
Utilizar herramientas nativas para migrar objetos y datos de las bases de datos.	En la base de datos de origen, utilice mysqldump o mariadb-dump para crear un archivo de salida que contenga objetos y datos de la base de datos. En la base de datos de destino, utilice mysql o mariadb para restaurar los datos.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Valide los datos.	Compruebe las bases de datos de origen y destino para confirmar que la migración de datos se ha realizado correctamente.	Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de migración de aplicaciones.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Cambie los clientes de la aplicación a la nueva infraestructura.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.		Administrador de sistemas
Revise y valide los documentos del proyecto.		Administrador de base de datos, propietario de la

Tarea	Descripción	Habilidades requeridas
		aplicación, administrador de sistemas
Recopilar métricas sobre tiempo de migración, ahorros de costos conseguidos con las herramientas, etc.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Cerrar el proyecto y enviar comentarios.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Recursos relacionados

Referencias de Amazon RDS

- Amazon RDS para MariaDB
- Amazon Virtual Private Cloud VPCs y Amazon RDS
- Implementaciones Multi-AZ de Amazon RDS
- Precios de Amazon RDS

Referencias de MySQL y MariaDB

- mariadb-dump/mysqldump
- mysql Command-line Client

Tutoriales y videos

- Introducción a Amazon RDS

Migración de una base de datos de MySQL en las instalaciones a Aurora MySQL

Igor Obradovic, Amazon Web Services

Resumen

En este patrón se explica cómo migrar una base de datos MySQL de origen en las instalaciones a la edición de Amazon Aurora compatible con MySQL. Describe dos opciones de migración: usar AWS Database Migration Service (AWS DMS) o usar herramientas nativas de MySQL, como mysqldbcopy y mysqldump.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Base de datos de origen MySQL en un centro de datos en las instalaciones

Limitaciones

- Límite de tamaño de la base de datos: 128 TB

Versiones de producto

- La versión 8.0 de MySQL (Aurora MySQL, versión 3) está disponible con el soporte estándar.
- La versión 5.7 de MySQL (Aurora MySQL, versión 2) está disponible con soporte extendido, por un costo adicional.

Para obtener la lista más reciente de versiones compatibles, consulte las versiones de Amazon Aurora en la AWS documentación. Si está utilizando AWS DMS, consulte también Uso de una base de datos compatible con MySQL como destino para las versiones de AWS DMS MySQL compatibles con. AWS DMS

Arquitectura

Pila de tecnología de origen

- Una base de datos MySQL en las instalaciones

Pila de tecnología de destino

- Amazon Aurora MySQL-Compatible Edition

Arquitectura de destino

Los datos de Aurora se almacenan en un volumen de clúster, que es un volumen virtual único que utiliza unidades de estado sólido (SSDs). Un volumen de clúster se compone de copias de los datos repartidas entre tres zonas de disponibilidad de una sola región de AWS. Como los datos se replican automáticamente entre zonas de disponibilidad, tienen una larga duración y se reduce el riesgo de pérdida de datos.

Aurora divide automáticamente el volumen de base de datos en segmentos de 10 GB repartidos en varios discos. Cada fragmento de 10 GB del volumen de base de datos se replica de seis maneras entre tres zonas de disponibilidad. En el siguiente diagrama se muestra la relación entre el volumen del clúster, la instancia de base de datos de escritor y las instancias de base de datos de lector en un clúster de bases de datos de Aurora, así como la separación del almacenamiento y la capacidad de computación. Para obtener más información sobre esta arquitectura, consulte la documentación de Aurora y FAQ.

Arquitectura de migración de datos

Uso de AWS DMS:

El siguiente diagrama ilustra la migración de una base de datos MySQL local a un clúster compatible con Aurora MySQL en, mediante. Nube de AWS AWS DMS

Uso de herramientas MySQL nativas:

El siguiente diagrama ilustra la migración de una base de datos MySQL local a un clúster compatible con Aurora MySQL en el, Nube de AWS mediante herramientas nativas de MySQL, como mysqldbcopy y mysqldump.

Tools (Herramientas)

- AWS Database Migration ServiceAWS DMS() admite varios motores de bases de datos de origen y destino. Para obtener información sobre las bases de datos de origen y destino de

MySQL compatibles con AWS DMS, consulte Migración de bases de datos compatibles con MySQL a. AWS Le recomendamos que utilice la última versión de AWS DMS para obtener una compatibilidad más completa con las versiones y funciones.

- mysqldbcopy es una utilidad de MySQL que copia una base de datos MySQL que se encuentra en un solo servidor o en varios servidores.
- mysqldump es una utilidad de MySQL que crea un archivo de volcado desde una base de datos MySQL con fines de copia de seguridad o migración.

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Valide la versión y el motor.	Valide la versión y el motor de las bases de datos de origen y de destino.	Administrador de base de datos
Identifique los requisitos de hardware.	Identifique los requisitos de hardware de la instancia del servidor de destino.	Administrador de base de datos, administrador de sistemas
Identifique los requisitos de almacenamiento.	Identifique los requisitos de almacenamiento (como el tipo y la capacidad de almacenamiento).	Administrador de base de datos, administrador de sistemas
Seleccione el tipo de instancia.	Elija el tipo de instancia adecuado en función de los requisitos de computación, almacenamiento y red.	Administrador de base de datos, administrador de sistemas
Determine los requisitos de seguridad de acceso a la red.	Identifique los requisitos de seguridad de acceso a la red para las bases de datos de origen y destino.	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Determine la estrategia.	Identificar la estrategia de migración de aplicaciones.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).	Para obtener instrucciones, consulte Create a VPC en la documentación de Amazon Virtual Private Cloud (Amazon VPC).	Administrador de sistemas
Cree grupos de seguridad.	Para obtener instrucciones, consulte Create a security group for your VPC en la documentación de Amazon VPC.	Administrador de sistemas
Configure e inicie un clúster de base de datos compatibl e con Aurora MySQL en su Cuenta de AWS.	Para obtener instrucciones, consulte Creación de un clúster de base de datos de Amazon Aurora en la documentación de Aurora.	Administrador de sistemas

Migración de datos: opción 1

Tarea	Descripción	Habilidades requeridas
Utilice las herramien tas nativas de MySQL o herramientas de terceros para	Para obtener instrucciones, consulte la documentación de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
migrar los objetos y datos de la base de datos.	herramientas de MySQL como mysqldbcopy y mysqldump.	

Migración de datos: opción 2

Tarea	Descripción	Habilidades requeridas
Migre datos con AWS DMS.	Para obtener instrucciones, consulte Uso de una base de datos compatible con MySQL como fuente y Uso de una base de datos compatible con MySQL como destino en la documentación. AWS DMS	Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Siga la estrategia.	Seguir la estrategia de migración de aplicaciones.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Cambie los clientes de la aplicación.	Cambie los clientes de la aplicación para que se conecten al nuevo punto de conexión del clúster de Aurora.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cierre los recursos.	Cierre los recursos temporales. AWS	Administrador de base de datos, administrador de sistemas
Revise la documentación.	Revise y valide los documentos del proyecto.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Recopile métricas.	Reúna métricas sobre el tiempo de migración, el porcentaje de pasos manuales frente al uso de la herramienta, el ahorro de costos, etc.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Complete el proyecto de migración.	Cerrar el proyecto y enviar comentarios.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Recursos relacionados

Referencias

- Migrating data to Amazon Aurora MySQL DB cluster
- AWS DMS sitio web
- AWS DMS documentación
- Precios de Amazon Aurora
- Creación de un clúster de base de datos Aurora MySQL y conexión a él
- Amazon VPC y Amazon RDS
- Documentación de Amazon Aurora

Tutoriales y videos

- Cómo empezar con AWS DMS
- Introducción a Amazon Aurora

Migre bases de datos MySQL locales a Aurora MySQL mediante Percona, XtraBackup Amazon EFS y Amazon S3

Rohan Jamadagni, Udayasimha Theepireddy y Sajith Menon, Amazon Web Services

Resumen

Este patrón describe cómo migrar bases de datos MySQL locales de gran tamaño de manera eficiente a Amazon Aurora MySQL mediante XtraBackup Percona. Percona XtraBackup es una utilidad de copia de seguridad de código abierto y sin bloqueo para servidores basados en MySQL. El patrón muestra cómo utilizar Amazon Elastic File System (Amazon EFS) para reducir el tiempo de carga de la copia de seguridad en Amazon Simple Storage Service (Amazon S3) y restaurar la copia de seguridad en Amazon Aurora MySQL. El patrón también proporciona detalles sobre cómo realizar copias de seguridad incrementales de Percona para minimizar la cantidad de registros binarios que se aplicarán a la base de datos Aurora MySQL de destino.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Permisos para crear roles y políticas de AWS Identity and Access Management (IAM).
- Conectividad de red entre la base de datos MySQL en las instalaciones y la nube privada virtual (VPC) en AWS

Limitaciones

- Los servidores de origen deben ser sistemas basados en Linux que puedan instalar un cliente de Network File System (NFS) (nfs-utils/nfs-common).
- El bucket de S3 utilizado para cargar los archivos de copia de seguridad solo admite el cifrado del servidor (SSE-S3/SSE-KMS).
- Amazon S3 limita el tamaño de los archivos de copia de seguridad a 5 TB. Si el archivo de copia de seguridad supera los 5 TB, puede dividirlo en varios archivos más pequeños.
- El número de archivos de origen cargados en un bucket de S3 se limita a un millón de archivos.
- El patrón solo admite la copia de seguridad completa y la copia de seguridad incremental de Percona XtraBackup . No admite copias de seguridad parciales que utilicen `--tables`, `--tables-exclude`, `--tables-file`, `--databases`, `--databases-exclude` o `--databases-file`.

- Aurora no restaura los usuarios, las funciones, los procedimientos almacenados ni la información de zona horaria de la base de datos MySQL de origen.

Versiones de producto

- La base de datos de origen debe ser MySQL versión 5.5, 5.6 o 5.7.
- Para MySQL 5.7, debe usar Percona XtraBackup 2.4.
- Para MySQL 5.6 y 5.6, debe usar Percona XtraBackup 2.3 o 2.4.

Arquitectura

Pila de tecnología de origen

- Sistema operativo basado en Linux
- Servidor de MySQL
- Percona XtraBackup

Pila de tecnología de destino

- Amazon Aurora
- Amazon S3
- Amazon EFS

Arquitectura de destino

Tools (Herramientas)

Servicios de AWS

- Amazon Aurora es un motor de base de datos relacional completamente administrado que simplifica y hace rentable configurar, usar y escalar las implementaciones de MySQL. Aurora MySQL es un sustituto directo de MySQL.
- Amazon Elastic File System (Amazon EFS) le ayuda a crear y configurar sistemas de archivos compartidos en la nube de AWS.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

- Percona XtraBackup es una utilidad de código abierto que realiza copias de seguridad en streaming, comprimidas e incrementales de bases de datos MySQL sin interrumpir ni bloquear sus bases de datos.

Epics

Crear un sistema de archivos de Amazon EFS

Tarea	Descripción	Habilidades requeridas
Cree un grupo de seguridad para asociarlo a los objetivos de montaje de Amazon EFS.	Cree un grupo de seguridad en la VPC que esté configurado con un adjunto de VPN a la base de datos en las instalaciones a través de AWS Transit Gateway. Para obtener más información sobre los comandos y los pasos descritos en este y otros artículos, consulte la sección «Recursos relacionados» al final de este patrón.	DevOps/database Administrador de AWS
Edite las reglas del grupo de seguridad.	Agregue una regla de entrada utilizando el tipo NFS, el puerto 2049 y el rango de IP del servidor de base de datos en las instalaciones como fuente. De forma predeterminada, la regla de salida permite salir a todo el tráfico. Si no es así, añada una regla	DevOps/database Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	de salida para abrir una conexión para el puerto NFS. Añada dos reglas de entrada más: el puerto 2049 (fuente: ID de grupo de seguridad del mismo grupo de seguridad) y el puerto 22 (fuente: rango de IP desde el que se conectará a una EC2 instancia).	
Cree un sistema de archivos.	En los objetivos de montaje, use la VPC y el grupo de seguridad que creó en la historia anterior. Elija el modo de procesamiento y el rendimiento en función de I/O los requisitos de la base de datos local. De manera opcional, habilite el cifrado en reposo.	DevOps/database Administrador de AWS

Monte el sistema de archivos.

Tarea	Descripción	Habilidades requeridas
Cree un rol de perfil de instancia de IAM para asociarlo a una EC2 instancia.	Cree un rol de IAM que tenga permisos para cargar y acceder a objetos en Amazon S3. Elija el bucket de S3 donde se almacenará la copia de seguridad como recurso de políticas.	AWS DevOps
Crea una EC2 instancia.	Lance una EC2 instancia basada en Linux y asocie	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	el rol de perfil de instancia de IAM que creó en el paso anterior y el grupo de seguridad que creó anteriormente.	
Instale el cliente NFS.	Instale el cliente NFS en el servidor de base de datos local y en la EC2 instancia. Para obtener instrucciones, consulte la sección «Información adicional».	DevOps
Monte el sistema de archivos de Amazon EFS.	Monte el sistema de archivos Amazon EFS en las instalaciones y en la EC2 instancia. En cada servidor, cree un directorio para almacenar la copia de seguridad y monte el sistema de archivos mediante el punto de conexión de destino de montaje. Para obtener ejemplos, consulte la sección «Información adicional».	DevOps

Crear una copia de seguridad de la base de datos de origen MySQL

Tarea	Descripción	Habilidades requeridas
Instale Percona XtraBackup.	Instale Percona XtraBackup 2.3 o 2.4 (según la versión de la base de datos MySQL) en el servidor de bases de datos local. Para obtener los enlaces	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de instalación, consulte la sección «Recursos relaciona dos».	
Cuente los esquemas y las tablas de la base de datos de origen.	Recopile y anote el número de esquemas y objetos de la base de datos MySQL de origen. Utilizará estos recuentos para validar la base de datos Aurora MySQL después de la migración.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
(Opcional) Anote la secuencia de registro binario más reciente de la base de datos de origen.	Realice este paso si desea establecer la replicación de registros binarios entre la base de datos de origen y Aurora MySQL para minimizar el tiempo de inactividad. log-bin debe estar habilitado y server_id debe ser único. Anote la secuencia de registros binarios actual de la base de datos de origen, justo antes de iniciar una copia de seguridad. Realice este paso justo antes de la copia de seguridad completa si planea usar solo una copia de seguridad completa. Si planea realizar copias de seguridad incrementales después de una copia de seguridad completa, lleve a cabo este paso justo antes de la última copia de seguridad incremental que restaurará en la instancia de base de datos Aurora MySQL.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Inicie una copia de seguridad completa de la base de datos MySQL de origen.	Realice una copia de seguridad completa de la base de datos fuente de MySQL con Percona XtraBacku p. Para ver ejemplos de comandos para copias de seguridad completas e incrementales, consulte la sección «Información adicional ».	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
(Opcional) Realice copias de seguridad incrementales con XtraBackup Percona.	Las copias de seguridad incrementales se pueden utilizar para reducir la cantidad de registros binarios que debe aplicar para sincronizar la base de datos de origen con Aurora MySQL. Las bases de datos de gran tamaño y con muchas transacciones pueden generar una gran cantidad de registros binarios durante las copias de seguridad. Al realizar copias de seguridad incrementales y almacenar las en un sistema de archivos Amazon EFS compartido, puede reducir considera blemente el tiempo de copia de seguridad y carga de la base de datos. Para obtener más información, consulte la sección «Información adicional ». Siga realizando copias de seguridad incrementales hasta que esté listo para iniciar el proceso de migración a Aurora.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Prepare copias de seguridad.	En este paso, los registros transaccionales se aplican a la copia de seguridad para las transacciones que estaban en curso durante la copia de seguridad. Siga aplicando registros transaccionales (--apply-log-only) a cada copia de seguridad increment al para fusionar las copias de seguridad, excepto la última copia de seguridad. Para obtener más ejemplos, consulte la sección «Informac ión adicional». Tras este paso, la copia de seguridad completa y combinada estará en ~/<efs_mount_name>/ fullbackup.	Administrador de base de datos
Comprima y divida la copia de seguridad final combinada.	Después de preparar la copia de seguridad final combinada , utilice los comandos tar, zip y split para crear archivos comprimidos más pequeños de la copia de seguridad. Para obtener más ejemplos, consulte la sección «Informac ión adicional».	Administrador de base de datos

Restauración de la copia de seguridad en un clúster de base de datos de Aurora MySQL

Tarea	Descripción	Habilidades requeridas
Cargue la copia de seguridad en Amazon S3.	El sistema de archivos Amazon EFS en el que se almacenan los archivos de copia de seguridad está montado tanto en la base de datos local como en una EC2 instancia, de modo que los archivos de copia de seguridad estén fácilmente disponibl es para la EC2 instancia. <bucket_name>Conéctese a la EC2 instancia mediante Secure Shell (SSH) y cargue los archivos de respaldo comprimidos en un bucket de S3 nuevo o existente; por ejemplo: aws s3 sync ~/ <efs_mount_name>/fullbackup s3:///fullbackup. Para obtener más información, consulte los enlaces de la sección «Recursos relacionados».	AWS DevOps
Crear un rol de servicio para que Aurora pueda acceder a Amazon S3	Cree un rol de IAM con la confianza «rds.amaz onaws.com» y una política que permita a Aurora acceder al bucket de S3 donde se almacenan los archivos de copia de seguridad. Los permisos necesarios son	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	ListBucket GetObject, y GetObjectVersion.	
Cree la configuración de red para Aurora.	Cree un grupo de subredes de base de datos de clúster con al menos dos zonas de disponibilidad y una configuración de tabla de enrutamiento de subred que permita la conectividad saliente a la base de datos de origen. Cree un grupo de seguridad que permita las conexiones salientes a la base de datos en las instalaciones y permita a los administradores conectarse al clúster de base de datos Aurora. Para obtener más información, consulte los enlaces de la sección «Recursos relacionados».	DevOps/database Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Restauración de la copia de seguridad en un clúster de base de datos de Aurora MySQL.	Restaure sus datos desde la copia de seguridad que cargó en Amazon S3. Especifique la versión MySQL de la base de datos de origen, proporcione el nombre del bucket de S3 y el prefijo de la ruta de la carpeta donde cargó el archivo de copia de seguridad (por ejemplo, «fullbackup» para los ejemplos de la sección «Información adicional») y proporcione el rol de IAM que creó para autorizar a Aurora a acceder a Amazon S3.	DevOps/database Administrador de AWS
Valide la base de datos de Aurora MySQL.	Valide el recuento de esquemas y objetos del clúster de base de datos Aurora restaurado con respecto al recuento obtenido de la base de datos de origen.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Configure la replicación de binlog.	Utilice la secuencia de registro binario que indicó anteriormente antes de realizar la última copia de seguridad que se restauró en el clúster de base de datos Aurora. Cree un usuario de replicación en la base de datos de origen y siga las instrucciones de la sección «Información adicional» para proporcionar los privilegios adecuados, habilitar la replicación en Aurora y confirmar que la replicación está sincronizada.	DevOps/database Administrador de AWS

Recursos relacionados

Creación de un sistema de archivos de Amazon EFS

- Creación de un grupo de seguridad (documentación de Amazon VPC)
- Adjuntos de VPN de puerta de enlace de tránsito (documentación de Amazon VPC)
- Escalar el rendimiento de la VPN con AWS Transit Gateway (blog sobre redes y entrega de contenido)
- Creación de un sistema de archivos de Amazon EFS (documentación de Amazon EFS)
- Creación de objetivos de montaje (documentación de Amazon EFS)
- Cifrado de datos en reposo (documentación de Amazon EFS)

Montaje de sistemas de archivos

- Funciones de IAM para Amazon EC2 (EC2 documentación de Amazon)
- Lanzamiento de una instancia de Amazon EC2 Linux (EC2 documentación de Amazon)
- Instalación del cliente NFS (documentación de Amazon EFS)

- Montaje del sistema de archivos Amazon EFS en el cliente en las instalaciones (documentación de Amazon EFS)
- Montaje de sistemas de archivos EFS (documentación de Amazon EFS)

Creación de un copia de seguridad completa de la base de datos MySQL de origen

- Instalación de Percona XtraBackup 2.3 (documentación de Percona XtraBackup)
- Instalación de Percona XtraBackup 2.4 (documentación de Percona) XtraBackup
- Cómo establecer la configuración maestra de replicación (documentación de MySQL)
- Migración de datos desde una base de datos MySQL externa a un clúster de base de datos de Amazon Aurora MySQL (documentación de Aurora)
- Respaldo incremental (documentación de Percona XtraBackup)

Restauración de la copia de seguridad en Amazon Aurora MySQL

- Creación de un bucket (documentación de Amazon S3)
- Conexión a la instancia de Linux mediante SSH (documentación de Amazon EC2)
- Configuración de la CLI de AWS (documentación de la CLI de AWS)
- comando sync (referencia de comandos de la CLI de AWS)
- Creación de una política de IAM para acceder a los recursos de Amazon S3 (documentación de Aurora
- Requisitos previos del clúster de base de datos (documentación de Aurora)
- Uso de los grupos de subredes de base de datos (documentación de Aurora)
- Creación de un grupo de seguridad de VPC para una instancia de base de datos privada (documentación de Aurora)
- Restauración de un clúster de base de datos de Aurora MySQL desde un bucket de S3 (documentación de Aurora)
- Configuración de la replicación con MySQL o con otro clúster de base de datos de Aurora (documentación de Aurora)
- Procedimiento mysql.rds_set_external_master (referencia de SQL para MySQL en Amazon RDS)
- Procedimiento mysql.rds_start_replication (referencia de SQL sobre MySQL en Amazon RDS)

Referencias adicionales

- Migración de datos desde una base de datos MySQL externa a un clúster de base de datos de Amazon Aurora MySQL (documentación de Aurora)
- Descargas del servidor MySQL (sitio web de Oracle)

Tutoriales y videos

- Migración de datos de MySQL a un clúster de base de datos Aurora MySQL mediante Amazon S3 (Centro de conocimientos de AWS)
- Configuración y montaje de Amazon EFS (video)

Información adicional

Instalación de un cliente NFS

- Si utiliza Red Hat o un sistema operativo Linux similar, utilice el comando:

```
$ sudo yum -y install nfs-utils
```

- Si utiliza Ubuntu o un sistema operativo Linux similar, utilice el comando:

```
$ sudo apt-get -y install nfs-common
```

Para obtener más información, consulte el tutorial en la documentación de Amazon EFS.

Montaje de un sistema de archivos de Amazon EFS

Utilice el comando:

```
mkdir ~/<efs_mount_name>
$ sudo mount -t nfs -o
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport mount-
target-IP:/ ~/<efs_mount_name>
```

Para obtener más información, consulte el tutorial y Montaje de un sistema de archivos en la documentación de Amazon EFS.

Hacer copias de seguridad de la base de datos fuente MySQL

Copias de seguridad completas

Use un comando como el siguiente, que toma la copia de seguridad, la comprime y la divide en fragmentos más pequeños de 1 GB cada uno:

```
xtrabackup --backup --user=dbuser --password=<password> --binlog-info=AUTO --stream=tar
 --target-dir=~/<efs_mount_name>/fullbackup | gzip - | split -d --bytes=1024MB - ~/
<efs_mount_name>/fullbackup/backup.tar.gz &
```

Si planea realizar copias de seguridad incrementales posteriores después de la copia de seguridad completa, no comprima ni divida la copia de seguridad. En su lugar, use un comando similar al siguiente:

```
xtrabackup --backup --user=dbuser --password=<password> --target-dir=~/
<efs_mount_name>/fullbackup/
```

Copias de seguridad incrementales

Utilice la ruta de copia de seguridad completa para el parámetro `--incremental-basedir`; por ejemplo:

```
xtrabackup --backup --user=dbuser --password=<password> --target-dir=~/
<efs_mount_name>/incremental/backupdate --incremental-basedir=~/<efs_mount_name>/
fullbackup
```

donde basedir es la ruta a la copia de seguridad completa y al archivo xtrabackup_checkpoints.

Para obtener más información sobre la creación de copias de seguridad, consulte Migración de datos desde una base de datos MySQL externa a un clúster de base de datos de MySQL de Amazon Aurora en la documentación de Aurora.

Preparación de copias de seguridad

Para preparar una copia de seguridad completa:

```
xtrabackup --prepare --apply-log-only --target-dir=~/<efs_mount_name>/fullbackup
```

Para preparar una copia de seguridad incremental:

```
xtrabackup --prepare --apply-log-only --target-dir=~/<efs_mount_name>/fullbackup --
incremental-dir=~/<efs_mount_name>/incremental/06062020
```

Para preparar la copia de seguridad final:

```
xtrabackup --prepare --target-dir=~/<efs_mount_name>/fullbackup --incremental-dir=~/
<efs_mount_name>/incremental/06072020
```

Para obtener más información, consulte las copias de seguridad incrementales en la documentación de Percona XtraBackup .

Comprimir y dividir la copia de seguridad combinada

Para comprimir la copia de seguridad combinada en ~/<efs_mount_name>/fullbackup:

```
tar -zcvf <backupfilename.tar.gz> ~/<efs_mount_name>/fullbackup
```

Para dividir la copia de seguridad:

```
split -d -b1024M --verbose  <backupfilename.tar.gz> <backupfilename.tar.gz>
```

Configure la replicación de binlog

Para crear un usuario de replicación en la base de datos de origen y proporcionar los privilegios adecuados:

```
CREATE USER 'repl_user'@'' IDENTIFIED BY ''; GRANT REPLICATION CLIENT, REPLICATION
 SLAVE ON *.* TO 'repl_user'@'';
```

Para habilitar la replicación en Aurora mediante la conexión al clúster de base de datos Aurora, habilite los registros binarios en el grupo de parámetros del clúster de base de datos. Configure `binlog_format = mixed` (se prefiere el modo mixto). Este cambio requiere que reinicies la instancia para aplicar la actualización.

```
CALL mysql.rds_set_external_master ('sourcedbinstanceIP', sourcedbport, 'repl_user',
 '', 'binlog_file_name', binlog_file_position, 0); CALL mysql.rds_start_replication;
```

Para confirmar que la replicación está sincronizada:

```
SHOW Slave Status \G;
```

El campo Segundos detrás del maestro muestra qué tan lejos está Aurora de la base de datos en las instalaciones.

Migración de aplicaciones Java locales en las instalaciones a AWS mediante AWS App2Container

Dhananjay Karanjkar, Amazon Web Services

Resumen

AWS App2Container (A2C) es una herramienta de línea de comandos que le ayuda a transformar en contenedores las aplicaciones existentes que se ejecutan en máquinas virtuales sin necesidad de cambiar el código. A2C descubre aplicaciones en ejecución en un servidor, identifica las dependencias y genera artefactos relevantes para una implementación sin interrupciones en Amazon Elastic Container Service (Amazon ECS) y Amazon Elastic Kubernetes Service (Amazon EKS).

Este patrón proporciona los pasos para migrar de forma remota las aplicaciones Java en las instalaciones implementadas en un servidor de aplicaciones a AWS Fargate o Amazon EKS mediante App2Container a través de la máquina de trabajo.

La máquina de trabajo se puede utilizar en los siguientes casos de uso:

- La instalación de Docker no está permitida o no está disponible en los servidores de aplicaciones donde se ejecutan las aplicaciones Java.
- Debe gestionar la migración de varias aplicaciones implementadas en distintos servidores físicos o virtuales.

Este patrón usa AWS CodeCommit AWS CodePipeline, y AWS CodeBuild.

Requisitos previos y limitaciones

Requisitos previos

- Un servidor de aplicaciones con una aplicación Java que se ejecuta en un servidor Linux
- Una máquina de trabajo con un sistema operativo Linux
- Una máquina de trabajo con al menos 20 GB de espacio disponible en disco

Limitaciones

- No todas las aplicaciones son compatibles. Para más información, consulte Aplicaciones compatibles para Linux.

Arquitectura

Pila de tecnología de origen

- Aplicaciones Java que se ejecutan en un servidor Linux

Pila de tecnología de destino

- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- Amazon Elastic Container Registry
- AWS Fargate

Arquitectura de destino

Tools (Herramientas)

Herramientas

- AWS App2Container (A2C) es una herramienta de la línea de comandos que le ayuda a migrar mediante lift-and-shift las aplicaciones que se ejecutan en centros de datos en las instalaciones o en máquinas virtuales, de modo que se ejecuten en contenedores administrados por Amazon ECS o Amazon EKS.
- AWS CodeBuild: AWS CodeBuild es un servicio de compilación en la nube totalmente gestionado. CodeBuild compila su código fuente, ejecuta pruebas unitarias y produce artefactos que están listos para su implementación.
- AWS CodeCommit: AWS CodeCommit es un servicio de control de versiones alojado por Amazon Web Services que puede utilizar para almacenar y gestionar activos (como documentos, código fuente y archivos binarios) en la nube de forma privada.
- AWS CodePipeline: AWS CodePipeline es un servicio de entrega continua que puede utilizar para modelar, visualizar y automatizar los pasos necesarios para lanzar su software.

- Amazon ECS: Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores altamente escalable y rápido que facilita la tarea de ejecutar, detener y administrar contenedores en un clúster.
- Amazon ECR: Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado por AWS que es seguro, escalable y fiable.
- Amazon EKS: Amazon Elastic Kubernetes Service (Amazon EKS) es un servicio administrado que puede utilizar para ejecutar Kubernetes en AWS sin necesidad de instalar, operar ni mantener su propio plano de control o nodos de Kubernetes.
- AWS Fargate: AWS Fargate es una tecnología que puede usar con Amazon ECS para ejecutar contenedores sin tener que administrar servidores o clústeres de instancias de Amazon Elastic Compute Cloud (Amazon). EC2 Con Fargate, ya no tendrá que aprovisionar, configurar ni escalar clústeres de máquinas virtuales para ejecutar los contenedores.

Epics

Configuración de credenciales

Tarea	Descripción	Habilidades requeridas
Cree un secreto para acceder al servidor de aplicaciones.	Para acceder al servidor de aplicaciones de forma remota desde la máquina de trabajo, cree un secreto en AWS Secrets Manager. Como secreto, puede utilizar la clave privada de SSH o el certifica do y la clave privada de SSH. Para obtener más información, consulte Administrar secretos para AWS App2Container.	DevOps, desarrollador

Configure la máquina de trabajo

Tarea	Descripción	Habilidades requeridas
Instalar el archivo tar.	Ejecute `sudo yum install -y tar`.	DevOps, Desarrollador
Instale la AWS CLI.	Para instalar la interfaz de la línea de comandos de AWS (AWS CLI), ejecute `curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip" .` Descomprima `awscliv2.zip .` Ejecute `sudo ./aws/install .`	DevOps, Desarrollador
Instale App2Container.	Ejecute los siguientes comandos : `curl -o AWSApp2Container-installer-linux.tar.gz https://app2container-release-us-east-1.s3.us-east-1.amazonaws.com/latest/linux/AWSApp2Container-installer-linux.tar.gz`	DevOps, Desarrollador

Tarea	Descripción	Habilidades requeridas

	`sudo tar xvf AWSApp2Container-installer-linux.tar.gz`
	
	`sudo ./install.sh`	

Configure los perfiles.	Para configurar el perfil predeterminado de AWS, ejecute `sudo aws configure .` Para configurar el perfil predeterminado de AWS con nombre, ejecute `sudo aws configure --profile <profile name>`.	DevOps, Desarrollador

Instale Docker.	Use los siguientes comandos.
	
	`sudo yum install -y docker`
	
	`sudo systemctl enable docker & sudo systemctl restart docker`	

Tarea	Descripción	Habilidades requeridas
Inicie App2Container.	Para inicializar App2Container, necesita la siguiente información: • `workspace` : para almacenar los artefactos de contenerización de aplicaciones. Recomendamos aportar una ruta de directorio que tenga al menos 20 GB de espacio libre en disco. • `awsProfile` : perfil de AWS configurado en el servidor. Esto es necesario para cargar artefactos en Amazon S3, ejecutar el comando `containerize` y generar artefactos de AWS para su implementación en Amazon ECS o Amazon EKS. • `s3Bucket`: para extraer y almacenar artefactos de AWS. • `metricsReportPermission` : para recopilar y almacenar las métricas reportadas. • `dockerContentTrust` : para firmar la imagen de Docker.	DevOps, Desarrollador

Tarea	Descripción	Habilidades requeridas
	Ejecute `sudo app2container init .`	

Configure la máquina de trabajo

Tarea	Descripción	Habilidades requeridas
Configure la máquina de trabajo para conectarse remotamente y ejecutar los comandos de App2Container en el servidor de aplicaciones.	Para configurar la máquina de trabajo, se requiere la siguiente información: • `Server FQDN`: el nombre completo del dominio del servidor de aplicaciones. • `Server IP address`: la dirección IP del servidor de aplicaciones. El FQDN o la dirección IP son suficientes. • `SecretARN` : el nombre de recurso de Amazon (ARN) del secreto que se utiliza para conectarse al servidor de aplicaciones y que se almacena en Secrets Manager. • `AuthMethod` : el método de autenticación `key` o `cert`. Ejecute `sudo app2container remote configure .`	DevOps, Desarrollador

Descubra, analice y extraiga aplicaciones en la máquina de trabajo

Tarea	Descripción	Habilidades requeridas
Descubra las aplicaciones Java en las instalaciones.	Para descubrir de forma remota todas las aplicaciones en ejecución en el servidor de aplicaciones, ejecute el siguiente comando. `sudo app2container remote inventory --target <FQDN/IP of App server>` Este comando genera una lista de las aplicaciones implementadas en `inventory.json` .	Desarrollador, DevOps
Analice las aplicaciones descubiertas.	Para analizar de forma remota cada aplicación mediante el identificador de aplicación obtenido en la fase de inventario, ejecute el siguiente comando. `sudo app2container remote analyze --application-id <java-app-id> --target <FQDN/IP of App Server>` Esto genera un archivo `analysis.json` en la ubicación del espacio de trabajo. Una vez generado	Desarrollador, DevOps

Tarea	Descripción	Habilidades requeridas
	este archivo, puede modificar los parámetros de conteneri zación en función de sus necesidades.	
Extraiga las aplicaciones analizadas.	Para generar un archivo de aplicaciones para la aplicació n analizada, ejecute de forma remota el siguiente comando, que generará el paquete tar en la ubicación del espacio de trabajo. `sudo app2container remote extract --application-id <application id> --target <FQDN/IP of App Server>` Los artefactos extraídos se pueden generar en la máquina de trabajo local.	Desarrollador, DevOps

Guarde en contenedores los artefactos extraídos en la máquina de trabajo

Tarea	Descripción	Habilidades requeridas
Coloque en contenedores los artefactos extraídos.	Guarde en contenedores los artefactos extraídos en el paso anterior ejecutando el siguiente comando. `sudo app2container containerize --input-`	Desarrollador, DevOps

Tarea	Descripción	Habilidades requeridas
	`archive <tar bundle location on worker machine>`	
Finalice el objetivo.	Para finalizar el objetivo, abra `deployment.json` , que se crea cuando se ejecuta el comando `containerize` . Para especificar AWS Fargate como objetivo, establezca `createEcsArtifacts` en `true`. Para establecer Amazon EKS como objetivo, establezca `createEksArtifacts` en true.	Desarrollador, DevOps

Genere y aprovisione artefactos de AWS

Tarea	Descripción	Habilidades requeridas
Genere artefactos de implementación de AWS en la máquina de trabajo.	Para generar artefactos de implementación, ejecute el siguiente comando. `sudo app2container generate app-deployment --application-id <application id>` Esto genera la CloudFormation plantilla de `ecs-master.yml` AWS en el espacio de trabajo.	DevOps

Tarea	Descripción	Habilidades requeridas
Aprovisione los artefactos.	Para aprovisionar aún más los artefactos generados, implemente la CloudFormation plantilla de AWS ejecutando el siguiente comando. `aws cloudformation deploy --template-file <path to ecs-master.yml> --capabilities CAPABILITY_NAMED_IAM --stack-name <application id>-ECS`	DevOps
Genere la canalización.	Modifique `pipeline.json` , que se creó en la historia anterior, en función de sus necesidades. A continuación, ejecute el comando `generate pipeline` para generar los artefactos de implementación de la canalización.	DevOps

Recursos relacionados

- ¿Qué es App2Container?
- Entrada de blog sobre AWS App2Container
- Conceptos básicos de configuración de la CLI de AWS
- Conceptos básicos de Docker para Amazon ECS
- Comandos de Docker

Migre sistemas de archivos compartidos en una migración AWS grande

Amit Rudraraju, Sam Apa, Bheemeswararao Balla, Wally Lu y Sanjeev Prakasam, Amazon Web Services

Resumen

La migración de 300 o más servidores se considera una migración grande. El objetivo de una gran migración es migrar las cargas de trabajo de sus centros de datos locales existentes a los centros de datos locales existentes Nube de AWS, y estos proyectos suelen centrarse en las cargas de trabajo de aplicaciones y bases de datos. Sin embargo, los sistemas de archivos compartidos requieren una atención específica y un plan de migración independiente. Este patrón describe el proceso de migración de los sistemas de archivos compartidos y proporciona las prácticas recomendadas para migrarlos correctamente como parte de un gran proyecto de migración.

Un sistema de archivos compartidos (SFS), también conocido como sistema de archivos de red o agrupado, es un recurso compartido de archivos que se monta en varios servidores. Se accede a los sistemas de archivos compartidos mediante protocolos como el Sistema de archivos de red (NFS), el Sistema de archivos común de Internet (CIFS) o el Bloque de mensajes del servidor (SMB).

Estos sistemas no se migran con herramientas de migración estándar, por ejemplo, AWS Transform MGN porque no están dedicados al host que se va a migrar ni se representan como un dispositivo de bloques. Si bien la mayoría de las dependencias del host se migran de forma transparente, la coordinación y la administración de los sistemas de archivos dependientes deben gestionarse por separado.

Los sistemas de archivos compartidos se migran en las siguientes fases: descubrir, planificar, preparar, recortar y validar. Con este patrón y los libros de trabajo adjuntos, se migra el sistema de archivos compartidos a un servicio de AWS almacenamiento, como Amazon Elastic File System (Amazon EFS), Amazon FSx for NetApp ONTAP o Amazon FSx for Windows File Server. Para transferir el sistema de archivos, puede utilizar AWS DataSync una herramienta de terceros, como. NetApp SnapMirror

> **Note**
>
> Este patrón forma parte de una serie de guías AWS prescriptivas sobre las grandes migraciones al. Nube de AWS Este patrón incluye las mejores prácticas e instrucciones para SFSs incorporarlas a sus planes de oleaje para servidores. Si va a migrar uno o más sistemas de archivos compartidos fuera de un proyecto de migración de gran tamaño,

consulte las instrucciones de transferencia de datos en la AWS documentación de Amazon EFS, Amazon FSx for Windows File Server y Amazon FSx for NetApp ONTAP.

Requisitos previos y limitaciones

Requisitos previos

Los requisitos previos pueden variar en función de los sistemas de archivos compartidos de origen y destino y del caso de uso. Los problemas más coqmunes son los siguientes:

- Un activo. Cuenta de AWS
- Ha completado la búsqueda de la cartera de aplicaciones para su gran proyecto de migración y ha empezado a desarrollar planes de onda. Para obtener más información, consulta el manual de estrategias de Portfolio para migraciones AWS grandes.
- Nubes privadas virtuales (VPCs) y grupos de seguridad que permiten el tráfico de entrada y salida entre el centro de datos local y su entorno. AWS Para obtener más información, consulte Opciones de conectividad de red a Amazon VPC y requisitos de red.AWS DataSync
- Permisos para crear AWS CloudFormation pilas o permisos para crear Amazon EFS o FSx recursos de Amazon. Para obtener más información, consulte la CloudFormation documentación, la documentación de Amazon EFS o la FSx documentación de Amazon.
- Si va AWS DataSync a realizar la migración, necesitará los siguientes permisos:
  - Permisos AWS DataSync para enviar registros a un grupo de CloudWatch registros de Amazon Logs. Para obtener más información, consulte Permitir DataSync la carga de registros a grupos de CloudWatch registros.
  - Permisos para acceder al grupo de CloudWatch registros. Para obtener más información, consulte Descripción general de la administración de los permisos de acceso a los recursos de CloudWatch Logs.
  - Permisos para crear agentes y tareas en DataSync. Para obtener más información, consulte Permisos de IAM necesarios para su uso AWS DataSync.

Limitaciones

- Este patrón está diseñado para migrar SFSs como parte de un gran proyecto de migración. Incluye las mejores prácticas e instrucciones para SFSs incorporarlos a sus planes de migración de aplicaciones. Si va a migrar uno o más sistemas de archivos compartidos fuera de un proyecto

de migración de gran tamaño, consulte las instrucciones de transferencia de datos en la AWS documentación de Amazon EFS, Amazon FSx for Windows File Server y Amazon FSx for NetApp ONTAP.

- Este patrón se basa en las arquitecturas, los servicios y los patrones de migración más utilizados. Sin embargo, los grandes proyectos y estrategias de migración pueden variar de una organización a otra. Es posible que necesite personalizar esta solución o los libros de trabajo proporcionados en función de sus necesidades.

Arquitectura

Pila de tecnología de origen

Una o varias de las siguientes:

- Servidor de archivos Linux (NFS)
- Servidor de archivos Windows (SMB)
- NetApp arreglo de almacenamiento
- Cabina de almacenamiento Dell EMC Isilon

Pila de tecnología de destino

Una o varias de las siguientes:

- Amazon Elastic File System
- Amazon FSx para NetApp ONTAP
- Servidor FSx de archivos Amazon para Windows

Arquitectura de destino

El diagrama muestra el proceso siguiente:

1. Para establecer una conexión entre el centro de datos local y el Nube de AWS centro de datos se utiliza un elemento Servicio de AWS como AWS Direct Connect o. AWS Site-to-Site VPN
2. El DataSync agente se instala en el centro de datos local.
3. Según su plan de oleaje, se utilizan DataSync para replicar los datos del sistema de archivos compartidos de origen al recurso compartido de AWS archivos de destino.

Fases de migración

La siguiente imagen muestra las fases y los pasos de alto nivel para migrar un SFS en un proyecto de migración de gran tamaño.

La sección Epics de este patrón contiene instrucciones detalladas sobre cómo completar la migración y utilizar los libros de trabajo adjuntos. A continuación, se brinda información general de alto nivel de los pasos de este enfoque por etapas.

Fase	Steps
Descubra	1. Con una herramienta de detección, se recopilan datos sobre el sistema de archivos compartido, incluidos los servidores, los puntos de montaje y las direcciones IP. 2. Mediante una base de datos de gestión de la configuración (CMDB) o una herramienta de migración, se recopilan detalles sobre el servidor, incluida información sobre la onda de migraciones, el entorno, el propietario de la aplicación, el nombre del servicio de gestión de servicios de TI (ITSM), la unidad organizativa y el identificador de la aplicación.
Planifique	3. Con la información recopilada sobre los servidores SFSs y los servidores, cree el plan de oleada del SFS. 4. Con la información de la hoja de trabajo de creación, elija un objetivo Servicio de AWS y una herramienta de migración para cada SFS.
Preparación	5. Configure la infraestructura de destino en Amazon EFS, Amazon FSx for NetApp ONTAP o Amazon FSx for Windows File Server.

	6. Configure el servicio de transferencia de datos, por ejemplo, y DataSync, a continuación, inicie la sincronización de datos inicial. Cuando se complete la sincronización inicial, puede configurar las sincronizaciones recurrentes para que se ejecuten según una programación,
	7. Actualice el plan de ondas del SFS con información sobre el recurso compartido de archivos de destino, como la dirección IP o la ruta.
Realizar la transición	8. Detenga las aplicaciones que acceden activamente al SFS de origen.
	9. En el servicio de transferencia de datos, realice una sincronización de datos final.
	10. Cuando se complete la sincronización, compruebe que se ha realizado correctamente revisando los datos de registro en CloudWatch Registros.
Valide	11. En los servidores, cambie el punto de montaje por la nueva ruta SFS.
	12. Reinicie y valide las aplicaciones.

Tools (Herramientas)

Servicios de AWS

- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas y aplicaciones Servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- AWS DataSynces un servicio de transferencia y descubrimiento de datos en línea que le ayuda a mover archivos u datos de objetos hacia, desde y entre los servicios AWS de almacenamiento.

- Amazon Elastic File System (Amazon EFS) lo ayuda a crear y configurar sistemas de archivos compartidos en la Nube de AWS.
- Amazon FSx proporciona sistemas de archivos que admiten los protocolos de conectividad estándares del sector y ofrecen alta disponibilidad y replicación en todos Regiones de AWS los niveles.

Otras herramientas

- SnapMirrores una herramienta de replicación de NetApp datos que replica datos de volúmenes de origen o qtrees específicos a volúmenes o qtrees de destino, respectivamente. Puedes usar esta herramienta para migrar un sistema de archivos NetApp fuente a Amazon FSx para NetApp ONTAP.
- Robocopy, abreviatura de Robust File Copy, es un directorio de línea de comandos y comandos para Windows. Puedes usar esta herramienta para migrar un sistema de archivos fuente de Windows a Amazon FSx for Windows File Server.

Prácticas recomendadas

Enfoques de planificación de olas

Al planificar las ondas para su gran proyecto de migración, tenga en cuenta la latencia y el rendimiento de las aplicaciones. Cuando el SFS y las aplicaciones dependientes funcionan en ubicaciones diferentes, como una en la nube y otra en el centro de datos en las instalaciones, esto puede aumentar la latencia y afectar al rendimiento de las aplicaciones. A continuación, se muestran las siguientes opciones al crear planes de onda:

1. Migre el SFS y todos los servidores dependientes en la misma oleada: este enfoque evita problemas de rendimiento y minimiza las tareas de retrabajo, como la reconfiguración de los puntos de montaje varias veces. Se recomienda cuando se requiere una latencia muy baja entre la aplicación y el SFS. Sin embargo, la planificación de ondas es compleja y, por lo general, el objetivo es eliminar las variables de las agrupaciones de dependencias, no añadirlas. Además, este enfoque no se recomienda si muchos servidores acceden al mismo SFS, ya que esto hace que la onda sea demasiado grande.
2. Migre el SFS una vez que se haya migrado el último servidor dependiente: por ejemplo, si varios servidores acceden a un SFS y dichos servidores tienen previsto migrar en las oleadas 4, 6 y 7, programe la migración del SFS en la oleada 7.

Este enfoque suele ser el más lógico para migraciones grandes y se recomienda para aplicaciones sensibles a la latencia. Reduce los costos asociados a la transferencia de datos. También minimiza el período de latencia entre el SFS y las aplicaciones de nivel superior (como las de producción), ya que las aplicaciones de nivel superior suelen estar programadas para migrar en último lugar, después de las aplicaciones de desarrollo y control de calidad.

Sin embargo, este enfoque aún requiere detección, planificación y agilidad. Es posible que tenga que migrar el SFS en una onda anterior. Confirme que las aplicaciones puedan soportar la latencia adicional durante el período de tiempo entre la primera onda dependiente y la onda que contiene el SFS. Realice una sesión de descubrimiento con los propietarios de las aplicaciones y migre la aplicación en la misma fase, es decir, la aplicación más sensible a la latencia. Si se descubren problemas de rendimiento después de migrar una aplicación dependiente, prepárese para migrar rápidamente el SFS lo más rápido posible.

3. Migre el SFS al final de un gran proyecto de migración: este enfoque se recomienda si la latencia no es un factor, por ejemplo, cuando se accede con poca frecuencia a los datos del SFS o no son críticos para el rendimiento de la aplicación. Este enfoque agiliza la migración y simplifica las tareas de transición.

Puede combinar estos enfoques en función de la sensibilidad a la latencia de la aplicación. Por ejemplo, puede migrar en función de la latencia SFSs utilizando los enfoques 1 o 2 y, a continuación, migrar el resto SFSs utilizando el enfoque 3.

Elegir un servicio de sistema de archivos AWS

AWS ofrece varios servicios en la nube para el almacenamiento de archivos. Cada uno ofrece diferentes ventajas y limitaciones en cuanto al rendimiento, la escala, la accesibilidad, la integración, la conformidad y la optimización de costos. Hay algunas opciones lógicas predeterminadas. Por ejemplo, si su sistema de archivos local actual utiliza Windows Server, Amazon FSx for Windows File Server es la opción predeterminada. O bien, si el sistema de archivos local utiliza NetApp ONTAP, Amazon FSx for NetApp ONTAP es la opción predeterminada. Sin embargo, puede elegir un servicio específico en función de los requisitos de su aplicación o para aprovechar otras ventajas operativas en la nube. Para obtener más información, consulte Elegir el servicio de almacenamiento de AWS archivos adecuado para su implementación (presentación en AWS Summit).

Elección de una herramienta de migración

Amazon EFS y Amazon FSx admiten el uso de AWS DataSync para migrar sistemas de archivos compartidos a Nube de AWS. Para obtener más información sobre los sistemas y servicios de almacenamiento compatibles, las ventajas y los casos de uso, consulte Qué es AWS DataSync. Para obtener una descripción general del proceso de uso DataSync para transferir archivos, consulte Cómo funcionan AWS DataSync las transferencias.

También hay varias herramientas de terceros disponibles, entre las que se incluyen las siguientes:

- Si eliges Amazon FSx for NetApp ONTAP, puedes usarlo NetApp SnapMirror para migrar los archivos del centro de datos local a la nube. SnapMirror utiliza la replicación a nivel de bloques, que puede ser más rápida DataSync y reducir la duración del proceso de transferencia de datos. Para obtener más información, consulte Migración a FSx ONTAP mediante. NetApp SnapMirror
- Si eliges Amazon FSx for Windows File Server, puedes usar Robocopy para migrar archivos a la nube. Para obtener más información, consulte Migración de archivos existentes a un servidor de archivos FSx de Windows mediante Robocopy.

Epics

Descubra

Tarea	Descripción	Habilidades requeridas
Prepare el libro de trabajo de descubrimiento del SFS.	1. Descargue los libros de trabajo de la sección Adjuntos de este patrón. Contiene dos archivos, SFS-Discovery-Workbook.xlsx y SFS-Wave-Plan-Workbook.xlsx. 2. Abra el archivo SFS-Discovery-Workbook en Microsoft Excel. 3. En la hoja de trabajo del Panel, haga lo siguiente: • En la columna A, actualice el nombre del entorno.	Ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
	• En la columna B, actualice el orden de los entornos para colocarlo s en orden desde la prioridad más baja (1) hasta la prioridad más alta. • En las columnas D a E, actualice el horario de oleaje. • En las columnas C y K, actualice los nombres de las cuentas de AWS. • En la columna L, actualice la VPC IDs. • En las columnas M—O, actualice la subred. IDs 4. Revise el resto de la plantilla del libro de trabajo y actualice cualquier otro valor necesario para su organización o caso de uso. 5. Guarde el cuaderno de trabajo.	

Tarea	Descripción	Habilidades requeridas
Recopile información sobre el SFS de origen.	1. Con la herramienta de detección que prefiera, identifique todos los montajes del SFS en todos los dispositivos de almacenamiento, servidores Linux y servidores Windows aplicables. En términos generales, necesitará recopilar la siguiente información: • Dispositivos cliente • Direcciones IP de clientes • Detalles de SFS • Punto de montaje **Note** Puede agregar los detalles del punto de montaje al manual de procedimientos de migración para volver a montar el SFS después de la migración. 2. Abra el archivo SFS-Discovery-Workbook. 3. En la hoja de trabajo Wave-Sheet, haga lo siguiente: • En la columna Ubicación del servidor	Ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
	(D), en la fórmula, confirme que el formato del rango CIDR de la fuente en las instalaciones funciona para su rango. Por ejemplo, si su rango de CIDR es `10.0.0.0/8` , introduzca `10.*.*.*`. • En la columna Ubicación SFS (E), en la fórmula, confirme que el formato del rango CIDR de la VPC de destino funciona para su rango. Por ejemplo, si su rango de CIDR es `176.16.0.0/16` , introduzca `176.16.*.*` . 4. En la hoja de trabajo SFS-Data, haga lo siguiente: • En la columna Nombre del servidor (A), introduzca el nombre del servidor en el que está montado el SFS. • En la columna Ruta del SFS (B), introduzca el nombre del SFS. • En la columna Dirección IP (C),	

Tarea	Descripción	Habilidades requeridas
	introduzca la dirección IP del servidor. • Agregue cualquier otra información relevante que haya recopilado durante la detección, como el punto de montaje y el tamaño del SFS. Puede utilizar estos datos más adelante para modificar los cálculos de planifica ción de las olas. 5. Guarde el cuaderno de trabajo.	

Tarea	Descripción	Habilidades requeridas
Recopile información sobre los servidores.	1. Con la CMDB o los datos registrados en la herramienta de migración, identifique toda la siguiente información sobre los servidores que tienen soportes SFS: • Nombre del servidor • Dirección IP • Onda • Unidad organizativa (OU) • Entorno de servidor, como `DEV`, `QA` o `PROD` • Nombre de la aplicación • Propietario de la aplicación e información de contacto 2. Abra el archivo SFS-Discovery-Workbook. 3. En la hoja de trabajo Server-Data, en las columnas A a H, introduzca la información que recopiló sobre los servidores de origen. Tenga en cuenta lo siguiente: • En la columna Wave # (C), introduzca el nombre de la onda (por ejemplo`Wave1`), out-of-scope (`OOS`) o. `Retire` • Si aparece en la columna de Contacto del propietar	Ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
	io de la aplicación (H), compruebe que la dirección de correo electrónico sea correcta. Esta dirección de correo electrónico se genera automáticamente en función del nombre que proporcionó en la columna del Propietario de la aplicación (G). Si es necesario, actualice manualmente el valor para que refleje la dirección de correo electrónico correcta. • No modifique las columnas I a J, que contienen fórmulas. 4. Guarde el cuaderno de trabajo.	

Plan

Tarea	Descripción	Habilidades requeridas
Cree el plan de olas del SFS.	1. Abra el archivo SFS-Disco very-Workbook. 2. Compruebe que toda la información recopilada en la fase de descubrimiento sea precisa y esté actualizada.	Responsable de compilación, líder de transición, ingeniero de migraciones, líder de migraciones

Tarea	Descripción	Habilidades requeridas
	3. En la hoja de trabajo Wave-Sheet, filtre la columna de onda SFS (K) según el valor 1. Esta es una lista de todos los elementos SFSs de la primera oleada. **Note** Un valor de `0` en esta columna indica que el SFS está fuera del ámbito de la migración. Esto puede deberse a que el SFS ya está alojado en él AWS o a que los servidores que acceden al recurso compartido están fuera del ámbito de la migración. 4. Compruebe que desea migrarlos SFSs en esta oleada. Para obtener más información sobre cómo asignar SFSs a las olas, consulte los enfoques de planificación de las olas en la sección Mejores prácticas. 5. Seleccione y copie las celdas que contienen los	

Tarea	Descripción	Habilidades requeridas
	valores filtrados. No copie la fila de encabezado que contiene los títulos de las columnas. 6. Abra el archivo SFS-Wave-Plan-Workbook que descargó anteriormente. 7. En la hoja de trabajo Export-from-Discovery, seleccione la celda A2. 8. Pegue los datos copiados. 9. Guarde los archivos SFS-Discovery-Workbook y SFS-Wave-Plan-Workbook.	

Tarea	Descripción	Habilidades requeridas
Elija el destino Servicio de AWS y la herramienta de migración.	1. En el SFS-Wave-Plan-Workbook archivo, en la Exported-from-Discovery hoja de trabajo, seleccione y copie los valores de la columna Ruta anterior (C). 2. En la hoja de trabajo Build-Wave, seleccione la celda A2. 3. Pegue los datos copiados. Las columnas B a M de esta hoja de trabajo se actualizan automáticamente para reflejar otros datos asociados a esta ruta. 4. Elimine los valores duplicados de la columna A. Para obtener instrucciones, consulte Eliminar valores duplicados (sitio web de soporte de Microsoft). 5. En la columna Patrón o servicio objetivo (F), revise el objetivo recomendado Servicio de AWS y actualícelo según sea necesario. Para obtener más información, consulte Elegir un servicio de sistema de AWS archivos en la sección Prácticas recomendadas de este patrón.	Ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
	6. En la columna Método de migración (G), revise la herramienta de migración recomendada y actualíce la según sea necesario. Para obtener más información, consulte Elegir una herramienta de migración en la sección de Prácticas recomendadas de este patrón. 7. Guarde el archivo SFS-Discovery-Workbook. Ha terminado de crear un plan de onda para esta ola. 8. Repita estas instrucciones para preparar un plan de onda para cada ola. Como los planes de onda están sujetos a cambios durante la migración, le recomendamos que planifique con no más de 5 ondas de antelación.	

Preparación

Tarea	Descripción	Habilidades requeridas
Configure el sistema de archivos de destino.	De acuerdo con los detalles registrados en su plan de oleada, configure los sistemas de archivos de destino en el destino Cuenta de AWS,	Ingeniero de migraciones, líder de migración, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	la VPC y las subredes. Para obtener instrucciones, consulte la siguiente documentación: AWS • Amazon EFS • Amazon FSx para NetApp ONTAP • Servidor FSx de archivos Amazon para Windows	

Tarea	Descripción	Habilidades requeridas
Configure la herramienta de migración y transfiera los datos.	1. Si lo está utilizando AWS DataSync, configure el registro de las DataSync tareas. Para obtener instrucciones, consulte Registrar las actividades de las AWS DataSync tareas. 2. Configure la herramien ta de migración y realice una transferencia de datos inicial según las instrucci ones de la herramienta que haya seleccionado: • Para Amazon EFS, consulte lo siguiente: • Transfiera archivos a Amazon EFS mediante AWS DataSync • Para Amazon FSx para NetApp ONTAP, consulta lo siguiente: • Cómo migrar a ONTAP FSx mediante NetApp SnapMirror • Migración a ONTAP para ONTAP mediante FSx AWS DataSync • Para Amazon FSx para Windows File Server, consulte lo siguiente: • Migración de archivos existentes a un servidor FSx de	Administrador de AWS, administrador de la nube, ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
	archivos de Windows mediante AWS DataSync • Migración de archivos existentes a un servidor de archivos FSx de Windows mediante Robocopy 3. Los cambios en el SFS de origen pueden producirse durante o después de la transferencia inicial. Configure transferencias de datos recurrentes entre los sistemas de archivos de origen y destino para mantener los datos sincronizados: • Si lo está utilizando DataSync, consulte Programar una tarea. AWS DataSync DataSync transfiere solo los archivos modificados o nuevos del SFS de origen. • Si utiliza una herramienta de terceros, consulte la documentación de la herramienta que hayas seleccionado.	

Tarea	Descripción	Habilidades requeridas
Actualice el plan de onda.	1. Abra el archivo SFS-Wave-Plan-Workbook para la oleada actual. 2. En la hoja de trabajo Build-Wave, en la columna Nueva dirección IP de ruta (N), introduzca la dirección IP del sistema de archivos de destino. Aplique alguna de las siguientes acciones para localizar la dirección IP: • FSx Para Windows File Server, en la FSx consola de Amazon, seleccion a Sistemas de archivos, elige tu sistema de archivos y, a continuac ión, consulta la sección Red y seguridad. • FSx Para ONTAP, consulte Montar volúmenes. • Para Amazon EFS, consulte Montaje con una dirección IP. 3. En la columna Nueva ruta (O), introduzca la nueva ruta de montaje. La ruta de montaje es el nombre de DNS del sistema de archivos. Aplique alguna de las siguientes acciones	Ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
	para localizar la ruta de montaje: • FSx Para Windows File Server, en la FSx consola de Amazon, seleccion a Sistemas de archivos, elige tu sistema de archivos y, a continuac ión, selecciona Adjuntar. • FSx Para ONTAP, consulta la página de detalles del sistema de archivos. Para obtener instrucciones, consulte Montaje de volúmenes. • Para Amazon EFS, consulte Obtener información. 4. En la hoja de trabajo Remount-Summary, confirme que las columnas Nueva ruta (C) y Nueva dirección IP de ruta (D) reflejan los valores actualizados. 5. Confirme que su organizac ión haya preparado manuales de procedimi entos para volver a montar los sistemas de archivos de Linux y Windows tras la transición. Para obtener instrucciones, consulte lo siguiente:	

Tarea	Descripción	Habilidades requeridas
	• Montaje de sistemas de archivos Amazon EFS • Acceso a FSx los recursos compartidos de archivos del servidor de archivos de Windows • Montaje FSx para volúmenes ONTAP 6. Si algún servidor dependiente no está incluido en esta onda, regístrelo en la hoja de trabajo App-Team-Communication. Informe a los propietarios de las aplicaciones o servidores correspondientes, ya que es posible que no estén incluidos en las comunicaciones estándar. 7. Si se SFSs retiran de la ola después de completar el plan de oleaje, haga un seguimiento de ellos en la hoja de trabajo Descoped.	

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Detener la aplicación.	Si las aplicaciones o los clientes están realizando operaciones de lectura y escritura de forma activa en	Propietario de la aplicación, desarrollador de la aplicación

Tarea	Descripción	Habilidades requeridas
	el SFS de origen, deténgalos antes de realizar la sincronización de datos final. Para obtener instrucciones, consulte la documentación de la aplicación o sus procesos internos para detener las actividades de lectura y escritura. Por ejemplo, consulte Iniciar o detener el servidor web (IIS 8) (documentación de Microsoft) o Administrar los servicios del sistema con systemctl (documentación de Red Hat).	

Tarea	Descripción	Habilidades requeridas
Realice la transferencia de datos final.	1. En la herramienta de migración, ejecute manualmente una tarea o trabajo final de transfere ncia de datos para sincronizar el sistema de archivos de destino con el SFS de origen. Para obtener instrucciones, consulte Cómo iniciar la DataSync tarea o consulte la documentación de la herramienta de migración de terceros que haya seleccionado. 2. Esperar a que se complete una transferencia. Para obtener más información, consulta Supervisar AWS DataSync la actividad con Amazon CloudWatch y Supervisar tu DataSync tarea desde la línea de comandos.	Ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
Valide la transferencia de datos.	Si lo estás utilizando AWS DataSync, haz lo siguiente para validar que la transfere ncia de datos final se haya realizado correctamente: 1. En la AWS DataSync consola, anota el ID de la tarea y la ejecución, por ejemplo `task-0000-exec-1111` . 2. Navegue hasta la sección de registro de tareas de la DataSync tarea. 3. Elija el enlace al grupo de CloudWatch registros. 4. En los registros, busque la tarea y el ID de ejecución. 5. Tome nota de cualquier error de transferencia. Para obtener más información, consulte Errores comunes en la DataSync documenta ción. 6. Valide lo siguiente: • Compare las listas de archivos de origen y destino SFSs para confirmar que se han transferido todos los datos • Compare los permisos de acceso a los archivos	Ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
	entre el origen y el destino SFSs. Si utiliza una herramienta de terceros, consulte las instrucciones de validación de la transferencia de datos en la documentación de la herramienta de migración seleccionada.	

Valide

Tarea	Descripción	Habilidades requeridas
Vuelva a montar el sistema de archivos y valide la función y el rendimiento de la aplicación.	1. Si los servidores dependientes se migraron en esta oleada, en el archivo SFS-Wave-Plan-Workbook, en la hoja de trabajo Remount-Summary, introduzca la nueva dirección IP del servidor en la columna Nueva dirección IP del servidor (F). 2. En todos los servidores, actualice el punto de montaje del sistema de archivos desde la ruta anterior a la nueva. Utilice el manual de instrucciones de su organización para volver a montarlo, tal como	Administrador de sistemas de AWS, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	se describió anteriormente en la fase de Preparación. 3. Confirme que el sistema de archivos está montado correctamente y que es accesible comprobando los montajes y verificando que los archivos estén presentes. El equipo de infraestructura suele realizar estas actividades. 4. Reinicie las aplicaciones y pida a sus propietarios o al equipo de control de calidad que realicen las pruebas funcionales y de rendimiento de la aplicación, según sea necesario.	

Resolución de problemas

Problema	Solución
Los valores de celda de Microsoft Excel no se actualizan.	Copie las fórmulas de las filas de muestra arrastrando el controlador de relleno. Para obtener más información, consulte las instrucciones para Windows o Mac (sitio web de soporte de Microsoft).

Recursos relacionados

AWS documentación

- AWS DataSync documentación

- Documentación de Amazon EFS
- FSx Documentación de Amazon
- Grandes migraciones al Nube de AWS
  - Guía para AWS grandes migraciones
  - Guía de portafolio para grandes migraciones AWS

Solución de problemas

- Solución de problemas AWS DataSync
- Solución de problemas de Amazon EFS
- Solución de problemas FSx de Amazon para Windows File Server
- Solución de problemas de Amazon FSx for NetApp ONTAP

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migre una base de datos Oracle a Amazon RDS for Oracle mediante adaptadores de archivos planos de GoldenGate Oracle

Dhairya Jindani y Baji Shaik, Amazon Web Services

Resumen

Oracle GoldenGate es un servicio de captura y replicación de datos en tiempo real para bases de datos y entornos de TI heterogéneos. Sin embargo, este servicio no admite actualmente Amazon Relational Database Service (Amazon RDS) para Oracle. Para obtener una lista de las bases de datos compatibles, consulte Oracle GoldenGate para bases de datos heterogéneas (documentación de Oracle). Este patrón describe cómo utilizar Oracle GoldenGate y los adaptadores de archivos GoldenGate planos de Oracle para generar archivos planos a partir de la base de datos Oracle de origen, que puede estar en las instalaciones o en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). A continuación, puede importar esos archivos planos a una instancia de base de datos de Amazon RDS para Oracle.

En este patrón, utiliza Oracle GoldenGate para extraer los archivos de seguimiento de la base de datos Oracle de origen. La bomba de datos copia los archivos de seguimiento en un servidor de integración, que es una EC2 instancia de Amazon. En el servidor de integración, Oracle GoldenGate utiliza el adaptador de archivos planos para generar una serie de archivos planos secuenciales basados en la captura de datos transacionales de los archivos de seguimiento. Oracle GoldenGate formatea los datos como valores separados por delimitadores o valores delimitados por longitud. A continuación, utilice Oracle SQL*Loader para importar los archivos planos a la instancia de base de datos Amazon RDS para Oracle de destino.

Destinatarios previstos

Este patrón está destinado a quienes tienen experiencia y conocimiento de los componentes fundamentales de un Oracle. GoldenGate Para obtener más información, consulte Descripción general de la GoldenGate arquitectura de Oracle (documentación de Oracle).

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.
- Una GoldenGate licencia de Oracle.
- Una licencia independiente para un GoldenGate adaptador de Oracle.

- Una base de datos Oracle de origen, que se ejecuta de forma local o en una EC2 instancia de Amazon.
- Una instancia de Amazon EC2 Linux que se utiliza como servidor de integración. Para obtener más información, consulte Introducción a las instancias de Amazon EC2 Linux (EC2 documentación de Amazon).
- Una instancia de base de datos de Amazon RDS para Oracle. Para obtener más información, consulte Creación de una instancia de base de datos de Oracle (documentación de Amazon RDS).

Versiones de producto

- Oracle Database Enterprise Edition, versión 10g, 11g, 12c o posterior
- Oracle, GoldenGate versión 12.2.0.1.1 o posterior

Arquitectura

Pila de tecnología de origen

Una base de datos Oracle (local o en una EC2 instancia de Amazon)

Pila de tecnología de destino

Amazon RDS para Oracle

Arquitectura de origen y destino

1. Oracle GoldenGate extrae las pistas de los registros de la base de datos de origen.
2. La bomba de datos extrae los rastros y los migra a un servidor de integración.
3. El adaptador de archivos GoldenGate planos de Oracle lee los registros, las definiciones de las fuentes y los parámetros de extracción.
4. Se sale de la extracción, que genera un archivo de control y archivos de datos planos.
5. Los archivos de datos sin formato se migran a una instancia de base de datos de Amazon RDS para Oracle en la Nube de AWS.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática escalable en el Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Relational Database Service (Amazon RDS) para Oracle lo ayuda a configurar, utilizar y escalar una base de datos relacional de Oracle en la Nube de AWS.

Otros servicios

- Oracle GoldenGate es un servicio que le ayuda a replicar, filtrar y transformar datos de una base de datos a otra base de datos heterogénea o a otra topología de destino, como archivos planos.
- Los adaptadores de GoldenGate aplicaciones de Oracle permiten GoldenGate a Oracle producir una serie de archivos planos secuenciales y archivos de control a partir de los datos transaccionales capturados en los archivos de seguimiento de una base de datos de origen. Estos adaptadores se utilizan ampliamente para operaciones de extracción, transformación y carga (ETL) en aplicaciones de data warehouse y en aplicaciones de propiedad o heredadas. Oracle GoldenGate realiza esta captura y la aplica prácticamente en tiempo real en bases de datos, plataformas y sistemas operativos heterogéneos. Los adaptadores admiten diferentes formatos para los archivos de salida, como CSV o Apache Parquet. Puede cargar estos archivos generados para cargar los datos en diferentes bases de datos heterogéneas.

Epics

Configure Oracle GoldenGate en el servidor de base de datos de origen

Tarea	Descripción	Habilidades requeridas
Descargue Oracle GoldenGate.	En el servidor de base de datos de origen, descargue Oracle, GoldenGate versión 12.2.0.1.1 o posterior. Para obtener instrucciones, consulte Descarga de Oracle GoldenGate (documentación de Oracle).	Administrador de base de datos
Instale Oracle GoldenGate.	Para obtener instrucciones, consulte Instalación de Oracle	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	GoldenGate (documentación de Oracle).	
Configure Oracle GoldenGate.	Para obtener instrucciones, consulte Preparación de la base de datos para Oracle GoldenGate (documentación de Oracle).	Administrador de base de datos

Configure Oracle GoldenGate en el servidor de integración

Tarea	Descripción	Habilidades requeridas
Descargue Oracle GoldenGate.	En el servidor de integración, descargue la GoldenGate versión 12.2.0.1.1 o posterior de Oracle. Para obtener instrucciones, consulte Descarga de Oracle GoldenGate (documentación de Oracle).	Administrador de base de datos
Instale Oracle GoldenGate.	Cree directorios, configure el proceso de administración y cree el archivo `defgen` para un entorno heterogéneo. Para obtener instrucciones, consulte Instalación de Oracle GoldenGate (documentación de Oracle).	Administrador de base de datos

Cambie la configuración de captura GoldenGate de datos de Oracle

Tarea	Descripción	Habilidades requeridas
Prepare los GoldenGate adaptadores de Oracle.	En el servidor de integración, configure el software del GoldenGate adaptador de Oracle. Haga lo siguiente: 1. Desde Oracle Software Delivery Cloud, descargue ggs_Adapters_Linux_x64.zip. 2. Descomprima ggs_Adapters_Linux_x64.zip. 3. Ejecute el siguiente comando para instalar los adaptadores: `tar -xvf ggs_Adapters_Linux_x64.tar`	Administrador de base de datos
Configure la bomba de datos.	En el servidor de origen, configure la bomba de datos para transferir el archivo de seguimiento del servidor de origen al servidor de integración. Cree el archivo de parámetros de la bomba de datos y el directorio de archivos de senderos. Para obtener instrucciones, consulte Configuración del adaptador de archivos planos (documentación de Oracle).	Administrador de base de datos

Generar y migrar los archivos planos

Tarea	Descripción	Habilidades requeridas
Genere los archivos planos.	Cree el archivo de extracción y el archivo de control y, a continuación, inicie el proceso de extracción en el servidor de integración. Esto extrae los cambios de la base de datos y graba la base de datos de origen en los archivos planos. Para obtener instrucciones, consulte Uso del adaptador de archivos planos (documentación de Oracle).	Administrador de base de datos
Cargue los archivos planos en la base de datos de destino.	Cargue los archivos planos en la instancia de base de datos de Amazon RDS para Oracle de destino. Para obtener más información, consulte Importación mediante Oracle SQL*Loader (documentación de Amazon RDS).	Administrador de base de datos

Resolución de problemas

Problema	Solución
El adaptador de archivos GoldenGate planos de Oracle genera un error.	Para obtener una descripción de los errores del adaptador, consulte Localización de mensajes de error (documentación de Oracle). Para obtener instrucciones de solución de problemas, consulte Solución de problemas del adaptador de archivos planos (documentación de Oracle).

Recursos relacionados

- Instalación de Oracle GoldenGate (documentación de Oracle)
- Configuración de Oracle GoldenGate (documentación de Oracle)
- Descripción de los GoldenGate adaptadores Oracle (documentación de Oracle)
- Configuración del adaptador de archivos planos (documentación de Oracle)

Cambie las aplicaciones de Python y Perl para que admitan la migración de bases de datos de Microsoft SQL Server a una edición compatible con PostgreSQL de Amazon Aurora

Dwarika Patra y Deepesh Jayaprakash, Amazon Web Services

Resumen

Este patrón describe los cambios en los repositorios de aplicaciones que pueden ser necesarios al migrar bases de datos de Microsoft SQL Server a una edición compatible con Amazon Aurora PostgreSQL. El patrón asume que estas aplicaciones están basadas en Python o en Perl, y proporciona instrucciones independientes para estos lenguajes de secuencias de comandos.

La migración de bases de datos de SQL Server a una versión compatible con Aurora PostgreSQL implica la conversión de esquemas, la conversión de objetos de base de datos, la migración de datos y la carga de datos. Debido a las diferencias entre PostgreSQL y SQL Server (en relación con los tipos de datos, los objetos de conexión, la sintaxis y la lógica), la tarea de migración más difícil consiste en realizar los cambios necesarios en la base de código para que funcione correctamente con PostgreSQL.

Para una aplicación basada en Python, los objetos y clases de conexión están dispersos por todo el sistema. Además, la base de código de Python puede usar varias bibliotecas para conectarse a la base de datos. Si la interfaz de conexión a la base de datos cambia, los objetos que ejecutan las consultas en línea de la aplicación también requieren cambios.

En el caso de una aplicación basada en Perl, los cambios se refieren a los objetos de conexión, los controladores de conexión a la base de datos, las sentencias SQL integradas estáticas y dinámicas y la forma en que la aplicación gestiona las consultas DML dinámicas y complejas y los conjuntos de resultados.

Al migrar la aplicación, también puede considerar posibles mejoras en AWS, como reemplazar el servidor FTP por el acceso a Amazon Simple Storage Service (Amazon S3).

El proceso de migración de la aplicación implica los siguientes desafíos:

- Objetos de conexión. Si los objetos de conexión están dispersos en el código con varias bibliotecas y llamadas a funciones, es posible que tenga que encontrar una forma generalizada de cambiarlos para que sean compatibles con PostgreSQL.
- Gestión de errores o excepciones durante la recuperación o actualización de registros. Si tiene operaciones condicionales de creación, lectura, actualización y eliminación (CRUD) en la base

de datos que devuelven variables, conjuntos de resultados o marcos de datos, cualquier error o excepción puede provocar errores de aplicación con efectos en cascada. Estas deben gestionarse con cuidado, con las validaciones adecuadas y ahorrándose puntos. Uno de estos puntos de ahorro es llamar a consultas SQL integradas de gran tamaño o a objetos de bases de datos dentro de bloques `BEGIN...EXCEPTION...END`.

- Controlar las transacciones y su validación. Esto incluye las confirmaciones y anulaciones manuales y automáticas. El controlador PostgreSQL para Perl requiere que siempre se establezca de forma explícita el atributo autocommit.
- Manejo de consultas SQL dinámicas. Esto requiere una sólida comprensión de la lógica de consultas y pruebas iterativas para garantizar que las consultas funcionen según lo esperado.
- Desempeño. Debe asegurarse de que los cambios en el código no reduzcan el rendimiento de la aplicación.

Este patrón explica el proceso de conversión en detalle.

Requisitos previos y limitaciones

Requisitos previos

- Conocimientos prácticos de la sintaxis de Python y Perl.
- Conocimientos básicos de SQL Server y PostgreSQL.
- Comprensión de la arquitectura de aplicaciones existente.
- Acceda al código de su aplicación, a la base de datos de SQL Server y a la base de datos PostgreSQL.
- Acceda al entorno de desarrollo Windows o Linux (u otro tipo de Unix) con credenciales para desarrollar, probar y validar los cambios en las aplicaciones.
- Para una aplicación basada en Python, las bibliotecas de Python estándar que pueda necesitar la aplicación, como Pandas para gestionar marcos de datos y psycopg2 o para conexiones a bases de datos. SQLAlchemy
- Para una aplicación basada en Perl, se requieren paquetes de Perl con bibliotecas o módulos dependientes. El módulo Comprehensive Perl Archive Network (CPAN) es compatible con la mayoría de los requisitos de las aplicaciones.
- Todas las bibliotecas o módulos personalizados dependientes necesarios.
- Credenciales de base de datos para el acceso de lectura a SQL Server y el read/write acceso a Aurora.

- PostgreSQL para validar y depurar los cambios en las aplicaciones con los servicios y los usuarios.
- Acceso a herramientas de desarrollo durante la migración de aplicaciones, como Visual Studio Code, Sublime Text o pgAdmin.

Limitaciones

- Algunas versiones, módulos, bibliotecas y paquetes de Python o Perl no son compatibles con el entorno de nube.
- Algunas bibliotecas y marcos de terceros utilizados para SQL Server no se pueden reemplazar para admitir la migración a PostgreSQL.
- Las variaciones de rendimiento pueden requerir cambios en la aplicación, en las consultas de Transact-SQL (T-SQL) integradas, en las funciones de las bases de datos y en los procedimientos almacenados.
- PostgreSQL admite nombres en minúsculas para nombres de tablas, nombres de columnas y otros objetos de bases de datos.
- Algunos tipos de datos, como las columnas UUID, se almacenan únicamente en minúsculas. Las aplicaciones Python y Perl deben gestionar estas diferencias entre mayúsculas y minúsculas.
- Las diferencias de codificación de caracteres deben gestionarse con el tipo de datos correcto para las columnas de texto correspondientes de la base de datos PostgreSQL.

Versiones de producto

- Python 3.6 o posterior (usa la versión compatible con su sistema operativo)
- Perl 5.8.3 o posterior (utilice la versión compatible con su sistema operativo)
- Aurora, compatible con PostgreSQL, edición 4.2 o posterior (consulte los detalles)

Arquitectura

Pila de tecnología de origen

- Lenguaje de secuencias de comandos (programación de aplicaciones): Python 2.7 o posterior, o Perl 5.8
- Base de datos: Microsoft SQL Server versión 13
- Sistema operativo: Red Hat Enterprise Linux (RHEL) 7

Pila de tecnología de destino

- Lenguaje de secuencias de comandos (programación de aplicaciones): Python 3.6 o posterior de Perl
- Base de datos: Compatible con Aurora PostgreSQL
- Sistema operativo: RHEL 7

Arquitectura de migración

Tools (Herramientas)

Servicios y herramientas de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de bases de datos relacionales, completamente administrado, compatible con PostgreSQL y conforme a ACID, que combina la velocidad y la fiabilidad de las bases de datos comerciales de tecnología avanzada con la sencillez y la rentabilidad de las bases de datos de código abierto. Aurora PostgreSQL es un reemplazo instántaneo para PostgreSQL que simplifica y hace más rentable configurar, usar y escalar las implementaciones de PostgreSQL nuevas y existentes.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.

Otras herramientas

- Bibliotecas de conexión a bases de datos de Python y PostgresSQL, como psycopg2 y SQLAlchemy
- Perl y sus módulos de DBI
- Terminal interactiva PostgreSQL (psql)

Epics

Migración de su repositorio de aplicaciones a PostgreSQL: pasos de alto nivel

Tarea	Descripción	Habilidades requeridas
Siga estos pasos de conversión de código para migrar su aplicación a PostgreSQL.	1. Configure bibliotecas y controladores ODBC específicos de la base de datos para PostgreSQL. Por ejemplo, puede usar uno de los módulos CPAN para Perl y pyodbc, psycopg2 o Python. SQLAlchemy 2. Convierta los objetos de la base de datos mediante estas bibliotecas para conectarse a Aurora compatible con PostgreSQL. 3. Aplique los cambios de código en los módulos de aplicación existentes para obtener sentencias T-SQL compatibles. 4. Reescriba las llamadas a funciones específicas de la base de datos y los procedimientos almacenados en el código de la aplicación. 5. Controle los cambios en las variables de la aplicación y sus tipos de datos que se	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	utilizan para las consultas SQL en línea. 6. Gestione funciones específicas de bases de datos incompatibles. 7. end-to-endPruebas completas del código de aplicación convertido para la migración de bases de datos. 8. Compare los resultados de Microsoft SQL Server con los de la aplicación que migró a PostgreSQL. 9. Realice una evaluación comparativa del rendimien to de las aplicaciones entre Microsoft SQL Server y PostgreSQL. 10. Revise los procedimi entos almacenados o las sentencias T-SQL en línea solicitadas por la aplicación para mejorar el rendimiento. Las siguientes epics proporcio nan instrucciones detalladas para algunas de estas tareas de conversión para aplicacio nes de Python y Perl.	

Tarea	Descripción	Habilidades requeridas
Use una lista de verificación para cada paso de la migración.	Añada lo siguiente a la lista de verificación para cada paso de la migración de la aplicación, incluido el paso final: • Revise la documentación de PostgreSQL para asegurarse de que todos los cambios son compatibles con el estándar PostgreSQL. • Compruebe si hay valores enteros y flotantes en las columnas. • Identifique el número de filas insertadas, actualizadas y extraídas, junto con los nombres y date/time sellos de las columnas. Puede utilizar una utilidad de diferencias o escribir un script para automatizar estas comprobaciones. • Realice las comprobaciones de rendimiento de las sentencias SQL integradas de gran tamaño y compruebe el rendimiento general de la aplicación. • Compruebe que los errores se gestionan correctamente en las operaciones de la base de datos y que el programa se cierre	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	correctamente utilizando varios try/catch bloques. • Asegúrese de que se hayan implementado los procesos de registro adecuados.	

Analice y actualice su aplicación: Base de código Python

Tarea	Descripción	Habilidades requeridas
Analice su base de código Python existente.	Su análisis debe incluir lo siguiente para facilitar el proceso de migración de la aplicación: • Identifique todos los objetos de conexión en el código. • Identifique todas las consultas SQL en línea incompatibles (como las sentencias T-SQL y los procedimientos almacenados) y analice los cambios necesarios. • Revise la documentación del código y realice un seguimiento del flujo de control para comprender la funcionalidad del código. Esto será útil más adelante, cuando pruebes la aplicación para comparar el rendimiento o la carga.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	• Comprenda el propósito de la aplicación para poder probarla eficazmente después de la conversió n de la base de datos. La mayoría de las aplicacio nes de Python que son aptas para la conversión con migraciones de bases de datos son fuentes que cargan datos de otras fuentes en tablas de bases de datos o extractores que recuperan datos de las tablas y los transform an en diferentes formatos de salida (como CSV, JSON o archivos planos) que son adecuados para crear informes o realizar llamadas a la API para realizar validaciones.	

Tarea	Descripción	Habilidades requeridas

Convierta sus conexiones de bases de datos para que sean compatibles con PostgreSQL.	La mayoría de las aplicaciones de Python utilizan la biblioteca pyodbc para conectarse con las bases de datos de SQL Server de la siguiente manera.
	
	`import pyodbc`
	`....`
	`try:`
	`conn_string = "Driver=ODBC Driver 17 for SQL Server;UID={};PWD={};Server={};Database={}".format (conn_user, conn_password, conn_server, conn_database)`
	`conn = pyodbc.connect(conn_string)`
	`cur = conn.cursor()`
	`result = cur.execute(query_string)`
	`for row in result:`
	`print (row)`
	`except Exception as e:`
	`print(str(e))`
	
	Convierta la conexión de base de datos para que sea compatible con PostgreSQL de la siguiente manera.
	
	`import pyodbc`
	`import psycopg2`
	`....`
	`try:`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	<pre> conn_string =
	 'postgresql+psycop
	g2://'+
	    conn_user+':'+conn
	_password+'@'+conn
	_server+'/'+conn_d
	atabase
	    conn = pyodbc.co
	nnect(conn_string,
	 connect_args={'opt
	ions':'-csearch_pa
	th=dbo'})
	    cur = conn.cursor()
	    result = cur.execu
	te(query_string)
	    for row in result:
	    print (row)
	except Exception as e:
	    print(str(e))</pre>	

Tarea	Descripción	Habilidades requeridas

Cambie las consultas SQL en línea a PostgreSQL.	Convierta sus consultas SQL en línea a un formato compatible con PostgreSQL. Por ejemplo, la siguiente consulta de SQL Server recupera una cadena de una tabla.
	
	`dtype = "type1"`
	`stm = ‘"SELECT TOP 1 searchcode FROM TypesTable (NOLOCK) WHERE code="’ + "’" + str(dtype) + "’"`
	`# For Microsoft SQL Server Database Connection`
	`engine = create_engine(‘mssql+pyodbc:///?odbc_connect=%s’ % urllib.parse.quote_plus(conn_string), connect_args={‘connect_timeout’:login_timeout})`
	`conn = engine_connect()`
	`rs = conn.execute(stm)`
	`for row in rs:`
	`print(row)`
	
	Tras la conversión, la consulta SQL en línea compatible con PostgreSQL tiene el siguiente aspecto.
	
	`dtype = "type1"`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	`stm = '"SELECT searchcode FROM TypesTable WHERE code="' + "'" + str(dtype) + "' LIMIT 1"`
	`# For PostgreSQL Database Connection`
	`engine = create_engine('postgres+psycopg2://%s' %conn_string, connect_args={'connect_timeout':login_timeout})`
	`conn = engine.connect()`
	`rs = conn.execute(stm)`
	`for row in rs:`
	`  print(row)`	

Tarea	Descripción	Habilidades requeridas

Gestione consultas SQL dinámicas.	El SQL dinámico puede estar presente en un script o en varios scripts de Python. Los ejemplos anteriores mostraron cómo utilizar la función de reemplazo de cadenas de Python para insertar variables con el fin de crear consultas SQL dinámicas. Un enfoque alternativo consiste en añadir variables a la cadena de consulta siempre que sea aplicable.
	
	En el ejemplo siguiente, la cadena de consulta se construye sobre la marcha en función de los valores devueltos por una función.
	
	`query = '"SELECT id from equity e join issues i on e.permId=i.permId where e.id'"`
	`query += get_id_filter(ids) + " e.id is NOT NULL`
	
	Estos tipos de consultas dinámicas son muy comunes durante la migración de aplicaciones. Siga estos pasos para gestionar consultas dinámicas:
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	• Compruebe la sintaxis general (por ejemplo, la sintaxis de la sentencia `SELECT` con una cláusula `JOIN`). • Compruebe todos los nombres de variables o columnas utilizados en la consulta, como `i` y `id`. • Compruebe las funciones, los argumentos y los valores devueltos utilizados en la consulta (por ejemplo, `get_id_filter` y su argumento `ids`).	

Tarea	Descripción	Habilidades requeridas

Gestione los conjuntos de resultados, las variables y los marcos de datos.	Para Microsoft SQL Server, se utilizan métodos de Python como `fetchone()` o `fetchall()` para recuperar el conjunto de resultados de la base de datos. También puede usar `fetchmany(size)` y especificar el número de registros que se van a devolver del conjunto de resultados. Para ello, puede utilizar el objeto de conexión pyodbc como se muestra en el siguiente ejemplo.
	
	pyodbc (Microsoft SQL Server)
	
	`import pyodbc`
	`server = 'tcp:myse`
	`rver.database.wind`
	`ows.net'`
	`database = 'exampledb'`
	`username = 'exampleu`
	`sername'`
	`password = 'examplep`
	`assword'`
	`conn = pyodbc.co`
	`nnect('DRIVER={ODB`
	`C Driver 17 for SQL`
	` Server};SERVER='+s`
	`erver+';DATABASE='`
	`+database+';UID='+`
	`username+';PWD='+`
	` password)`
	`cursor = conn.cursor()`
	`cursor.execute("SELECT`
	` * FROM ITEMS")`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	row = cursor.fe
	tchone()
	while row:
	    print(row[0])
	    row = cursor.fe
	tchone()
	
	En Aurora, para realizar tareas similares, como conectars e a PostgreSQL y obtener conjuntos de resultados, puede usar psycopg2 o. SQLAlchemy Estas bibliotec as de Python proporcionan el módulo de conexión y el objeto de cursor para recorrer los registros de la base de datos PostgreSQL, como se muestra en el siguiente ejemplo.
	
	psycopg2 (Aurora compatible con PostgreSQL)
	
	import psycopg2
	query = "SELECT * FROM
	ITEMS;"
	//Initialize
	variables
	host=dbname=user=
	password=port=sslm
	ode=connect_timeou
	t=""
	connstring = "host='{h
	ost}' dbname='{
	dbname}' user='{user}'
	\	

Tarea	Descripción	Habilidades requeridas
	password='{passw ord}'port='{port}' ".format(host=host ,dbname=dbname,\ user=user,password= password,port=port) conn = psycopg2. connect(connstring) cursor = conn.cursor() cursor.execute(query) column_names = [column[0] for column in cursor.description] print("Column Names: ", column_names) print("Column values: " for row in cursor: print("itemid :", row[0]) print("itemdescrpt ion :", row[1]) print("it emprice :", row[3])) SQLAlchemy (Compatible con Aurora PostgreSQL) from sqlalchemy import create_engine from pandas import DataFrame conn_string = 'postgres ql://core:database @localhost:5432/ex ampledatabase' engine = create_en gine(conn_string) conn = engine.co nnect() dataid = 1001	

Tarea	Descripción	Habilidades requeridas
	`result = conn.exec ute("SELECT * FROM ITEMS") df = DataFrame (result.fetchall()) df.columns = result.ke ys() df = pd.DataFrame() engine.connect() df = pd.read_sql_query( sql_query, engine, coerce_float=False) print("df=", df)`	

Tarea	Descripción	Habilidades requeridas
Pruebe la aplicación durante y después de la migración.	La prueba de la aplicación Python migrada es un proceso continuo. Como la migración incluye cambios en los objetos de conexión (psycopg2 o SQLAlchemy), la gestión de errores, nuevas funciones (marcos de datos), cambios en el SQL en línea, funcionalidades de copia masiva (`bcp` en lugar de `COPY`) y cambios similares, debe probarse detenidamente durante y después de la migración de la aplicación. Consultar si: • Condiciones y manejo del error • Algún desajuste en los registros tras la migración • Actualizaciones o eliminaciones de registros • Tiempo necesario para poder ejecutar la aplicación	Desarrollador de aplicaciones

Analice y actualice su aplicación: base de código Perl

Tarea	Descripción	Habilidades requeridas
Analice su base de código Perl existente.	Su análisis debe incluir lo siguiente para facilitar el proceso de migración de la aplicación. Debe identificar:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	• Cualquier código INI o basado en la configuración • Controladores Perl de Open Database Connectivity (ODBC) estándar para bases de datos específicos de bases de datos o cualquier controlador personalizado • Se requieren cambios de código para las consultas en línea y T-SQL • Interacciones entre varios módulos de Perl (por ejemplo, un único objeto de conexión ODBC de Perl al que varios componentes funcionales llaman o utilizan) • Manejo de conjuntos de datos y conjuntos de resultados • Bibliotecas de Perl externas y dependientes • Todas las APIs que se utilicen en la aplicación • Compatibilidad de versiones de Perl y compatibilidad de controladores con Aurora compatible con PostgreSQL	

Tarea	Descripción	Habilidades requeridas

Convierta las conexiones de la aplicación Perl y el módulo DBI para que sean compatibl es con PostgreSQL.	Las aplicaciones basadas en Perl suelen utilizar el módulo DBI de Perl, que es un módulo de acceso a bases de datos estándar para el lenguaje de programación Perl. Puede usar el mismo módulo DBI con controladores diferentes para SQL Server y PostgreSQL.
	
	Para obtener más informaci ón sobre los módulos de Perl necesarios, las instalaci ones y otras instrucciones, consulte la documentación de DBD::Pg. El siguiente ejemplo se conecta a Aurora compatible con PostgreSQL en `exampletest-aurora pg-database.cluste r-sampleclusture.u s-east-.rds.amazon aws.com` .
	
	`#!/usr/bin/perl`
	`use DBI;`
	`use strict;`
	`my $driver = "Pg";`
	`my $hostname = "examplet`
	`est-aurorapg-datab`
	`ase-sampleclusture`
	`.us-east.rds.amazo`
	`naws.com"`
	`my $dsn = "DBI:$driver:`
	` dbname = $hostname`
	`;host = 127.0.0.1;port`
	` = 5432";`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	`my $username = "postgres";`
	`my $password = "pass123";`
	`$dbh = DBI->connect("dbi:Pg:dbname=$hostname;host=$host;port=$port;options=$options",`
	`$username,`
	`$password,`
	`{AutoCommit => 0, RaiseError => 1, PrintError => 0}`
	`);`	

Tarea	Descripción	Habilidades requeridas

Cambie las consultas SQL en línea a PostgreSQL.	Es posible que su aplicación tenga consultas SQL en línea con `SELECT`, `DELETE`, `UPDATE` y sentencias similares que incluyan cláusulas de consulta que PostgreSQL no admite. Por ejemplo, consulte palabras clave como `TOP` y `NOLOCK` no se admiten en PostgreSQL. En los siguientes ejemplos, se muestra cómo se pueden gestionar `TOP`, `NOLOCK` y variables booleanas.
	
	En SQL Server:
	
	`$sqlStr = $sqlStr . "WHERE a.student_id in (SELECT TOP $numofRecords c_student_id \ FROM active_student_record b WITH (NOLOCK) \ INNER JOIN student_contributor c WITH (NOLOCK) on c.contributor_id = b.c_st)`
	
	Para PostgreSQL, conviértalo a:
	
	`$sqlStr = $sqlStr . "WHERE a.student_id in (SELECT TOP $numofRecords c_student_id \`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	FROM active_student_rec ord b INNER JOIN student_contributor c \ on c.contributor_id = b.c_student_contr_id WHERE b_current_1 is true \ LIMIT $numofRecords)"	

Tarea	Descripción	Habilidades requeridas
Gestione consultas SQL dinámicas y variables de Perl.	Las consultas SQL dinámicas son sentencias SQL que se crean durante el tiempo de ejecución de la aplicación. Estas consultas se crean de forma dinámica cuando la aplicación está en ejecución , en función de determinadas condiciones, por lo que el texto completo de la consulta no se conoce hasta el tiempo de ejecución. Un ejemplo es una aplicación de análisis financiero que analiza las 10 principales acciones a diario, y estas acciones cambian todos los días. Las tablas SQL se crean en función de los mejores resultados y los valores no se conocen hasta el tiempo de ejecución. Supongamos que las consultas SQL en línea de este ejemplo se pasan a una función contenedora para obtener los resultados establecidos en una variable y, a continuación, una variable utiliza una condición para determinar si la tabla existe: • Si la tabla existe, no la cree; procésela.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	• Si la tabla no existe, créela y, a continuación, procésela.
	
	A continuación, se muestra un ejemplo de gestión de variables, seguido de las consultas de SQL Server y PostgreSQL para este caso de uso.
	
	`my $tableexists = db_read( arg 1, $sql_qry, undef, 'writer'); my $table_already_exists = $tableexists->[0]{table_exists}; if ($table_already_exists){ # do some thing } else { # do something else }`
	
	SQL Server:
	
	`my $sql_qry = "SELECT OBJECT_ID('$backendTable', 'U') table_exists", undef, 'writer') ";`
	
	PostgreSQL:
	
	`my $sql_qry = "SELECT TO_REGCLASS('$backendTable', 'U')`	

Tarea	Descripción	Habilidades requeridas

	table_exists", undef, 'writer')";
	
	En el siguiente ejemplo, se utiliza una variable de Perl en SQL en línea, que ejecuta una sentencia `SELECT` con un `JOIN` para obtener la clave principal de la tabla y la posición de la columna clave.
	
	SQL Server:
	
	`my $sql_qry = "SELECT column_name', character_maxi mum_length \ FROM INFORMATION_SCHEMA .COLUMNS \ WHERE TABLE_SCH EMA='$example_sche maInfo' \ AND TABLE_NAME='$examp le_table' \ AND DATA_TYPE IN ('varchar','nvarch ar');";`
	
	PostgreSQL:
	
	`my $sql_qry = "SELECT c1.column_name, c1.ordinal_position \ FROM information_schema .key_column_usage AS c LEFT \ JOIN information_schema .table_constraints AS t1 \`	

Tarea	Descripción	Habilidades requeridas
	`ON t1.constraint_name = c1.constraint_name \ WHERE t1.table_name = $example_schemaInfo'.'$example_table' \ AND t1.constraint_type = 'PRIMARY KEY' ;";`	

Realice cambios adicionales en su aplicación basada en Perl o Python para admitir PostgreSQL

Tarea	Descripción	Habilidades requeridas
Convierta construcciones adicionales de SQL Server a PostgreSQL.	Los siguientes cambios se aplican a todas las aplicaciones, independientemente del lenguaje de programación. • Califique los objetos de base de datos que utiliza su aplicación con nombres de esquema nuevos y adecuados. • Gestione los operadores LIKE para hacer coincidir mayúsculas de minúsculas con la característica de intercalación de PostgreSQL. • Gestione funciones específicas de bases de datos no compatibles, como `DATEDIFF`, `DATEADD`, `GETDATE`, `CONVERT` y los operadores `CAST`. Para ver funciones equivalentes	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	compatibles con PostgreSQL, consulte Funciones SQL nativas o integradas en la sección Información adicional. • Maneje los valores booleanos en las declaraciones comparativas. • Maneje los valores de retorno de las funciones. Pueden ser conjuntos de registros, marcos de datos, variables y valores booleanos. Gestiónelos de acuerdo con los requisitos de su aplicación y para admitir PostgreSQL. • Gestione bloques anónimos (por ejemplo, `BEGIN TRAN`) con nuevas funciones de PostgreSQL definidas por el usuario. • Convierta inserciones masivas en filas. El equivalente en PostgreSQL de la utilidad Copia masiva (`bcp`) de SQL Server, a la que se llama desde dentro de la aplicación, es `COPY`. • Convierta los operadores de concatenación de columnas. SQL Server usa + para la	

Tarea	Descripción	Habilidades requeridas
	concatenación de cadenas, pero PostgreSQL usa ||.	

Mejoró el desempeño

Tarea	Descripción	Habilidades requeridas
Aproveche los servicios de AWS para mejorar el rendimiento.	Al migrar a la nube de AWS, puede refinar el diseño de sus aplicaciones y bases de datos para aprovechar los servicios de AWS. Por ejemplo, si las consultas de su aplicación Python, que está conectada a un servidor de bases de datos compatibl e con Aurora PostgreSQL, tardan más que las consultas originales de Microsoft SQL Server, podría considerar la posibilidad de crear una fuente de datos históricos directamente a un bucket de Amazon Simple Storage Service (Amazon S3) desde el servidor Aurora y utilizar consultas SQL basadas en Amazon Athena para generar informes y consultas de datos analíticos para sus usuarios. cuadros de mando.	Desarrollador de aplicaciones, arquitecto de la nube

Recursos relacionados

- Perl
- Módulo Perl DBI
- Python
- psycopg2
- SQLAlchemy
- Copia masiva - PostgreSQL
- Copia masiva - Microsoft SQL Server
- PostgreSQL
- Uso de Amazon Aurora PostgreSQL

Información adicional

Tanto Microsoft SQL Server como Aurora PostgreSQL son compatibles con ANSI SQL. Sin embargo, debe tener en cuenta cualquier incompatibilidad en la sintaxis, los tipos de datos de columnas, las funciones nativas específicas de las bases de datos, las inserciones masivas y la distinción entre mayúsculas y minúsculas cuando migre su aplicación de Python o Perl de SQL Server a PostgreSQL.

Las siguientes secciones brindan más información sobre posibles inconsistencias.

Comparación de tipos de datos

Los cambios en el tipo de datos de SQL Server a PostgreSQL pueden provocar diferencias significativas en los datos resultantes en los que funcionan las aplicaciones. Para ver una comparación de los tipos de datos, consulte la tabla del sitio web de Sqlines.

Funciones SQL nativas o integradas

El comportamiento de algunas funciones difiere entre las bases de datos de SQL Server y PostgreSQL. La siguiente tabla muestra una comparación.

Microsoft SQL Server	Description (Descripción)	PostgreSQL
`CAST`	Convierte un valor de un tipo de datos a otro tipo.	PostgreSQL `type :: operator`

`GETDATE()`	Devuelve la fecha y la hora del sistema de base de datos actual, en un formato `YYYY-MM-DD hh:mm:ss.mmm` .	`CLOCK_TIMESTAMP`
`DATEADD`	Añade un time/date intervalo a una fecha.	`INTERVAL` expression
`CONVERT`	Convierte un valor en un formato de datos específico.	`TO_CHAR`
`DATEDIFF`	Devuelve la diferencia entre dos campos de fecha.	`DATE_PART`
`TOP`	Limita el número de filas de un conjunto de resultados de `SELECT`.	`LIMIT/FETCH`

Bloques anónimos

Una consulta SQL estructurada se organiza en secciones como la declaración, los ejecutables y el manejo de excepciones. En la siguiente tabla se comparan las versiones Microsoft SQL Server y PostgreSQL de un bloque anónimo simple. En el caso de bloques anónimos complejos, le recomendamos que llame una función de base de datos personalizada en su aplicación.

Microsoft SQL Server

```
my $sql_qry1=
my $sql_qry2 =
my $sqlqry = "BEGIN TRAN
$sql_qry1 $sql_qry2
if @\@error !=0 ROLLBACK
TRAN
else COMIT TRAN";
```

PostgreSQL

```
my $sql_qry1=
my $sql_qry2 =
my $sql_qry = " DO \$\$
BEGIN
$header_sql $content_sql
END
\$\$";
```

Otras diferencias

- Inserciones masivas de filas: el equivalente en PostgreSQL de la utilidad bcp de Microsoft SQL Server es COPY.
- Distinción entre mayúsculas y minúsculas: los nombres de las columnas distinguen entre mayúsculas y minúsculas en PostgreSQL, por lo que debe convertir los nombres de las columnas de SQL Server a minúsculas o mayúsculas. Esto se convierte en un factor al extraer o comparar datos, o al colocar los nombres de las columnas en los conjuntos de resultados o las variables. El siguiente ejemplo identifica las columnas en las que los valores se pueden almacenar en mayúsculas o minúsculas.

```
my $sql_qry = "SELECT $record_id FROM $exampleTable WHERE LOWER($record_name) =
 \'failed transaction\'";
```

- Concatenación: SQL Server usa + como operador para la concatenación de cadenas, mientras que PostgreSQL usa `||`.
- Validación: debe probar y validar las consultas y funciones de SQL en línea antes de usarlas en el código de la aplicación para PostgreSQL.
- Inclusión de la biblioteca ORM: también puede buscar incluir o reemplazar la biblioteca de conexiones de bases de datos existente con bibliotecas ORM de Python, como SQLAlchemyPynomoDB. Esto ayudará a consultar y manipular fácilmente los datos de una base de datos utilizando un paradigma orientado a objetos.

Patrones de migración por carga de trabajo

Temas

- IBM
- Microsoft
- N/A
- Código abierto
- Oracle
- SAP

IBM

- Migre una base de datos Db2 de Amazon EC2 a Aurora compatible con MySQL mediante AWS DMS
- Migre Db2 for LUW a Amazon EC2 mediante el envío de registros para reducir el tiempo de interrupción
- Migración de Db2 para LUW a Amazon EC2 con recuperación de desastres de alta disponibilidad
- Migre de IBM Db2 en Amazon EC2 a Aurora compatible con PostgreSQL mediante AWS DMS y AWS SCT
- Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2

Microsoft

- Acelere el descubrimiento y la migración de las cargas de trabajo de Microsoft a AWS
- Cambie las aplicaciones de Python y Perl para que admitan la migración de bases de datos de Microsoft SQL Server a una edición compatible con PostgreSQL de Amazon Aurora
- Cree CloudFormation plantillas de AWS para las tareas de AWS DMS con Microsoft Excel y Python
- Exportación de una base de datos de Microsoft SQL Server a Amazon S3 mediante AWS DMS
- Implemente SHA1 el hash para los datos de PII al migrar de SQL Server a PostgreSQL
- Incorpore y migre instancias de EC2 Windows a una cuenta de AWS Managed Services
- Migración de una cola de mensajes de Microsoft Azure Service Bus a Amazon SQS
- Migre una base de datos de Microsoft SQL Server de Amazon EC2 a Amazon DocumentDB mediante AWS DMS
- Migración de una base de datos de Microsoft SQL Server a Aurora MySQL mediante AWS DMS y AWS SCT
- Migración de una aplicación .NET de Microsoft Azure App Service a AWS Elastic Beanstalk
- Migre una base de datos local de Microsoft SQL Server a Amazon EC2
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server
- Migración de bases de datos en las instalaciones de Microsoft SQL Server a Amazon RDS para SQL Server mediante servidores vinculados
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server mediante métodos nativos de copia de seguridad y restauración
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon Redshift mediante AWS DMS
- Migración de una base de datos en las instalaciones de Microsoft SQL Server a Amazon Redshift mediante agentes de extracción de datos de AWS SCT
- Migre una base de datos local de Microsoft SQL Server a Microsoft SQL Server en Amazon EC2 con Linux
- Migración de datos de Microsoft Azure Blob a Amazon S3 mediante Rclone
- Migre IIS-hosted aplicaciones a Amazon EC2 mediante appcmd.exe
- Migre una base de datos local de Microsoft SQL Server a Amazon EC2 mediante MGN

- Migración de los certificados SSL de Windows a un equilibrador de carga de aplicación mediante ACM
- Vuelva a alojar las cargas de trabajo en las instalaciones en la nube de AWS: lista de verificación de migración
- Resolver los errores de conexión después de migrar Microsoft SQL Server a la nube de AWS
- Configure una infraestructura Multi-AZ para una FCI Always On de SQL Server mediante Amazon FSx

N/A

- Cree un proceso de aprobación para las solicitudes de firewall durante una migración de rehospedaje a AWS

Código abierto

- Crear usuarios y roles de aplicaciones en Aurora compatible con PostgreSQL
- Migre Amazon RDS for Oracle a Amazon RDS for PostgreSQL con y utilizando y AWS SCT AWS DMS AWS CLI CloudFormation
- Migración de una base de datos de MariaDB en las instalaciones hasta Amazon RDS para MariaDB mediante herramientas nativas
- Migración de una base de datos MySQL en las instalaciones a Amazon RDS para MySQL
- Migración de una base de datos de MySQL en las instalaciones a Aurora MySQL
- Migración de una base de datos PostgreSQL en las instalaciones a Aurora PostgreSQL
- Migrar una base de datos de Couchbase Server a Amazon EC2
- Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2 con Auto Scaling
- Migre de PostgreSQL en EC2 Amazon a Amazon RDS para PostgreSQL mediante pglogical
- Migración de aplicaciones Java locales en las instalaciones a AWS mediante AWS App2Container
- Migre bases de datos MySQL locales a Aurora MySQL mediante Percona, XtraBackup Amazon EFS y Amazon S3
- Migración de tablas externas de Oracle a Amazon Aurora compatible con PostgreSQL
- Reinicie automáticamente el AWS El agente de replicación tras un reinicio de RHEL sin deshabilitar SELinux
- Transportar bases de datos PostgreSQL entre dos instancias de base de datos de Amazon RDS utilizando pg_transport

Oracle

- Convierta VARCHAR2 (1) el tipo de datos de Oracle en un tipo de datos booleano para Amazon Aurora PostgreSQL
- Emule Oracle DR mediante una base de datos global de Aurora compatible con PostgreSQL
- Migración gradual de Amazon RDS para Oracle a Amazon RDS para PostgreSQL con Oracle SQL Developer y AWS SCT
- Cargar archivos BLOB en TEXT mediante la codificación de archivos en Aurora compatible con PostgreSQL
- Migración de Amazon RDS para Oracle a Amazon RDS para PostgreSQL en modo SSL mediante AWS DMS
- Migre una base de datos de Amazon RDS for Oracle a Cuenta de AWS otra Región de AWS y AWS DMS utilícela para la replicación continua
- Migre una base de datos Oracle local a Amazon EC2 mediante Oracle Data Pump
- Migre una base de datos Oracle local a Amazon OpenSearch Service mediante Logstash
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para MySQL con AWS DMS y AWS SCT
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para PostgreSQL mediante Oracle Bystander y AWS DMS
- Migre una base de datos Oracle local a Oracle on Amazon EC2
- Migre una base de datos Oracle de Amazon EC2 a Amazon RDS para MariaDB con AWS DMS y AWS SCT
- Migre una base de datos Oracle de Amazon EC2 a Amazon RDS for Oracle mediante AWS DMS
- Migre una base de datos Oracle a Amazon RDS for Oracle mediante adaptadores de archivos planos de GoldenGate Oracle
- Migración de una base de datos de Oracle a Amazon Redshift con AWS DMS y AWS SCT
- Migración de una base de datos de Oracle a Aurora PostgreSQL con AWS DMS y AWS SCT
- Migre una EnterpriseOne base de datos de Oracle JD Edwards a AWS mediante Oracle Data Pump y AWS DMS
- Migración de una tabla particionada de Oracle a PostgreSQL mediante AWS DMS

- Migre una PeopleSoft base de datos de Oracle a AWS mediante AWS DMS
- Migración de datos de una base de datos de Oracle en las instalaciones a Aurora PostgreSQL
- Migración de de Amazon RDS para Oracle a Amazon RDS para MySQL
- Migración de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante la vista materializada y AWS DMS
- Migre de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante AWS DMS SharePlex
- Migre de Oracle Database a Amazon RDS for PostgreSQL mediante Oracle GoldenGate
- Migración de Oracle en Amazon EC2 a Amazon RDS para MySQL con AWS DMS y AWS SCT
- Migre de Oracle WebLogic a Apache Tomcat (ToMEE) en Amazon ECS
- Migración de índices basados en funciones de Oracle a PostgreSQL
- Migración de aplicaciones heredadas de Oracle Pro*C a ECPG
- Migración de valores CLOB de Oracle a filas individuales en PostgreSQL en AWS
- Migración de códigos de error de Oracle Database a una base de datos Amazon Aurora compatible con PostgreSQL
- Migración de las funciones nativas de Oracle a PostgreSQL mediante extensiones
- Migre Oracle PeopleSoft a Amazon RDS Custom
- Migración de la funcionalidad ROWIdentificador de Oracle a PostgreSQL en AWS
- Migración de los paquetes pragma SERIALLY_REUTILIZABLE de Oracle a PostgreSQL
- Migración de columnas generadas de forma virtual de Oracle a PostgreSQL
- Configure la funcionalidad UTL_FILE de Oracle en Aurora compatible con PostgreSQL
- Validar los objetos de la base de datos después de migrar de Oracle a Amazon Aurora PostgreSQL

SAP

- Migración de SAP ASE a Amazon RDS para SQL Server utilizando AWS DMS
- Migre SAP ASE de Amazon EC2 a Amazon Aurora compatible con PostgreSQL mediante AWS SCT y AWS DMS

Más patrones

- Acceda Servicios de AWS desde IBM z/OS instalando el AWS CLI
- Evaluar el rendimiento de las consultas para migrar bases de datos de SQL Server a MongoDB Atlas en AWS
- Automatización de la conmutación por error y la conmutación por recuperación entre regiones mediante DR Orchestrator Framework
- Automatice las tareas de bases de datos en SQL Server Express en Amazon EC2 mediante un programador AWS Lambda de tareas
- Cree un visor de archivos de unidad central avanzada en la nube de AWS
- Connect to MGN data and control planes over a private network
- Almacenamiento en contenedores de las cargas de trabajo de mainframe que Blu Age ha modernizado
- Convertir consultas JSON de Oracle en SQL de bases de datos PostgreSQL
- Convierta la característica temporal NORMALIZE de Teradata en Amazon Redshift SQL
- Convierta la característica RESET WHEN de Teradata en Amazon Redshift SQL
- Copie tablas de Amazon DynamoDB entre cuentas mediante AWS Backup
- Implemente un clúster de Cassandra en Amazon EC2 con estática privada IPs para evitar el reequilibrio
- Implemente aplicaciones de varias pilas mediante AWS CDK con TypeScript
- Implemente instancias de clústeres de conmutación por error de SQL Server en Amazon EC2 y Amazon FSx mediante Terraform
- Emule las matrices PL/SQL asociativas de Oracle en Amazon Aurora PostgreSQL y Amazon RDS for PostgreSQL
- Calcule el tamaño del motor de Amazon RDS para una base de datos de Oracle mediante informes de AWR
- Genere información de datos mediante AWS Mainframe Modernization Amazon Q en Quick Sight
- Gestionar bloques anónimos en instrucciones SQL dinámicas en Aurora PostgreSQL
- Identificación automática de las imágenes de contenedor duplicadas al migrar a un repositorio de Amazon ECR
- Configure un clúster de conmutación por error de Microsoft SQL Server en Amazon EC2 FSx mediante Windows File Server

- Migración de cargas de trabajo de Apache Cassandra a Amazon Keyspaces mediante AWS Glue
- Migre sus cargas de trabajo de contenedores de Azure Red Hat OpenShift (ARO) a Red Hat OpenShift Service en AWS (ROSA)
- Migre de Oracle 8i o 9i a Amazon RDS para Oracle con AWS DMS SharePlex
- Migre el grupo de disponibilidad Always On de Microsoft SQL Server mediante AWS Transform MGN
- Migración de funciones y procedimientos de Oracle con más de 100 argumentos a PostgreSQL
- Migración de SAP HANA a AWS mediante SAP HSR con el mismo nombre de host
- Migración de SQL Server a AWS mediante grupos de disponibilidad distribuidos
- Modernice e implemente aplicaciones de mainframe con Terraform AWS Transform
- Modernizar las cargas de trabajo de impresión en línea de mainframe en AWS mediante Micro Focus Enterprise Server y LRS VPSX/MFI
- Modernice la administración de la producción del mainframe AWS mediante Rocket Enterprise Server y LRS X PageCenter
- Cómo modificar los encabezados HTTP al migrar de F5 a un equilibrador de carga de aplicación en AWS
- Administración de la conmutación por error de multi-AZ para clústeres de EMR mediante el Controlador de recuperación de aplicaciones
- Análisis de las dependencias de los objetos para realizar migraciones parciales de bases de datos de Oracle a PostgreSQL
- Configure una CI/CD canalización para la migración de bases de datos mediante Terraform
- Configure la recuperación ante desastres para Oracle JD Edwards EnterpriseOne con AWS Elastic Disaster Recovery
- Simplifique la administración de certificados privados mediante AWS Private CA y AWS RAM
- Transfiera z/OS datos de Db2 a gran escala a Amazon S3 en archivos CSV
- Transforma Easytrieve a lenguajes modernos usando AWS Transform personalizado

Modernización

Temas

- Archivar automáticamente los elementos en Amazon S3 con DynamoDB TTL
- Cree una arquitectura sin servidor multiusuario en Amazon Service OpenSearch
- Implemente aplicaciones de varias pilas mediante AWS CDK con TypeScript
- Automatice la implementación de aplicaciones anidadas mediante SAM de AWS
- Implemente el aislamiento de inquilinos de SaaS para Amazon S3 mediante una máquina expendedora de AWS Lambda fichas
- Implementar el patrón saga sin servidor mediante AWS Step Functions
- Gestión de las aplicaciones de contenedores en las instalaciones mediante la configuración de Amazon ECS Anywhere con AWS CDK
- Incorporación de inquilinos en la arquitectura SaaS para el modelo de silo mediante C# y AWS CDK
- Descomponga monolitos en microservicios mediante CQRS y abastecimiento de eventos
- Más patrones

Archivar automáticamente los elementos en Amazon S3 con DynamoDB TTL

Tabby Ward, Amazon Web Services

Resumen

Este patrón proporciona los pasos para eliminar datos antiguos de una tabla de Amazon DynamoDB y archivarlos en un bucket de Amazon Simple Storage Service (Amazon S3) en Amazon Web Services (AWS) sin tener que gestionar una flota de servidores.

Este patrón utiliza el Tiempo de vida (TTL) de Amazon DynamoDB para eliminar automáticamente los elementos antiguos y Amazon DynamoDB Streams para capturar los elementos de TTL que han vencido. A continuación, conecta DynamoDB Streams a AWS Lambda, que ejecuta el código sin aprovisionar ni administrar ningún servidor.

Cuando se añaden nuevos elementos al flujo de DynamoDB, se inicia la función de Lambda y escribe los datos en un flujo de entrega de Amazon Data Firehose. Firehose proporciona una solución sencilla y totalmente administrada para cargar los datos como un archivo en Amazon S3.

DynamoDB se utiliza a menudo para almacenar datos de serie temporal, como datos de secuencias de clics de páginas web o datos de Internet de las cosas (IoT) procedentes de sensores y dispositivos conectados. En lugar de eliminar los elementos a los que se accede con menos frecuencia, muchos clientes prefieren archivarlos con fines de auditoría. TTL simplifica este archivado, ya que elimina automáticamente los elementos en función del atributo de marca de tiempo.

Los elementos que TTL ha eliminado pueden identificarse en DynamoDB Streams, que captura una secuencia en orden cronológico de las modificaciones de los elementos y almacena la secuencia en un registro durante 24 horas como máximo. Una función de Lambda puede consumir estos datos y archivarlos en un bucket de Amazon S3 para reducir el costo de almacenamiento. Para reducir aún más los costes, se pueden crear reglas de ciclo de vida de Amazon S3 para hacer la transición automática de los datos (tan pronto como se creen) a las clases de almacenamiento de menor coste.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.

- Interfaz de la línea de comandos de AWS (AWS CLI) 1.7 o posterior, instalada y configurada en macOS, Linux o Windows.
- Python 3.7 o versiones posteriores.
- Boto3, instalado y configurado. Si Boto3 no está instalado, ejecute el comando `python -m pip install boto3` para instalarlo.

Arquitectura

Pila de tecnología

- Amazon DynamoDB
- Amazon DynamoDB Streams
- Amazon Data Firehose
- AWS Lambda
- Amazon S3

1. TTL elimina los elementos.
2. El activador de flujos de DynamoDB invoca la función de procesador de flujos Lambda.
3. La función de Lambda coloca los registros en el flujo de entrega de Firehose en formato de lote.
4. Los registros de datos se archivan en el bucket de S3.

Tools (Herramientas)

- AWS CLI: la interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta unificada para administrar los servicios de AWS.
- Amazon DynamoDB: Amazon DynamoDB es una base de datos de documentos y valores clave que ofrece un rendimiento de milisegundos de un solo dígito a cualquier escala.
- Tiempo de vida (TTL) de Amazon DynamoDB: TTL de Amazon DynamoDB le permite definir una marca temporal por elemento para determinar cuándo ya no se necesita un elemento.
- Amazon DynamoDB Streams: Amazon DynamoDB Streams captura una secuencia en orden cronológico de las modificaciones de los elementos en una tabla de DynamoDB y almacena esta información en un registro durante 24 horas como máximo.

- Amazon Data Firehose: Amazon Data Firehose es la forma más sencilla de cargar datos de streaming con fiabilidad en lagos de datos, almacenes de datos y servicios de análisis.
- AWS Lambda: AWS Lambda ejecuta código sin necesidad de aprovisionar ni administrar servidores. Solo paga por el tiempo de computación que consume.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento líderes del sector.

Código

El código de este patrón está disponible en los elementos de GitHub Archivar en S3 mediante el repositorio TTL de DynamoDB.

Epics

Configurar una tabla de DynamoDB, un TTL y una transmisión de DynamoDB

Tarea	Descripción	Habilidades requeridas

Crear una tabla de DynamoDB.	Utilice la CLI de AWS para crear una tabla en DynamoDB llamada `Reservation` . Seleccione una unidad de capacidad de lectura (RCU) y una unidad de capacidad de escritura (WCU) al azar, y asigne a su tabla dos atributos: `ReservationID` y `ReservationDate` .
	
	`aws dynamodb create-table \`
	`--table-name Reservation \`
	`--attribute-definitions AttributeName=ReservationID,AttributeType=S`
		Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`AttributeName=ReservationDate,AttributeType=N \ --key-schema AttributeName=ReservationID,KeyType=HASH AttributeName=ReservationDate,KeyType=RANGE \ --provisioned-throughput ReadCapacityUnits=100,WriteCapacityUnits=100` `ReservationDate` es una marca de tiempo epoch que se utilizará para activar el TTL.	
Active el TTL de DynamoDB.	Utilice la CLI de AWS para activar el TTL de DynamoDB para el atributo `ReservationDate` . `aws dynamodb update-time-to-live \ --table-name Reservation\ --time-to-live-specification Enabled=true,AttributeName=ReservationDate`	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Active un flujo de DynamoDB.	Utilice la CLI de AWS para activar un flujo de DynamoDB para la tabla `Reservation` mediante el tipo de flujo `NEW_AND_OLD_IMAGES`.
	
	`aws dynamodb update-table \`
	`--table-name Reservation \`
	`  --stream-specification StreamEnabled=true,StreamViewType=NEW_AND_OLD_IMAGES`
	
	Este flujo contendrá registros de los elementos nuevos, los elementos actualizados, los elementos eliminados y los elementos eliminados por TTL. Los registros de los elementos que se eliminan mediante TTL incluyen un atributo de metadatos adicional para distinguirlos de los elementos que se eliminaron manualmente. El campo `userIdentity` para eliminaciones de TTL indica que el servicio DynamoDB realizó la acción de eliminación.
	
	En este patrón, solo se archivan los elementos
		Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	eliminados por TTL, pero solo puede archivar los registros donde `eventName` sea `REMOVE` y `userIdentity` incluya `principalId` igual a `dynamodb.amazonaws.com`.	

Crear y configurar un bucket de S3

Tarea	Descripción	Habilidades requeridas

Cree un bucket de S3.	Utilice la CLI de AWS para crear un bucket de S3 de destino en su región de AWS, `us-east-1` sustituyéndolo por su región y amzn-s3-demo-destination-bucket por el nombre de su bucket.
	`aws s3api create-bucket \`
	`--bucket amzn-s3-demo-destination-bucket \`
	`--region us-east-1`
	Asegúrese de que el nombre del bucket de S3 sea único a nivel mundial, ya que todas las cuentas de AWS comparten el espacio de nombres.
		Arquitecto de la nube, desarrollador de aplicaciones

Cree una política de ciclo de vida de 30 días para el bucket de S3.	1. Inicie sesión en la consola de administración de	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	AWS y abra la consola de Amazon S3. 2. Seleccione el bucket de S3 que tiene los datos de Firehose. 3. En el bucket de S3, seleccione la pestaña Administración y, luego,Agregar regla de ciclo de vida. 4. Escriba un nombre para la regla en el cuadro de diálogo Regla de ciclo de vida y configure una regla del ciclo de vida de 30 días para su bucket.	

Creación de un flujo de entrega de Firehose

Tarea	Descripción	Habilidades requeridas
Cree y configure un flujo de entrega de Firehose.	Descargue y edite el ejemplo de `CreateFireHoseToS3.py` código del repositorio. GitHub Este código está escrito en Python y muestra cómo crear un flujo de entrega de Firehose y un rol de AWS Identity and Access Management (IAM). El rol de IAM tiene una política que Firehose puede utilizar para	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	escribir en el bucket de S3 de destino. Para ejecutar el script, utilice los siguientes comandos y argumentos de línea de comando: Argumento 1 = <Your_S3_bucket_ARN> , que es el nombre de recurso de Amazon (ARN) del bucket que creó con anterioridad. Argumento 2= su nombre de Firehose (este piloto utiliza `firehose_to_s3_stream`). Argumento 3 = su nombre de rol de IAM (Este piloto utiliza `firehose_to_s3`). `python CreateFirehoseToS3.py <Your_S3_Bucket_ARN> firehose_to_s3_stream firehose_to_s3` Si el rol de IAM especificado no existe, el script creará un rol de asunción con una política de relaciones de confianza, así como una política que conceda suficientes permisos de Amazon S3. Para ver ejemplos de estas	

Tarea	Descripción	Habilidades requeridas
	políticas, consulte la sección Información adicional.	
Verifique el flujo de entrega de Firehose.	Describa el flujo de entrega de Firehose mediante la AWS CLI para verificar si el flujo de entrega se creó correctam ente. `aws firehose describe-delivery-stream --delivery-stream-name firehose_to_s3_stream`	Arquitecto de la nube, desarrollador de aplicaciones

Crear una función de Lambda para procesar el flujo de entrega de Firehose

Tarea	Descripción	Habilidades requeridas
Cree una política de confianza para la función de Lambda.	Cree un archivo de política de confianza con la siguiente información. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, ...`	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	<pre>"Action":
	"sts:AssumeRole"
	}
	]
	}</pre>
	Esto le concederá a su función permiso para acceder a los recursos de AWS.	

Cree un rol de ejecución para la función de Lambda.	Para crear el rol de ejecución, ejecute el siguiente código.
	<pre>aws iam create-role
	--role-name lambda-
	ex --assume-role-poli
	cy-document file://Tr
	ustPolicy.json</pre>
		Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Agregue permisos al rol.	Para agregar permisos al rol, use el comando `attach-policy-to-role` .
	
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/IAMFullAccess`
		Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Creación de una función de Lambda.	Ejecute el siguiente comando para comprimir el archivo `LambdaStreamProcessor.py` del repositorio de código.
	`zip function.zip LambdaStreamProcessor.py`
	Cuando cree la función de Lambda, necesitará el ARN del rol de ejecución de Lambda. Para obtener el ARN, ejecute el siguiente código.
	`aws iam get-role \ --role-name lambda-ex`
	Para crear la función de Lambda, ejecute el siguiente código.
	`# Review the environment variables and replace them with your values.`
	`aws lambda create-function --function-name LambdaStreamProcessor \ --zip-file fileb://function.zip --handler LambdaStreamProcessor.handler --runtime python3.8 \`
		Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`--role {Your Lamda Execution Role ARN}\ --environment Variables="{firehose_name=firehose_to_s3_stream,bucket_arn = <Your_S3_bucket_ARN>,iam_role_name = firehose_to_s3, batch_size=400}"`	
Configure el desencadenador de la función de Lambda.	Utilice la CLI de AWS para configurar el desencadenador (DynamoDB Streams), que invoca la función de Lambda. El tamaño del lote de 400 es para evitar problemas de simultaneidad de Lambda. `aws lambda create-event-source-mapping --function-name LambdaStreamProcessor \ --batch-size 400 --starting-position LATEST \ --event-source-arn <Your Latest Stream ARN From DynamoDB Console>`	Arquitecto de la nube, desarrollador de aplicaciones

Probar la funcionalidad

Tarea	Descripción	Habilidades requeridas
Añada elementos con marcas de tiempo vencidas a la tabla de Reserva.	Para probar la funcionalidad, añada a la tabla `Reservation` los elementos con marcas de tiempo epoch vencidos. El TTL eliminará automáticamente los elementos en función de la marca de tiempo. La función de Lambda se inicia con las actividades de DynamoDB Stream y filtra el evento para identificar la actividad `REMOVE` o los elementos eliminados. A continuación, permite colocar los registros en el flujo de entrega de Firehose en formato de lote. El flujo de entrega de Firehose transfiere los elementos a un bucket de S3 de destino con el prefijo `firehose3example/year=current year/month=current month/day=current day/hour=current hour/` . ⚠ Important Para optimizar la recuperación de	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	datos, configure Amazon S3 con `Prefix` y `ErrorOutputPrefix` que se detallan en la sección Información adicional.	

Limpiar los recursos

Tarea	Descripción	Habilidades requeridas
Elimine todos los recursos.	Elimine todos los recursos para asegurarse de que no se le cobre por ningún servicio que no utilice.	Arquitecto de la nube, desarrollador de aplicaciones

Recursos relacionados

- Administración del ciclo de vida del almacenamiento
- Clases de almacenamiento de Amazon S3
- Documentación de AWS SDK para Python (Boto3)

Información adicional

Creación y configuración de un flujo de entrega deFirehose: ejemplos de políticas

Documento de ejemplo de política de relaciones de confianza de Firehose

```
firehose_assume_role = {
        'Version': '2012-10-17',
        'Statement': [
            {
                'Sid': '',
                'Effect': 'Allow',
```

```
                'Principal': {
                    'Service': 'firehose.amazonaws.com'
                },
                'Action': 'sts:AssumeRole'
            }
        ]
    }
```

Ejemplos de políticas de permisos de S3

```
s3_access = {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "",
                "Effect": "Allow",
                "Action": [
                    "s3:AbortMultipartUpload",
                    "s3:GetBucketLocation",
                    "s3:GetObject",
                    "s3:ListBucket",
                    "s3:ListBucketMultipartUploads",
                    "s3:PutObject"
                ],
                "Resource": [
                    "{your s3_bucket ARN}/*",
                    "{Your s3 bucket ARN}"
                ]
            }
        ]
    }
```

Probar la funcionalidad: configuración de Amazon S3

Se elige la configuración de Amazon S3 con el siguiente `Prefix` y `ErrorOutputPrefix` para optimizar la recuperación de datos.

Prefijo

```
firehosetos3example/year=! {timestamp: yyyy}/month=! {timestamp:MM}/day=!
 {timestamp:dd}/hour=!{timestamp:HH}/
```

Firehose primero crea una carpeta base llamada `firehosetos3example` directamente debajo del bucket de S3. A continuación, evalúa las expresiones`!{timestamp:yyyy}`, `!{timestamp:MM}`!`{timestamp:dd}`, y `!{timestamp:HH}` para indicar el año, el mes, el día y la hora con el DateTimeFormatterformato Java.

Por ejemplo, una marca de tiempo de llegada aproximada de 1604683577 en tiempo de época de Unix se evalúa como `year=2020`, `month=11`, `day=06` y `hour=05`. Por lo tanto, se evalúa en `firehosetos3example/year=2020/month=11/day=06/hour=05/` la ubicación de Amazon S3 en la que se entregan los registros de datos.

ErrorOutputPrefix

```
firehosetos3erroroutputbase/!{firehose:random-string}/!{firehose:error-output-type}/!
{timestamp:yyyy/MM/dd}/
```

Los `ErrorOutputPrefix` generan una carpeta base llamada `firehosetos3erroroutputbase` directamente debajo del bucket de S3. La expresión `!{firehose:random-string}` se evalúa como una cadena aleatoria de 11 caracteres, como `ztWxkdg3Thg`. Se podría evaluar como `firehosetos3erroroutputbase/ztWxkdg3Thg/processing-failed/2020/11/06/` la ubicación de un objeto de Amazon S3 en la que se entregan los registros fallidos.

Cree una arquitectura sin servidor multiusuario en Amazon Service OpenSearch

Tabby Ward y Nisha Gambhir, Amazon Web Services

Resumen

Amazon OpenSearch Service es un servicio gestionado que facilita la implementación, el funcionamiento y el escalado de Elasticsearch, un popular motor de búsqueda y análisis de código abierto. OpenSearch El servicio ofrece una búsqueda de texto libre, así como una recopilación y un panel de control prácticamente en tiempo real para la transmisión de datos, como registros y métricas.

Los proveedores de software como servicio (SaaS) suelen utilizar el OpenSearch Servicio para abordar una amplia gama de casos de uso, como obtener información sobre los clientes de forma escalable y segura y, al mismo tiempo, reducir la complejidad y el tiempo de inactividad.

El uso del OpenSearch servicio en un entorno multiusuario introduce una serie de consideraciones que afectan a la partición, el aislamiento, la implementación y la administración de su solución SaaS. Los proveedores de SaaS deben considerar cómo escalar de manera efectiva sus clústeres de Elasticsearch con cargas de trabajo en constante cambio. También deben tener en cuenta cómo pueden afectar la estratificación y el ruido aledaño a su modelo de particionamiento.

Este patrón revisa los modelos empleados para representar y aislar los datos de los usuarios con constructos de Elasticsearch. Además, el patrón se centra en una arquitectura de referencia sencilla y sin servidor como ejemplo para demostrar la indexación y la búsqueda mediante OpenSearch Service en un entorno multiusuario. Implementa el modelo de particionamiento de datos de grupos, que comparte un mismo índice entre todos los usuarios y, al mismo tiempo, mantiene el aislamiento de los datos de los mismos. Este patrón utiliza los siguientes AWS servicios: Amazon API Gateway AWS Lambda, Amazon Simple Storage Service (Amazon S3) y Service. OpenSearch

Para obtener más información sobre el modelo de grupo y otros modelos de particionamiento de datos, consulte la sección de Información adicional.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS

- AWS Command Line Interface (AWS CLI) versión 2.x, instalada y configurada en macOS, Linux o Windows
- Python versión 3.9
- pip3: el código fuente de Python se proporciona como un archivo .zip para implementarlo en una función de Lambda. Si quiere usar el código localmente o personalizarlo, siga estos pasos para desarrollar y recompilar el código fuente:
  1. Genere el archivo `requirements.txt` ejecutando el siguiente comando en el mismo directorio que los scripts de Python: `pip3 freeze > requirements.txt`
  2. Instale las dependencias: `pip3 install -r requirements.txt`

Limitaciones

- Este código se ejecuta en Python y, actualmente, no es compatible con otros lenguajes de programación.
- La aplicación de ejemplo no incluye compatibilidad AWS entre regiones ni con la recuperación ante desastres (DR).
- Este patrón sólo pretende servir de ejemplo. No está pensado para ser utilizado en un entorno de producción.

Arquitectura

El siguiente diagrama ilustra la arquitectura de alto nivel de este patrón. La arquitectura incluye lo siguiente:

- Lambda para indexar y consultar el contenido
- OpenSearch Servicio para realizar búsquedas
- API Gateway para proporcionar a la API interacción con el usuario
- Amazon S3, para almacenar datos sin procesar (no indexados)
- Amazon CloudWatch supervisará los registros
- AWS Identity and Access Management (IAM) para crear las funciones y políticas de los inquilinos

Automatización y escala

Para simplificar, el patrón se utiliza AWS CLI para aprovisionar la infraestructura e implementar el código de muestra. Puede crear una CloudFormation plantilla o AWS Cloud Development Kit (AWS CDK) scripts para automatizar el patrón.

Tools (Herramientas)

Servicios de AWS

- AWS CLIes una herramienta unificada para administrar Servicios de AWS los recursos mediante el uso de comandos en el shell de la línea de comandos.
- Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- API Gateway es Servicio de AWS para crear, publicar, mantener, monitorear y proteger REST, HTTP y WebSocket APIs a cualquier escala.
- Amazon S3 es un servicio de almacenamiento de objetos que permite almacenar y recuperar cualquier cantidad de información en cualquier momento y desde cualquier lugar de la web.
- OpenSearch El servicio es un servicio totalmente gestionado que facilita la implementación, la protección y la ejecución de Elasticsearch a escala y de forma rentable.

Código

El archivo adjunto incluye archivos de muestra para este patrón. Entre ellos se incluyen:

- `index_lambda_package.zip`— La función Lambda para indexar datos en OpenSearch Service mediante el modelo de grupo.
- `search_lambda_package.zip`— La función Lambda para buscar datos en OpenSearch Service.
- `Tenant-1-data` — Muestra de datos sin procesar (no indexados) para Usuario-1.
- `Tenant-2-data`: muestra de datos sin procesar (no indexados) para Usuario-2.

> **Important**
>
> Las historias de este patrón incluyen ejemplos de AWS CLI comandos formateados para Unix, Linux y macOS. Para Windows, sustituya la barra diagonal invertida (\) utilizada como carácter de continuación de Unix al final de cada línea por el signo de intercalación (^).

> **Note**
>
> En AWS CLI los comandos, sustituya todos los valores entre los corchetes angulares (<>) por los valores correctos.

Epics

Creación y configuración de un bucket de S3

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Cree un bucket de S3 en su. Región de AWS Este bucket contendrá los datos de usuarios no indexados de la aplicación de muestra. Asegúrese de que el nombre del bucket de S3 sea único a nivel mundial, ya que todos comparten el espacio de nombres. Cuentas de AWS Para crear un bucket de S3, puedes usar el comando AWS CLI create-bucket de la siguiente manera: `aws s3api create-bucket \ --bucket <tenantrawdata> \ --region <your-AWS-Region>` donde `tenantrawdata` es el nombre de bucket de S3. (Puede usar cualquier nombre	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	único que siga las pautas de nomenclatura de buckets).	

Cree y configure un clúster de Elasticsearch

Tarea	Descripción	Habilidades requeridas

Cree un dominio de OpenSearch servicio.	Ejecute el AWS CLI create-elasticsearch-domain comando para crear un dominio OpenSearch de servicio:
	`aws es create-elasticsearch-domain \`
	`  --domain-name vpc-cli-example \`
	`  --elasticsearch-version 7.10 \`
	`  --elasticsearch-cluster-config InstanceType=t3.medium.elasticsearch,InstanceCount=1 \`
	`  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=10 \`
	`  --domain-endpoint-options "{\"EnforceHTTPS\": true}" \`
	`  --encryption-at-rest-options "{\"Enabled\": true}" \`
	`  --node-to-node-encryption-options "{\"Enabled\": true}" \`
	`  --advanced-security-options "{\"Enabl`
		Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	`ed\": true, \"Interna lUserDatabaseEnabled \": true, \ \"MasterUserOption s\": {\"MasterUserName \": \"KibanaUser\", \ \"MasterUserPasswo rd\": \"NewKiba naPassword@123\"}}" \ --vpc-options "{\"SubnetIds\": [\"<subnet-id>\"], \"SecurityGroupIds\": [\"<sg-id>\"]}" \ --access-policies "{\"Version\": \"2012-10-17\", \"Statement\": [{ \"Effect\": \"Allow\", \ \"Principal\": {\"AWS\": \"*\" }, \"Action\":\"es:*\", \ \"Resource\": \"arn:aws:es:<regi on>:<account-id>:d omain\/vpc-cli-exa mple\/*\" }] }"`  El número de instancias está establecido en 1, ya que el dominio se usa para realizar pruebas. Debe habilitar un control de acceso detallado mediante el parámetro `advanced-security-options` , ya que los detalles	

Tarea	Descripción	Habilidades requeridas
	no se pueden cambiar una vez creado el dominio. Este comando crea un nombre de usuario maestro (`KibanaUser`) y una contraseña que le permitirá iniciar sesión en la consola de Kibana. Como el dominio forma parte de una nube privada virtual (VPC), debe asegurarse de poder acceder a la instancia de Elasticsearch especific ando la política de acceso que va a usar. Para obtener más informaci ón, consulta Cómo lanzar tus dominios de Amazon OpenSearch Service dentro de una VPC en la AWS documentación.	

Tarea	Descripción	Habilidades requeridas
Instale un host bastión.	Configura una instancia Windows de Amazon Elastic Compute Cloud (Amazon EC2) como host bastión para acceder a la consola de Kibana. El grupo de seguridad de Elasticsearch debe permitir el tráfico del grupo de EC2 seguridad de Amazon. Para obtener instrucciones, consulte la entrada del blog Cómo controlar el acceso a la red a las EC2 instancias mediante un servidor Bastion. Cuando se haya configura do el host bastión y tenga disponible el grupo de seguridad asociado a la instancia, utilice el AWS CLI authorize-security-group-ingresscomando para añadir permiso al grupo de seguridad de Elasticsearch a fin de permitir el puerto 443 del grupo de seguridad de Amazon EC2 (host bastión). `aws ec2 authorize-security-group-ingress \ --group-id <SecurityGroupIdfElasticSearch> \ --protocol tcp \ --port 443 \`	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	`--source-group <SecurityGroupIdfBashionHostEC2>`	

Crear y configurar la función de índice de Lambda

Tarea	Descripción	Habilidades requeridas

Para crear el rol de ejecución de Lambda	Ejecute el comando AWS CLI create-role para conceder a la función de índice Lambda acceso a los recursos y a los recursos: Servicios de AWS
	`aws iam create-role \ --role-name index-lambda-role \ --assume-role-policy-document file://lambda_assume_role.json`
	donde `lambda_assume_role.json` es un documento JSON que concede permisos de `AssumeRole` a la función de Lambda, de la siguiente manera:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow",`
		Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas

	<pre>"Principa
	l": {
	
	"Service": "lambda.a
	mazonaws.com"
	},
	"Action":
	"sts:AssumeRole"
	}
	]
	}</pre>	

Tarea	Descripción	Habilidades requeridas

Adjunte políticas gestionadas al rol de Lambda.	Ejecute el AWS CLI attach-role-policycomando para adjuntar las políticas administradas al rol creado en el paso anterior. Estas dos políticas otorgan al rol permisos para crear una interfaz de red elástica y escribir CloudWatch registros en Logs.
	
	`aws iam attach-role-policy \`
	`  --role-name index-lambda-role \`
	`  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	
	`aws iam attach-role-policy \`
	`  --role-name index-lambda-role \`
	`  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`
		Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas

Cree una política para dar permisos a la función de índice de Lambda de modo que pueda leer los objetos de S3.	Ejecute el comando AWS CLI create-policy para dar `s3:GetObject` permiso a la función de índice de Lambda para leer los objetos del bucket de S3:
	`aws iam create-policy \ --policy-name s3-permission-policy \ --policy-document file://s3-policy.json`
	El archivo `s3-policy.json` es un documento JSON que se muestra a continuación y que concede permisos de `s3:GetObject` para permitir el acceso de lectura a los objetos de S3. Si ha usado un nombre diferente al crear el bucket de S3, proporcione el nombre de bucket correcto en sección de `Resource` :
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::<tenantrawdata>/*"`
		Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	<pre> }] }</pre>	

Adjunte la política de permisos de Amazon S3 al rol de ejecución de Lambda.	Ejecute el AWS CLI attach-role-policycomando para adjuntar la política de permisos de Amazon S3 que creó en el paso anterior a la función de ejecución de Lambda:
	<pre>aws iam attach-role-policy \
	  --role-name index-lambda-role \
	  --policy-arn <PolicyARN></pre>
	donde `PolicyARN` es el Nombre de recurso de Amazon (ARN) de la política de permisos de Amazon S3. Puede obtener este valor del resultado del comando anterior.
		Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas

Cree la función de indexar de Lambda.	Ejecute el comando AWS CLI create-function para crear la función de índice Lambda, que accederá al servicio: OpenSearch
	
	`aws lambda create-function \`
	`  --function-name index-lambda-function \`
	`  --zip-file fileb://index_lambda_package.zip \`
	`  --handler lambda_index.lambda_handler \`
	`  --runtime python3.9 \`
	`  --role "arn:aws:iam::account-id:role/index-lambda-role" \`
	`  --timeout 30 \`
	`  --vpc-config "{\"SubnetIds\": [\"<subnet-id1\>", \"<subnet-id2>\"], \`
	`  \"SecurityGroupIds\": [\"<sg-1>\"]}"`
		Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Permita que Amazon S3 llame a la función de índice de Lambda.	Ejecute el comando AWS CLI add-permission para conceder a Amazon S3 el permiso de llamar a la función de índice Lambda: `aws lambda add-permission \ --function-name index-lambda-function \ --statement-id s3-permissions \ --action lambda:InvokeFunction \ --principal s3.amazonaws.com \ --source-arn "arn:aws:s3:::<tenantrawdata>" \ --source-account "<account-id>"`	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Añada un desencadenante de Lambda para el evento de Amazon S3.	Ejecute el AWS CLI put-bucket-notification-configuration comando para enviar notificaciones a la función de índice Lambda cuando se detecte el `ObjectCreated` evento de Amazon S3. La función de índice se ejecuta cada vez que se carga un objeto en el bucket de S3. `aws s3api put-bucket-notification-configuration \ --bucket <tenantrawdata> \ --notification-configuration file://s3-trigger.json` El archivo `s3-trigger.json` es un documento JSON de la carpeta actual que añade la política de recursos a la función de Lambda cuando se produce el evento `ObjectCreated` de Amazon S3.	Arquitecto de la nube, administrador de la nube

Crear y configurar la función de búsqueda de Lambda

Tarea	Descripción	Habilidades requeridas
Para crear el rol de ejecución de Lambda	Ejecute el comando AWS CLI create-role para conceder	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas

	a la función de búsqueda de Lambda acceso a los recursos: Servicios de AWS
	`aws iam create-role \ --role-name search-lambda-role \ --assume-role-policy-document file://lambda_assume_role.json`
	donde `lambda_assume_role.json` es un documento JSON en la carpeta actual que concede permisos de `AssumeRole` a la función de Lambda, de la siguiente manera:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" } ] }`	

Tarea	Descripción	Habilidades requeridas

Adjunte políticas gestionadas al rol de Lambda.	Ejecute el AWS CLI attach-role-policycomando para adjuntar las políticas administradas al rol creado en el paso anterior. Estas dos políticas otorgan al rol permisos para crear una interfaz de red elástica y escribir CloudWatch registros en Logs.
	
	`aws iam attach-role-policy \`
	`  --role-name search-lambda-role \`
	`  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	
	`aws iam attach-role-policy \`
	`  --role-name search-lambda-role \`
	`  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`
		Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree la función de búsqueda de Lambda.	Ejecute el comando AWS CLI create-function para crear la función de búsqueda de Lambda, que accederá al servicio: OpenSearch `aws lambda create-function \ --function-name search-lambda-function \ --zip-file fileb://search_lambda_package.zip \ --handler lambda_search.lambda_handler \ --runtime python3.9 \ --role "arn:aws:iam::account-id:role/search-lambda-role" \ --timeout 30 \ --vpc-config "{\"SubnetIds\": [\"<subnet-id1\>", \"<subnet-id2>\"], \ \"SecurityGroupIds\": [\"<sg-1>\"]}"`	Arquitecto de la nube, administrador de la nube

Cree y configure los roles de usuario

Tarea	Descripción	Habilidades requeridas
Cree roles de IAM para los usuarios.	Ejecute el comando AWS CLI create-role para crear dos roles arrendatarios que se utilizarán para probar la funcionalidad de búsqueda:	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	`aws iam create-role \ --role-name Tenant-1-role \ --assume-role-policy-document file://assume-role-policy.json`	
	`aws iam create-role \ --role-name Tenant-2-role \ --assume-role-policy-document file://assume-role-policy.json`	
	El archivo `assume-role-policy.json` es un documento JSON en la carpeta actual que concede permisos de `AssumeRole` al rol de ejecución de Lambda: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "<Lambda execution role for index function>", "AWS": "<Lambda execution role for search function>" }, "Action": "sts:AssumeRole"`	

Tarea	Descripción	Habilidades requeridas

	`}`
	`]`
	`}`	

Tarea	Descripción	Habilidades requeridas

Crear una política de IAM de usuario.	Ejecuta el comando AWS CLI create-policy para crear una política de inquilinos que otorgue acceso a las operaciones de Elasticsearch:
	`aws iam create-policy \ --policy-name tenant-policy \ --policy-document file://policy.json`
	El archivo `policy.json` es un documento JSON en la carpeta actual que concede permisos en Elasticsearch:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "es:ESHttpDelete", "es:ESHttpGet", "es:ESHttpHead", "es:ESHttpPost", "es:ESHttpPut", "es:ESHttpPatch" ],`
		Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	<pre>"Resource": ["<ARN of Elasticsearch domain created earlier>"] }] }</pre>	

Adjunte la política de IAM del usuario a los roles del usuario.	Ejecute el AWS CLI attach-role-policycomando para adjuntar la política de IAM de inquilinos a las dos funciones de inquilino que creó en el paso anterior:
	<pre>aws iam attach-role-policy \ --policy-arn arn:aws:iam::account-id:policy/tenant-policy \ --role-name Tenant-1-role
	
	aws iam attach-role-policy \ --policy-arn arn:aws:iam::account-id:policy/tenant-policy \ --role-name Tenant-2-role</pre>
	La política ARN procede de lo obtenido en el paso anterior.
		Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas

Cree una política de IAM para conceder permisos de asunción de rol a Lambda.	Ejecute el comando AWS CLI create-policy para crear una política para que Lambda asuma el rol de inquilino:
	`aws iam create-policy \ --policy-name assume-tenant-role-policy \ --policy-document file://lambda_policy.json`
	El archivo `lambda_policy.json` es un documento JSON en la carpeta actual que concede permisos a `AssumeRole` :
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "<ARN of tenant role created earlier>" } ] }`
	En `Resource`, puede usar un carácter comodín para evitar
		Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	crear una nueva política para cada usuario.	

Cree una política de IAM para conceder permisos al rol de indexación de Lambda para acceder a Amazon S3.	Ejecute el comando AWS CLI create-policy para dar permiso al rol de índice de Lambda para acceder a los objetos del bucket de S3:
	`aws iam create-policy \ --policy-name s3-permission-policy \ --policy-document file://s3_lambda_policy.json`
	El archivo `s3_lambda_policy.json` es el siguiente documento de política de JSON de la carpeta actual:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::tenantrawdata/*" } ] }`
		Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas

Adjunte la política al rol de ejecución de Lambda.	Ejecute el AWS CLI attach-role-policycomando para adjuntar la política creada en el paso anterior al índice Lambda y a las funciones de ejecución de búsquedas que creó anteriormente:
	
	`aws iam attach-role-policy \`
	`  --policy-arn arn:aws:iam::account-id:policy/assume-tenant-role-policy \`
	`  --role-name index-lambda-role`
	
	`aws iam attach-role-policy \`
	`  --policy-arn arn:aws:iam::account-id:policy/assume-tenant-role-policy \`
	`  --role-name search-lambda-role`
	
	`aws iam attach-role-policy \`
	`  --policy-arn arn:aws:iam::account-id:policy/s3-permission-policy \`
	`  --role-name index-lambda-role`
	
	La política ARN procede de lo obtenido en el paso anterior.
		Arquitecto de la nube, administrador de la nube

Cree y configure una API de búsqueda

Tarea	Descripción	Habilidades requeridas
Cree una API de REST en API Gateway.	Ejecute el AWS CLI create-rest-api comando para crear un recurso de API REST: `aws apigateway create-rest-api \ --name Test-Api \ --endpoint-configuration "{ \"types\": [\"REGIONAL\"] }"` En el tipo de configuración de punto de conexión, puede especificar `EDGE` en lugar de `REGIONAL` para usar ubicaciones periféricas en lugar de una Región de AWS concreta. Anote el valor del campo `id` en el resultado del comando. Esta es la ID de API que usará en los siguientes comandos.	Arquitecto de la nube, administrador de la nube
Cree un recurso para la API de búsqueda.	El recurso de la API de búsqueda inicia la función de búsqueda de Lambda con el nombre de recurso `search`. (No es necesario crear una API para la función de índice de Lambda, ya que se ejecuta automáticamente cuando se cargan objetos en el bucket de S3).	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas

	1. Ejecute el comando AWS CLI get-resources para obtener el ID principal de la ruta raíz:
	
	`aws apigateway get-resources \ --rest-api-id <API-ID>`
	
	Observe el valor del campo ID. Usará esta ID principal en el siguiente comando.
	
	`{ "items": [ { "id": "zpsri964ck", "path": "/" } ] }`
	
	2. Ejecuta el comando AWS CLI create-resource para crear un recurso para la API de búsqueda. En `parent-id` , especifique la ID del comando anterior.
	
	`aws apigateway create-resource \ --rest-api-id <API-ID> \ --parent-id <Parent-ID> \`	

Tarea	Descripción	Habilidades requeridas
	`--path-part search`	
Cree un método GET para la API de búsqueda.	Ejecuta el comando AWS CLI put-method para crear un `GET` método para la API de búsqueda: `aws apigateway put-method \ --rest-api-id <API-ID> \ --resource-id <ID from the previous command output> \ --http-method GET \ --authorization-type "NONE" \ --no-api-key-required` Para `resource-id` , especifique la ID de lo obtenido del comando `create-resource` .	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree un método de respuesta para la API de búsqueda.	Ejecuta el AWS CLI put-method-responsecomando para añadir una respuesta de método para la API de búsqueda: `aws apigateway put-method-response \ --rest-api-id <API-ID> \ --resource-id <ID from the create-resource command output> \ --http-method GET \ --status-code 200 \ --response-models "{\"application/json\": \"Empty\"}"` En `resource-id` , especifique el ID del resultado del anterior comando `create-resource` .	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas

Configure una integración de Lambda proxy para la API de búsqueda.	Ejecute el comando AWS CLI put-integration para configurar una integración con la función de búsqueda de Lambda:
	
	`aws apigateway put-integration \`
	`  --rest-api-id <API-ID> \`
	`  --resource-id  <ID from the create-resource command output> \`
	`  --http-method GET \`
	`  --type AWS_PROXY \`
	`  --integration-http-method GET \`
	`  --uri arn:aws:apigateway:region:lambda:path/2015-03-31/functions/arn:aws:lambda:<region>:<account-id>:function:<function-name>/invocations`
	
	En `resource-id` , especifique la ID del anterior comando `create-resource` .
		Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas

Otorgue permiso a API Gateway para llamar a la función de búsqueda de Lambda.	Ejecute el comando AWS CLI add-permission para conceder permiso a API Gateway para usar la función de búsqueda:
	
	`aws lambda add-permission \`
	`  --function-name <function-name> \`
	`  --statement-id apigateway-get \`
	`  --action lambda:InvokeFunction \`
	`  --principal apigateway.amazonaws.com \`
	`  --source-arn "arn:aws:execute-api:<region>:<account-id>:api-id/*/GET/search`
	
	Cambie la ruta `source-arn` si ha usado un nombre de recurso de API en lugar de `search`.
		Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas

Implemente la API de búsqueda.	Ejecute el comando AWS CLI create-deployment para crear un recurso de etapa denominado: `dev`
	
	`aws apigateway create-deployment \`
	`  --rest-api-id <API-ID> \`
	`  --stage-name dev`
	
	Si actualizas la API, puedes usar el mismo AWS CLI comando para volver a implementarla en la misma etapa.
		Arquitecto de la nube, administrador de la nube

Crear y configurar roles de Kibana

Tarea	Descripción	Habilidades requeridas
Inicie sesión en la consola Kibana.	1. Busca el enlace a Kibana en el panel de control de tu dominio en la OpenSearch consola de servicio. La URL tiene el formato: `<domain-endpoint>/_plugin/kibana/` . 2. Use el host bastión que configuró en la primera épica para acceder a la consola de Kibana. 3. Inicia sesión en la consola de Kibana con el nombre	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	de usuario y la contraseña maestros del paso anterior, cuando creaste el dominio del OpenSearch servicio. 4. Cuando se le pida que seleccione un usuario, elija Privado.	

Tarea	Descripción	Habilidades requeridas
Cree y configure roles de Kibana.	Para aislar los datos y garantizar que un usuario no pueda recuperar los datos de otro, debe proteger los documentos con seguridad . Así, los usuarios podrán acceder únicamente a aquellos documentos que contienen su ID de usuario. 1. En la consola Kibana, en el panel de navegación, seleccione Seguridad, Rol. 2. Cree un nuevo rol de usuario. 3. Configura los permisos del clúster en`indices_all` , lo que otorga permisos de creación, lectura, actualización y eliminación (CRUD) en el índice de OpenSearch servicios. 4. Restrinja los permisos de indexación al índice `tenant-data` . (El nombre del índice debe coincidir con el nombre de las funciones de búsqueda e indexación de Lambda). 5. Defina los permisos de indexación en `indices_all` para que los usuarios puedan realizar todas las operaciones relacionadas	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	con la indexación. (Puede restringir las operaciones para brindar un acceso más detallado en función de sus necesidades). 6. Para garantizar la seguridad a nivel de documento, use la siguiente política para filtrar los documentos por ID de usuario, a fin de aislar los datos de los usuarios en un índice compartido: `{ "bool": { "must": { "match": { "TenantId": "Tenant-1" } } } }` El nombre del índice, las propiedades y los valores distinguen entre mayúsculas y minúsculas.	

Tarea	Descripción	Habilidades requeridas
Asigne usuarios a los roles.	1. Seleccione la pestaña Usuarios asignados para el rol y, a continuación, elija Asignar usuarios. 2. En la sección Roles de backend, especifique el ARN del rol de usuario de IAM que creó anteriorm ente y, a continuación, elija Asignar. Se asignará el rol de usuario de IAM al rol de Kibana para que la búsqueda específica del usuario arroje datos únicamente de ese usuario. Por ejemplo, si el nombre del rol de IAM del Usuario-1 es `Tenant-1-Role` , especifique el ARN de `Tenant-1-Role` (de la épica Crear y configura r roles de usuario) en la casilla Roles de backend para el rol Usuario-1 de Kibana. 3. Repita los pasos 1 y 2 para Usuario-2. Le recomendamos que automatice la creación de los roles de usuario y roles de Kibana en el momento de la incorporación del usuario.	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree el índice de datos de usuarios.	En el panel de navegación, en Administración, seleccione Herramientas de desarrollo y, a continuación, ejecute el siguiente comando. Este comando crea el índice `tenant-data` para definir la asignación de la propiedad `TenantId`. `PUT /tenant-data { "mappings": { "properties": { "TenantId": { "type": "keyword"} } } }`	Arquitecto de la nube, administrador de la nube

Cree puntos de enlace de VPC para Amazon S3 y AWS STS

Tarea	Descripción	Habilidades requeridas
Crear un punto de conexión de VPC para Amazon S3 .	Ejecute el AWS CLI create-vpc-endpointcomando para crear un punto de enlace de VPC para Amazon S3. El punto de conexión permite que la función de índice de Lambda de la VPC acceda a Amazon S3. `aws ec2 create-vpc-endpoint \`	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas

	<pre>--vpc-id <VPC-ID> \
	--service-name
	com.amazonaws.us-east-1.s3 \
	--route-table-ids
	<route-table-ID></pre>
	En `vpc-id`, especifique la VPC que está usando para la función de índice de Lambda. En `service-name`, use la URL correcta del punto de conexión Amazon S3. En `route-table-ids`, especifique la tabla de enrutamiento asociada al punto de conexión de VPC.	

Tarea	Descripción	Habilidades requeridas
Cree un punto final de VPC para. AWS STS	Ejecute el AWS CLI create-vpc-endpointcomando para crear un punto final de VPC para AWS Security Token Service ()AWS STS. El punto de conexión permite que las funciones de índice y búsqueda de Lambda en la VPC accedan al servicio AWS STS. Las funciones AWS STS se utilizan cuando asumen la función de IAM. `aws ec2 create-vpc-endpoint \ --vpc-id <VPC-ID> \ --vpc-endpoint-type Interface \ --service-name com.amazonaws.us-east-1.sts \ --subnet-id <subnet-ID> \ --security-group-id <security-group-ID>` Para `vpc-id`, especifique la VPC que va a utilizar para las funciones de índice y búsqueda de Lambda. En `subnet-id` , proporcione la subred en la que se debe crear este punto de conexión. En `security-group-id` , especifique el grupo de seguridad al que	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	desea asociar este punto de conexión. (Puede ser el mismo que el grupo de seguridad que usa Lambda).	

Pruebe el multiusuario y el aislamiento de datos

Tarea	Descripción	Habilidades requeridas
Actualice los archivos de Python para las funciones de índice y búsqueda.	1. En el `index_lambda_package.zip` archivo, edítelo para actualizar el `lamba_index.py` Cuenta de AWS ID y la información del punto Región de AWS final de Elasticsearch. 2. En el `search_lambda_package.zip` archivo, edítelo para actualizar el `lambda_search.py` Cuenta de AWS ID y la información del punto final Región de AWS de Elasticsearch. Puedes obtener el punto final de Elasticsearch desde la pestaña Descripción general de la consola de servicio. OpenSearch Tiene el formato `<AWS-Region>.es.amazonaws.com` .	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Actualizar el código de Lambda.	Use el AWS CLI update-function-codecomando para actualizar el código Lambda con los cambios que realizó en los archivos de Python:
	
	`aws lambda update-function-code \`
	`  --function-name index-lambda-function \`
	`  --zip-file fileb://index_lambda_package.zip`
	
	`aws lambda update-function-code \`
	`  --function-name search-lambda-function \`
	`  --zip-file fileb://search_lambda_package.zip`
		Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Cargue los datos sin procesar en el bucket de S3.	Use el comando AWS CLI cp para cargar los datos de los objetos Tenant-1 y Tenant-2 al `tenantrawdata` bucket (especifique el nombre del bucket S3 que creó para este propósito):
	`aws s3 cp tenant-1-data s3://tenantrawdata`
	`aws s3 cp tenant-2-data s3://tenantrawdata`
	El bucket de S3 está configura do para ejecutar la función de índice de Lambda siempre que se carguen datos, de modo que el documento se indexe en Elasticsearch.
		Arquitecto de la nube, administrador de la nube

Busque datos desde la consola de Kibana.	En la consola de Kibana, ejecute la siguiente consulta: `GET tenant-data/_search` Esta consulta muestra todos los documentos indexados en Elasticsearch. En este caso, debería ver dos documentos separados para Inquilino-1 e Inquilino-2.	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas

Pruebe la API de búsqueda desde API Gateway.	1. En la consola de API Gateway, abra la API de búsqueda, elija el método `GET` en recurso de búsqueda y seleccione Probar.
	2. En la ventana de prueba, introduzca la siguiente cadena de consulta (distingue entre mayúsculas y minúsculas) para la ID de usuario y, a continuación, seleccione Probar.
	`TenantId=Tenant-1`
	La función Lambda envía una consulta a OpenSearch Service que filtra el documento arrendatario en función de la seguridad a nivel de documento. El método devuelve el documento que pertenece a Usuario-1.
	3. Cambie la cadena de consulta a:
	`TenantId=Tenant-2`
	Esta consulta nos devuelve el documento que pertenece al Usuario-2.
		Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	Para ver una ilustración de la pantalla, consulte la sección de Información adicional.	
Eliminación de recursos.	Limpie todos los recursos que haya creado para evitar cargos adicionales en su cuenta.	AWS DevOps, arquitecto de nube, administrador de nube

Recursos relacionados

- AWS SDK para Python (Boto)
- AWS Lambda documentación
- Documentación de API Gateway
- Documentación de Amazon S3
- Documentación OpenSearch de Amazon Service
  - Control de acceso detallado en Amazon Service OpenSearch
  - Creación de una aplicación de búsqueda con Amazon OpenSearch Service
  - Lanzamiento de tus dominios OpenSearch de Amazon Service dentro de una VPC

Información adicional

Modelos de particionamiento de datos

Hay tres modelos comunes de particionamiento de datos que se emplean en los sistemas multiusuario: silos, agrupados e híbridos. El modelo que elija dependerá de las necesidades de cumplimiento, ruido, operaciones y aislamiento de su entorno.

Modelo de silo

En el modelo de silo, los datos de cada usuario se almacenan en un área de almacenamiento distinta, por lo que los datos de los usuarios no se mezclan. Puede utilizar dos enfoques para implementar el modelo de silo con OpenSearch Service: dominio por inquilino e índice por inquilino.

- Dominio por inquilino: puedes usar un dominio de OpenSearch servicio independiente (sinónimo de un clúster de Elasticsearch) por inquilino. Tener a cada usuario en su propio dominio proporciona todos los beneficios de tener los datos en un constructo independiente. Sin embargo, este enfoque presenta desafíos de gestión y agilidad. Su naturaleza distribuida dificulta la agregación y la evaluación del estado operativo y la actividad de los usuarios. Se trata de una opción costosa que requiere que cada dominio de OpenSearch servicio tenga como mínimo tres nodos principales y dos nodos de datos para las cargas de trabajo de producción.

- Índice por inquilino: puede colocar los datos del inquilino en índices separados dentro de un clúster de OpenSearch servicios. Con este enfoque, se usa un identificador de inquilino al crear y asignar un nombre al índice, anteponiendo el identificador de inquilino al nombre del índice. El enfoque de índice por usuario le ayuda a alcanzar sus objetivos de compartimentación sin tener que introducir un clúster completamente separado para cada usuario. Sin embargo, si aumenta el número de índices, es posible que la memoria se agote, ya que este enfoque requiere más particiones y el nodo maestro tiene que gestionar una mayor asignación y reequilibrio.

Modelo de aislamiento en silo: en el modelo de silo, se emplean políticas de IAM para aislar los dominios o índices que contienen los datos de cada usuario. Estas políticas impiden que un usuario acceda a los datos de otro. Para implementar su modelo de aislamiento en silos, puede crear una política basada en recursos que controle el acceso al recurso de su usuario. Suele ser una política de acceso al dominio que especifica qué acciones puede realizar un principal en los subrecursos del dominio, incluidos los índices de Elasticsearch y. APIs Con las políticas de IAM basadas en la identidad, puede especificar las acciones permitidas o denegadas en el dominio, los índices o dentro del Servicio. APIs OpenSearch El elemento `Action` de una política de IAM describe la acción o acciones específicas permitidas y denegadas por la política. El elemento `Principal` especifica las cuentas, usuarios o roles afectados.

El siguiente ejemplo de política otorga a Usuario-1 acceso total (según lo especificado en `es:*`) únicamente a los subrecursos del dominio `tenant-1`. El `/*` de seguimiento en el elemento `Resource` indica que esta política se aplica a los sub-recursos del dominio, no al dominio en sí. Cuando esta política esté en vigor, los usuarios no podrán crear un dominio nuevo ni modificar la configuración de un dominio existente.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::<aws-account-id>:user/Tenant-1"
         },
         "Action": "es:*",
         "Resource": "arn:aws:es:<Region>:<account-id>:domain/tenant-1/*"
      }
   ]
}
```

Para implementar el modelo de silo de índice por inquilino, tendrá que modificar este ejemplo de política para restringir aún más a Inquilino-1 al índice o índices especificados, indicando el nombre del índice. El siguiente ejemplo de política restringe a Usuario-1 al índice `tenant-index-1`.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/Tenant-1"
         },
         "Action": "es:*",
         "Resource": "arn:aws:es:<Region>:<account-id>:domain/test-domain/tenant-
index-1/*"
      }
   ]
}
```

Modelo de grupo

En el modelo de grupo, todos los datos de los usuarios se almacenan en un índice dentro del mismo dominio. El identificador del usuario se incluye en los datos (documento) y se usa como clave de partición, de modo que puede determinar qué datos pertenecen a cada usuario. Este modelo reduce la sobrecarga de administración. Operar y administrar un índice agrupado es más fácil y eficiente que administrar varios índices. Sin embargo, dado que los datos de los usuarios están mezclados en el

mismo índice, se pierde el aislamiento natural de los usuarios que proporciona el modelo de silos. Este enfoque también podría reducir el rendimiento debido al efecto de ruido aledaño.

Aislamiento de usuarios en el modelo de grupo: en general, el aislamiento de usuarios es difícil de implementar en el modelo de grupo. El mecanismo de IAM usado con el modelo de silo no permite describir el aislamiento en función del identificador de usuario almacenado en el documento.

Un enfoque alternativo consiste en usar el control de acceso detallado (FGAC) que proporciona Open Distro para Elasticsearch. El FGAC permite controlar los permisos a nivel de índice, documento o campo. En cada solicitud, el FGAC evalúa las credenciales del usuario y autentica o deniega el acceso. Si el FGAC autentica al usuario, obtiene todos los roles mapeados a ese usuario y utiliza el conjunto completo de permisos para determinar cómo gestionar la solicitud.

Para lograr el aislamiento requerido en el modelo agrupado, puede usar seguridad a nivel de documento, que le permite restringir un rol a un subconjunto de documentos de un índice. El siguiente ejemplo de rol restringe las consultas a Usuario-1. Al aplicar este rol a Usuario-1, puede lograr el aislamiento necesario.

```
{
   "bool": {
     "must": {
       "match": {
         "tenantId": "Tenant-1"
       }
     }
   }
 }
```

Modelo híbrido

El modelo híbrido emplea una combinación de los modelos de silo y grupo en el mismo entorno para ofrecer experiencias únicas a cada nivel de usuario (como los niveles gratuito, estándar y prémium). Cada nivel sigue el mismo perfil de seguridad que se usó en el modelo de grupo.

Aislamiento de usuarios en el modelo híbrido: en el modelo híbrido, se sigue el mismo perfil de seguridad que en el modelo de grupo. El uso del modelo de seguridad FGAC a nivel de documento proporciona aislamiento a los usuarios. Si bien esta estrategia simplifica la administración de

clústeres y ofrece agilidad, complica otros aspectos de la arquitectura. Por ejemplo, el código requiere una complejidad adicional para determinar qué modelo está asociado a cada usuario. También deberá asegurarse de que las consultas de un solo usuario no saturen todo el dominio ni degraden la experiencia de otros usuarios.

Pruebas en API Gateway

Ventana de prueba para consulta de Usuario-1

Ventana de prueba para consulta de Usuario-2

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Implemente aplicaciones de varias pilas mediante AWS CDK con TypeScript

Dr. Rahul Sharad Gaikwad, Amazon Web Services

Resumen

Este patrón proporciona un step-by-step enfoque para la implementación de aplicaciones en Amazon Web Services (AWS) mediante el AWS Cloud Development Kit (AWS CDK) con TypeScript. Por ejemplo, el patrón implementa una aplicación de análisis en tiempo real sin servidor.

El patrón crea e implementa aplicaciones de pila anidada. La CloudFormation pila de AWS principal llama a las pilas secundarias o anidadas. Cada pila secundaria crea e implementa los recursos de AWS que se definen en la CloudFormation pila. AWS CDK Toolkit, el comando de la interfaz de línea de comandos (CLI)`cdk`, es la interfaz principal de las CloudFormation pilas.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una nube privada virtual (VPC) y subredes existentes
- Kit de herramientas de AWS CDK instalado y configurado
- Un usuario con permisos de administrador y un conjunto de claves de acceso.
- Node.js
- Interfaz de la línea de comandos de AWS (AWS CLI)

Limitaciones

- Como la CDK de AWS utiliza AWS CloudFormation, las aplicaciones de la CDK de AWS están sujetas a cuotas de CloudFormation servicio. Para obtener más información, consulte CloudFormation Cuotas de AWS.

Versiones de producto

Este patrón se ha creado y probado usando las siguientes herramientas y versiones.

- Kit de herramientas de AWS CDK 1.83.0

- Node.js 14.13.0
- npm 7.0.14

El patrón debería funcionar con cualquier versión de AWS CDK o npm. Tenga en cuenta que las versiones 13.0.0 a 13.6.0 de Node.js no son compatibles con AWS CDK.

Arquitectura

Pila de tecnología de destino

- Consola de AWS Amplify
- Amazon API Gateway
- AWS CDK
- Amazon CloudFront
- Amazon Cognito
- Amazon DynamoDB
- Amazon Data Firehose
- Amazon Kinesis Data Streams
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)

Arquitectura de destino

En el siguiente diagrama se muestra la implementación de aplicaciones de varias pilas mediante AWS CDK con. TypeScript

En el siguiente diagrama se muestra la arquitectura de la aplicación en tiempo real sin servidor de ejemplo.

Tools (Herramientas)

Herramientas

- La Consola de AWS Amplify es el centro de control para las implementaciones de aplicaciones web y móviles de pila completa en AWS. El alojamiento de la consola de Amplify proporciona un flujo de trabajo basado en Git para alojar aplicaciones web sin servidor de pila completa con implementación continua. La interfaz de usuario de administración es una interfaz visual para que los desarrolladores de frontend web y móvil puedan crear y administrar el backend de aplicaciones fuera de la Consola de AWS.
- Amazon API Gateway es un servicio de AWS para crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket APIs a cualquier escala.
- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- El Kit de herramientas de AWS CDK es un kit de desarrollo en la nube de línea de comandos que le ayuda a interactuar con su aplicación AWS CDK. El comando `cdk` de la CLI es la herramienta principal para interactuar con su aplicación AWS CDK. Ejecuta su aplicación, interroga el modelo de aplicación que ha definido y produce e implementa las CloudFormation plantillas de AWS generadas por la CDK de AWS.
- Amazon CloudFront es un servicio web que acelera la distribución de contenido web estático y dinámico, como .html, .css, .js y archivos de imagen. CloudFront entrega su contenido a través de una red mundial de centros de datos denominados ubicaciones perimetrales para reducir la latencia y mejorar el rendimiento.
- Amazon Cognito ofrece autenticación, autorización y administración de usuarios para sus aplicaciones móviles y web. Sus usuarios pueden iniciar sesión directamente o a través de un tercero.
- Amazon DynamoDB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido y predecible, así como una perfecta escalabilidad.
- Amazon Data Firehose es un servicio totalmente gestionado para entregar datos de streaming en tiempo real a destinos como Amazon S3, Amazon Redshift, OpenSearch Amazon Service, Splunk y cualquier punto de enlace HTTP personalizado o punto de enlace HTTP propiedad de proveedores de servicios externos compatibles.
- Amazon Kinesis Data Streams es un servicio que permite recopilar y procesar grandes flujos de registros de datos en tiempo real.
- AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Código

Se adjunta el código de este patrón.

Epics

Instalación del kit de herramientas de AWS CDK

Tarea	Descripción	Habilidades requeridas
Instale el kit de herramientas de AWS CDK.	Para instalar el kit de herramientas de AWS CDK a nivel global, ejecute el siguiente comando. `npm install -g aws-cdk`	DevOps
Verificar la versión.	Para verificar la versión del kit de herramientas de AWS CDK, ejecute el siguiente comando. `cdk --version`	DevOps

Configuración de las credenciales de AWS

Tarea	Descripción	Habilidades requeridas
Configurar las credenciales.	Para configurar las credencia les, ejecute el comando `aws configure` y siga las instrucciones. `$aws configure`	DevOps

Tarea	Descripción	Habilidades requeridas

	`AWS Access Key ID [None]:`
	`AWS Secret Access Key [None]: your_secret_access_key`
	`Default region name [None]:`
	`Default output format [None]:`	

Descarga del código del proyecto

Tarea	Descripción	Habilidades requeridas
Descargar el código del proyecto adjunto.	Para obtener más información sobre la estructura de los directorios y archivos, consulte la sección Información adicional.	DevOps

Inicie el entorno de AWS CDK

Tarea	Descripción	Habilidades requeridas
Inicie el entorno.	Para implementar la CloudFormation plantilla de AWS en la cuenta y la región de AWS que desee usar, ejecute el siguiente comando. `cdk bootstrap <account>/<Region>`	DevOps

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte la documentación de AWS.	

Crear e implementar el proyecto

Tarea	Descripción	Habilidades requeridas
Compilar el proyecto.	Para compilar el código del proyecto, ejecute el comando `npm run build`.	DevOps
Implementar el proyecto.	Para implementar el código del proyecto, ejecute el comando `cdk deploy`.	

Verificación de resultados

Tarea	Descripción	Habilidades requeridas
Verificar la creación de la pila.	En la consola de administración de AWS, elija CloudFormation. En las pilas del proyecto, verifique que se hayan creado una pila principal y dos pilas secundarias.	DevOps

Pruebe la aplicación

Tarea	Descripción	Habilidades requeridas
Enviar datos a Kinesis Data Streams.	Configure su cuenta de AWS para enviar datos a Kinesis Data Streams mediante Amazon Kinesis Data Generator (KDG). Para obtener más información, consulte Amazon Kinesis Data Generator.	DevOps
Crear un usuario de Amazon Cognito.	Para crear un usuario de Amazon Cognito, descargue la plantilla cognito-setup.json de la sección Crear un usuario de Amazon Cognito de CloudFormation la página de ayuda del generador de datos de Kinesis. Inicie la plantilla y, a continuación, introduzc a su nombre de usuario y contraseña de Amazon Cognito. La pestaña Salidas muestra la URL de Kinesis Data Generator.	DevOps
Inicio de sesión en Kinesis Data Generator	Para iniciar sesión en KDG, utilice las credenciales de Amazon Cognito que ha introducido y la URL de Kinesis Data Generator.	DevOps
Probar la aplicación.	En KDG, en Plantilla de registro, Plantilla 1, pegue	DevOps

Tarea	Descripción	Habilidades requeridas
	el código de prueba de la sección Información adicional y seleccione Enviar datos.	
Probar API Gateway.	Una vez incorporados los datos, pruebe API Gateway mediante el método `GET` para recuperar los datos.	DevOps

Recursos relacionados

Referencias

- AWS Cloud Development Kit
- AWS CDK en GitHub
- Uso de pilas anidadas
- Ejemplo de muestra de AWS: análisis en tiempo real sin servidor

Información adicional

Detalles del directorio y el archivo

Este patrón configura las tres siguientes pilas.

- `parent-cdk-stack.ts`: esta pila actúa como pila principal y llama a las dos aplicaciones secundarias como pilas anidadas.
- `real-time-analytics-poc-stack.ts`: esta pila anidada contiene la infraestructura y el código de la aplicación.
- `real-time-analytics-web-stack.ts`: esta pila anidada contiene únicamente el código estático de la aplicación web.

Archivos importantes y su funcionalidad

- `bin/real-time-analytics-poc.ts`: punto de entrada de la aplicación AWS CDK. Carga todas las pilas definidas en `lib/`.

- `lib/real-time-analytics-poc-stack.ts`: definición de la pila de la aplicación AWS CDK (`real-time-analytics-poc`).
- `lib/real-time-analytics-web-stack.ts`: definición de la pila de la aplicación AWS CDK (`real-time-analytics-web-stack`).
- `lib/parent-cdk-stack.ts`: definición de la pila de la aplicación AWS CDK (`parent-cdk`).
- `package.json`: manifiesto del módulo npm, que incluye el nombre, la versión y las dependencias de la aplicación.
- `package-lock.json`: mantenimiento por parte de npm.
- `cdk.json`: kit de herramientas para ejecutar la aplicación.
- `tsconfig.json`— La TypeScript configuración del proyecto.
- `.gitignore`: lista de archivos que Git debe excluir del control de código de origen.
- `node_modules`: mantenimiento por parte de npm; incluye las dependencias del proyecto.

La siguiente sección de código de la pila principal llama a las aplicaciones secundarias como pilas anidadas de AWS CDK.

```
import * as cdk from '@aws-cdk/core';
import { Construct, Stack, StackProps } from '@aws-cdk/core';
import { RealTimeAnalyticsPocStack } from './real-time-analytics-poc-stack';
import { RealTimeAnalyticsWebStack } from './real-time-analytics-web-stack';


export class CdkParentStack extends Stack {
  constructor(scope: Construct, id: string, props?: StackProps) {
    super(scope, id, props);


    new RealTimeAnalyticsPocStack(this, 'RealTimeAnalyticsPocStack');
    new RealTimeAnalyticsWebStack(this, 'RealTimeAnalyticsWebStack');
  }
}
```

Código para realizar pruebas

```
session={{date.now('YYYYMMDD')}}|sequence={{date.now('x')}}|
reception={{date.now('x')}}|instrument={{random.number(9)}}|
l={{random.number(20)}}|price_0={{random.number({"min":10000,
 "max":30000})}}|price_1={{random.number({"min":10000, "max":30000})}}|
```

```
price_2={{random.number({"min":10000, "max":30000})}}|
price_3={{random.number({"min":10000, "max":30000})}}|
price_4={{random.number({"min":10000, "max":30000})}}|
price_5={{random.number({"min":10000, "max":30000})}}|
price_6={{random.number({"min":10000, "max":30000})}}|
price_7={{random.number({"min":10000, "max":30000})}}|
price_8={{random.number({"min":10000, "max":30000})}}|
```

Pruebas de API Gateway

En la consola de API Gateway, pruebe API Gateway mediante el método `GET`.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Automatice la implementación de aplicaciones anidadas mediante SAM de AWS

Dr. Rahul Sharad Gaikwad, Ishwar Chauthaiwale, Dmitry Gulin y Tabby Ward, Amazon Web Services

Resumen

En Amazon Web Services (AWS), el AWS Serverless Application Model (AWS SAM) es un marco de código abierto que proporciona una sintaxis abreviada para expresar funciones APIs, bases de datos y mapeos de fuentes de eventos. Con solo unas pocas líneas para cada recurso, puede definir la aplicación que desee y modelarla mediante YAML. Durante la implementación, SAM transforma y expande la sintaxis de SAM en una CloudFormation sintaxis de AWS que puede usar para crear aplicaciones sin servidor con mayor rapidez.

SAM de AWS simplifica el desarrollo, la implementación y la administración de aplicaciones sin servidor en la plataforma AWS. Proporciona un marco estandarizado, una implementación más rápida, capacidades de pruebas locales, administración de recursos, una integración perfecta con las herramientas de desarrollo y una comunidad de apoyo. Estas características lo convierten en una herramienta valiosa para crear aplicaciones sin servidor de manera eficiente y eficaz.

Este patrón utiliza plantillas SAM de AWS para automatizar la implementación de aplicaciones anidadas. Una aplicación anidada es una aplicación dentro de otra aplicación. Las aplicaciones principales llaman a las aplicaciones secundarias. Se trata de componentes con acoplamiento flexible de una arquitectura sin servidor.

Con aplicaciones anidadas, puede crear rápidamente arquitecturas sin servidor altamente sofisticadas mediante la reutilización de servicios o componentes que se crean y mantienen de forma independiente, pero que se componen con SAM de AWS y Repositorio de aplicaciones sin servidor. Las aplicaciones anidadas le ayudan a crear aplicaciones más potentes, evitar la duplicación del trabajo y garantizar la coherencia y las prácticas recomendadas en todos sus equipos y organizaciones. Para mostrar las aplicaciones anidadas, el patrón implementa un ejemplo de aplicación de carrito de compras sin servidor de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una nube privada virtual (VPC) y subredes existentes

- Un entorno de desarrollo integrado como Visual Studio Code (para obtener más información, consulte Herramientas para crear en AWS)
- Biblioteca de ruedas de Python instalada con pip install wheel, si aún no está instalada

Limitaciones

- El número máximo de aplicaciones que se pueden anidar en una aplicación sin servidor es de 200.
- El número máximo de parámetros que puede tener una aplicación anidada es 60.

Versiones de producto

- Esta solución se basa en la versión 1.21.1 de la interfaz de la línea de comandos de SAM de AWS (CLI de SAM de AWS), pero esta arquitectura debería funcionar con versiones posteriores de la CLI de SAM de AWS.

Arquitectura

Pila de tecnología de destino

- Amazon API Gateway
- SAM de AWS
- Amazon Cognito
- Amazon DynamoDB
- AWS Lambda
- Cola de Amazon Simple Queue Service (Amazon SQS)

Arquitectura de destino

El siguiente diagrama muestra cómo se realizan las solicitudes de los usuarios a los servicios de compras llamando por teléfono APIs. La solicitud del usuario, incluida toda la información necesaria, se envía a Amazon API Gateway y al autorizador de Amazon Cognito, que ejecuta los mecanismos de autenticación y autorización para el. APIs

Cuando se agrega, elimina o actualiza un elemento en DynamoDB, se coloca un evento en DynamoDB Streams, que a su vez inicia una función de Lambda. Para evitar la eliminación inmediata

de elementos antiguos como parte de un flujo de trabajo sincrónico, los mensajes se colocan en una cola de SQS, lo que inicia una función de trabajo para eliminarlos.

En esta configuración de solución, la CLI de AWS SAM sirve de interfaz para las CloudFormation pilas de AWS. Las plantillas SAM de AWS implementan automáticamente aplicaciones anidadas. La plantilla SAM principal llama a las plantillas secundarias y la CloudFormation pila principal implementa las pilas secundarias. Cada pila secundaria crea los recursos de AWS que se definen en las CloudFormation plantillas de AWS SAM.

1. Genere e implemente las pilas.
2. La CloudFormation pila de autenticación contiene Amazon Cognito.
3. La CloudFormation pila de productos contiene una función Lambda y Amazon API Gateway
4. La CloudFormation pila de compras contiene una función Lambda, Amazon API Gateway, la cola SQS y la base de datos Amazon DynamoDB.

Tools (Herramientas)

Herramientas

- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket APIs a cualquier escala.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- Amazon Cognito ofrece autenticación, autorización y administración de usuarios para aplicaciones móviles y web.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Serverless Application Model (AWS SAM) es un marco de código abierto que permite crear aplicaciones sin servidor en la nube de AWS.

- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.

Código

El código de este patrón está disponible en el repositorio de muestras de GitHub AWS SAM Nested Stack.

Epics

Instalar la CLI de SAM de AWS

Tarea	Descripción	Habilidades requeridas
Instalar la CLI de SAM de AWS.	Para instalar la CLI de SAM de AWS, siga las instrucciones de la documentación de SAM de AWS.	DevOps ingeniero

Configure las credenciales de AWS.	Para configurar las credenciales de AWS para que la CLI de SAM de AWS pueda realizar llamadas a los servicios de AWS en su nombre, ejecute el comando `aws configure` y siga las instrucciones.
	`$aws configure`
	`AWS Access Key ID [None]: <your_access_key_id>`
	`AWS Secret Access Key [None]: your_secret_access_key`
	`Default region name [None]:`
	`Default output format [None]:`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Para obtener más información sobre cómo configurar sus credenciales, consulte credenciales de autenticación y acceso.	

Inicie el proyecto SAM de AWS

Tarea	Descripción	Habilidades requeridas

Clone el repositorio de código de SAM de AWS.	1. Introduzca el siguiente comando para clonar el repositorio de pilas de muestras anidadas de AWS para este patrón.
	`git clone https://github.com/aws-samples/aws-sam-nested-stack-sample.git`
	2. Acceda al directorio clonado ejecutando el siguiente comando.
	`cd aws-sam-nested-stack-sample`
		DevOps ingeniero

Implemente plantillas para iniciar el proyecto.	Ejecute el comando `SAM init` para iniciar el proyecto. Cuando se le pida que elija una fuente de plantilla, elija `Custom Template Location`.	DevOps ingeniero

Compile y cree el código de la plantilla SAM

Tarea	Descripción	Habilidades requeridas
Revise las plantillas de aplicaciones SAM de AWS.	Revise las plantillas de las aplicaciones anidadas. En este ejemplo se utilizan las siguientes plantillas de aplicaciones anidadas: • `auth.yaml` : esta plantilla configura los recursos relacionados con la autenticación, como Amazon Cognito y Almacén de parámetros de AWS Systems Manager. • `product-mock.yaml` : esta plantilla implement a recursos relacionados con el producto, como las funciones de Lambda y Amazon API Gateway. • `shoppingcart-servi ce.yaml` : esta plantilla configura los recursos relacionados con los carritos de compras, como AWS Identity and Access Management (IAM), tablas de DynamoDB y funciones de Lambda.	DevOps ingeniero
Revise la plantilla principal.	Revise la plantilla que invocará las plantillas de aplicación anidadas. En este ejemplo, la plantilla principal	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	es `template.yml` . Todas las aplicaciones independientes están anidadas en la plantilla principal única `template.yml` .	
Compile y cree el código de la plantilla SAM de AWS.	Ejecute el siguiente comando utilizando la CLI de SAM de AWS. `sam build`	DevOps ingeniero

Implemente la plantilla SAM de AWS

Tarea	Descripción	Habilidades requeridas
Implemente las aplicaciones.	Para lanzar el código de plantilla SAM que crea las CloudFormation pilas de aplicaciones anidadas y despliega el código en el entorno de AWS, ejecute el siguiente comando. `sam deploy --guided --stack-name shopping-cart-nested-stack --capabilities CAPABILITY_IAM CAPABILITY_AUTO_EXPAND` El comando aparecerá con algunas preguntas. Responda a todas las preguntas con y.	DevOps ingeniero

Verifique la implementación

Tarea	Descripción	Habilidades requeridas
Verifique las pilas.	Para revisar las CloudFormation pilas de AWS y los recursos de AWS que se definieron en las plantillas de AWS SAM, haga lo siguiente: 1. Inicie sesión en la consola de administración de AWS y navegue hasta la CloudFormationconsola. 2. Compruebe que las pilas principal y secundaria estén en la lista. En este ejemplo, `sam-shopping-cart` es la pila principal que llama a las pilas anidadas de Auth, Product y Shopping. La pila de productos proporciona el enlace URL de Product API Gateway como salida.	DevOps ingeniero

Recursos relacionados

Referencias

- AWS Serverless Application Model (AWS SAM)
- AWS SAM en GitHub
- Microservicio de carrito de compras sin servidor (ejemplo de aplicación de AWS)

Tutoriales y videos

- Cree una aplicación sin servidor
- Charlas técnicas online de AWS: creación e implementación de aplicaciones sin servidor con SAM de AWS

Información adicional

Una vez colocado todo el código, el ejemplo tiene la siguiente estructura de directorios:

- sam_stacks: esta carpeta contiene la capa `shared.py`. Una capa es un archivo que contiene bibliotecas, un tiempo de ejecución personalizado u otras dependencias. Con las capas, puede utilizar las bibliotecas en la función sin necesidad de incluirlas en el paquete de implementación.
- product-mock-service— Esta carpeta contiene todos los archivos y funciones de Lambda relacionados con el producto.
- shopping-cart-service— Esta carpeta contiene todas las funciones y archivos de Lambda relacionados con las compras.

Implemente el aislamiento de inquilinos de SaaS para Amazon S3 mediante una máquina expendedora de AWS Lambda fichas

Tabby Ward, Thomas Davis y Sravan Periyathambi, Amazon Web Services

Resumen

Las aplicaciones SaaS multiusuario deben implementar sistemas para garantizar que se mantenga el aislamiento de los usuarios. Cuando almacenas datos de inquilinos en el mismo AWS recurso (por ejemplo, cuando varios inquilinos almacenan datos en el mismo depósito de Amazon Simple Storage Service (Amazon S3), debes asegurarte de que no se pueda producir el acceso entre inquilinos. Las máquinas expendedoras de fichas (TVMs) son una forma de aislar los datos de los inquilinos. Estas máquinas proporcionan un mecanismo para obtener tokens y, al mismo tiempo, simplifican la complejidad inherente a la creación de dichos tokens. Los desarrolladores pueden usar una TVM sin tener un conocimiento detallado de cómo la máquina produce los tokens.

Este patrón implementa una TVM mediante el uso de. AWS Lambda La TVM genera un token con credenciales del servicio de token de seguridad (STS) temporales que limitan el acceso a los datos de un único usuario de SaaS en un bucket de S3.

TVMs, y el código que se proporciona con este patrón, se suelen utilizar con afirmaciones derivadas de los JSON Web Tokens (JWTs) para asociar las solicitudes de AWS recursos a una política orientada a los inquilinos AWS Identity and Access Management (IAM). Puede usar el código de este patrón como base para implementar una aplicación SaaS que genere credenciales STS temporales y limitadas en función de las afirmaciones proporcionadas en un token JWT.

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- AWS Command Line Interface (AWS CLI) versión 1.19.0 o posterior, instalada y configurada en macOS, Linux o Windows. Como alternativa, puede utilizar la AWS CLI versión 2.1 o posterior.

Limitaciones

- Este código se ejecuta en Java y, actualmente, no es compatible con otros lenguajes de programación.

- La aplicación de ejemplo no incluye compatibilidad AWS entre regiones ni con la recuperación ante desastres (DR).
- Este patrón demuestra cómo puede proporcionar acceso limitado a los usuarios una TVM de Lambda para una aplicación SaaS. Este patrón no está diseñado para usarse en entornos de producción sin pruebas de seguridad adicionales como parte de su aplicación o caso de uso específicos.

Arquitectura

Pila de tecnología de destino

- AWS Lambda
- Amazon S3
- IAM
- AWS Security Token Service (AWS STS)

Arquitectura de destino

Tools (Herramientas)

Servicios de AWS

- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que te ayuda a interactuar Servicios de AWS mediante comandos en el shell de la línea de comandos.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Security Token Service (AWS STS) le ayuda a solicitar credenciales temporales con privilegios limitados para los usuarios.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Código

El código fuente de este patrón está disponible como archivo adjunto, e incluye los siguientes archivos:

- `s3UploadSample.jar` proporciona el código fuente de una función de Lambda que carga un documento JSON en un bucket de S3.
- `tvm-layer.zip` proporciona una biblioteca Java reutilizable que suministra un token (credenciales temporales de STS) para que la función de Lambda acceda al bucket de S3 y cargue el documento JSON.
- `token-vending-machine-sample-app.zip` proporciona el código fuente usado para crear estos artefactos y las instrucciones de compilación.

Para usar el código de muestra, siga las instrucciones de la siguiente sección.

Epics

Determine los valores de las variables

Tarea	Descripción	Habilidades requeridas
Determine los valores de las variables.	La implementación de este patrón incluye varios nombres de variables que deben usarse de manera coherente . Determine los valores a usar para cada variable y proporcio ne cada valor cuando se le solicite en los siguientes pasos. • `<AWS Account ID>`— El identificador de cuenta de 12 dígitos asociado a la cuenta en la Cuenta de AWS que está implement ando este patrón. Para obtener información sobre	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	cómo encontrar su Cuenta de AWS ID, consulte Uso de un alias para su Cuenta de AWS ID en la documentación de IAM. • `<AWS Region>`— El lugar en el Región de AWS que está implementando este patrón. Para obtener más información Regiones de AWS, consulte Regiones y zonas de disponibilidad en el AWS sitio web. • `<sample-tenant-name>` : nombre de un inquilino para utilizarlo en la aplicación. Le recomendamos que introduzca únicamente caracteres alfanuméricos en este valor por motivos de simplicidad, pero puede usar cualquier nombre válido para una clave de objeto de S3. • `<sample-tvm-role-name>` : nombre del rol de IAM asociado a la función de Lambda que ejecuta la TVM y la aplicación de muestra. El nombre del rol es una cadena compuesta por caracteres alfanuméricos en mayúscula y minúscula sin espacios.	

Tarea	Descripción	Habilidades requeridas
	También puede incluir los siguientes caracteres: guion bajo (_), signo más (+), signo igual (=), coma (,), punto (.), arroba (@) y guion (-). El nombre del rol debe ser único dentro de la cuenta. • `<sample-app-role-name>` : nombre del rol de IAM que asumirá la función de Lambda cuando genere credenciales de STS temporales y limitadas . El nombre del rol es una cadena compuesta por caracteres alfanuméricos en mayúscula y minúscula sin espacios. También puede incluir los siguiente s caracteres: guion bajo (_), signo más (+), signo igual (=), coma (,), punto (.), arroba (@) y guion (-). El nombre del rol debe ser único dentro de la cuenta. • `<sample-app-functi on-name>` : nombre de la función de Lambda. Es una cadena de hasta 64 caracteres de longitud. • `<sample-app-bucket -name>` : nombre de un bucket de S3 al que el	

Tarea	Descripción	Habilidades requeridas
	inquilino debe acceder con permisos específicos. Nombre del bucket de S3: • Deben tener entre 3 y 63 caracteres de longitud. • Deben contener solo letras minúsculas, números, puntos (.) y guiones (-). • Deben comenzar y terminar por una letra o un número. • No pueden tener el formato de una dirección IP (por ejemplo, 192.168.5.4). • Debe ser exclusivo dentro de una partición . Una partición es una agrupación de regiones. AWS actualmente tiene tres particiones: `aws` para las regiones estándar, `aws-cn` para las regiones de China y `aws-us-gov` para AWS GovCloud (US) Regions.	

Creación de un bucket de S3

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3 para la aplicación de ejemplo.	Usa el siguiente AWS CLI comando para crear un bucket de S3. Proporcione el valor de `<sample-app-bucket-name>` en el fragmento de código: `aws s3api create-bucket --bucket <sample-app-bucket-name>` La aplicación de ejemplo de Lambda carga archivos JSON en este bucket.	Administrador de la nube

Creación de una política y un rol de IAM TVM

Tarea	Descripción	Habilidades requeridas
Crear un rol de TVM.	Utilice uno de los siguientes AWS CLI comandos para crear un rol de IAM. Proporcione el valor de `<sample-tvm-role-name>` en el comando. Para los intérprete de comandos para macOS o Linux: `aws iam create-role \ --role-name <sample-tvm-role-name> \`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas

	`--assume-role-policy-document '{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "sts:AssumeRole" ], "Principal": { "Service": [ "lambda.amazonaws.com" ] }, "Condition": { "StringEquals": { "aws:SourceAccount": "<AWS Account ID>" } } } } ] }'`
	
	En la línea de comandos de Windows:
	
	`aws iam create-role ^ --role-name <sample-tvm-role-name> ^`	

Tarea	Descripción	Habilidades requeridas
	`--assume-role-policy-document "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow\", \"Action\": [\"sts:AssumeRole\"], \"Principal\": {\"Service\": [\"lambda.amazonaws.com\"]}, \"Condition\": {\"StringEquals\": {\"aws:SourceAccount\": \"<AWS Account ID>\"}}}]}"` La aplicación de ejemplo de Lambda asume este rol cuando se invoca la aplicación. La capacidad de asumir el rol de aplicación con una política específica otorga al código permisos más amplios para acceder al bucket de S3.	

Tarea	Descripción	Habilidades requeridas

Cree una política de rol de TVM en línea.	Utilice uno de los siguientes AWS CLI comandos para crear una política de IAM. Proporcione los valores de `<sample-tvm-role-name>` , `<AWS Account ID>` y `<sample-app-role-name>` en el comando.
	
	Para los intérprete de comandos para macOS o Linux:
	
	`aws iam put-role-policy \`
	`--role-name <sample-tvm-role-name> \`
	`--policy-name assume-app-role \`
	`--policy-document '{`
	`"Version": "2012-10-17",`
	`"Statement": [`
	`{`
	`"Effect": "Allow",`
	`"Action": "sts:AssumeRole",`
	`"Resource": "arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>"`
	`}`
	`]}'`
	
	En la línea de comandos de Windows:
		Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	`aws iam put-role-policy ^ --role-name <sample-tvm-role-name> ^ --policy-name assume-app-role ^ --policy-document "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow\", \"Action\": \"sts:AssumeRole\", \"Resource\": \"arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>\"}]}"` Esta política está asociada al rol de TVM. Proporciona la capacidad de asumir el rol de aplicación que otorga permisos más amplios para acceder al bucket de S3.	

Tarea	Descripción	Habilidades requeridas

Adjunte la política de Lambda gestionada.	Utilice el siguiente AWS CLI comando para adjuntar la política de `AWSLambdaBasicExecutionRole` IAM. Proporcione el valor de `<sample-tvm-role-name>` en el comando:
	`aws iam attach-role-policy \ --role-name <sample-tvm-role-name> \ --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	En la línea de comandos de Windows:
	`aws iam attach-role-policy ^ --role-name <sample-tvm-role-name> ^ --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	Esta política gestionada se adjunta a la función TVM para permitir que Lambda envíe registros a Amazon. CloudWatch
		Administrador de la nube

Cree la política y el rol de aplicación de IAM

Tarea	Descripción	Habilidades requeridas
Crear el rol de la aplicación.	Utilice uno de los siguiente s AWS CLI comandos para crear un rol de IAM. Proporcio ne los valores de `<sample-app-role-name>` , `<AWS Account ID>` y `<sample-tvm-role-name>` en el comando. Para los intérprete de comandos para macOS o Linux: `aws iam create-role \ --role-name <sample-app-role-name> \ --assume-role-policy-document '{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::<AWS Account ID>:role/<sample-tvm-role-name>" }, "Action": "sts:AssumeRole" } ]}'`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	En la línea de comandos de Windows: `aws iam create-role ^ --role-name <sample-app-role-name> ^ --assume-role-policy-document "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow\",\"Principal\": {\"AWS\": \"arn:aws:iam::<AWS Account ID>:role/<sample-tvm-role-name>\"},\"Action\": \"sts:AssumeRole\" }]}"` La aplicación de ejemplo de Lambda asume esta función con una política específica para obtener acceso basado en usuario a un bucket de S3.	

Tarea	Descripción	Habilidades requeridas
Cree una política de rol de aplicación en línea.	Utilice uno de los siguientes comandos para crear una AWS CLI política de IAM. Proporcione los valores de `<sample-app-role-name>` y `<sample-app-bucket-name>` en el comando. Para los intérprete de comandos para macOS o Linux: `aws iam put-role-policy \ --role-name <sample-app-role-name> \ --policy-name s3-bucket-access \ --policy-document '{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "s3:PutObject", "s3:GetObject", "s3:DeleteObject" ], "Resource": "arn:aws:s3:::<sample-app-bucket-name>/*" },`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas

	<pre>{
	"Effect":
	"Allow",
	"Action":
	["s3:ListBucket"],
	"Resource
	": "arn:aws:s3:::<sam
	ple-app-bucket-name>"
	}
	]}'</pre>
	En la línea de comandos de Windows:
	<pre>aws iam put-role-policy
	^
	--role-name <sample-a
	pp-role-name> ^
	--policy-name s3-bucket
	-access ^
	--policy-documen
	t "{\"Version\":
	\"2012-10-17\",
	\"Statement\":
	[{\"Effect\": \"Allow
	\", \"Action\":
	[\"s3:PutObject\",
	\"s3:GetObject\",
	\"s3:DeleteObject\
	"], \"Resource\":
	\"arn:aws:s3:::<sa
	mple-app-bucket-na
	me>/*\"}, {\"Effect\":
	\"Allow\", \"Action\
	": [\"s3:ListBucket
	\"], \"Resource\":
	\"arn:aws:s3:::<sa
	mple-app-bucket-name>
	\"}]}"</pre>	

Tarea	Descripción	Habilidades requeridas
	Esta política está asociada al rol de la aplicación. Proporciona un acceso amplio a los objetos del bucket de S3. Cuando la aplicación de ejemplo asume el rol, estos permisos se asignan a un usuario específico con la política de TVM generada de forma dinámica.	

Cree la aplicación de muestra de Lambda con TVM

Tarea	Descripción	Habilidades requeridas
Descargue los archivos fuente compilados.	Descargue los archivos `s3UploadSample.jar` y `tvm-layer.zip`, que se incluyen como adjuntos. El código fuente utilizado para crear estos artefactos y las instrucciones de compilación se proporcionan en `token-vending-machine-sample-app.zip`.	Administrador de la nube
Cree la capa de Lambda.	Utilice el siguiente AWS CLI comando para crear una capa Lambda, que haga que Lambda pueda acceder a la TVM.	Administrador de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	Note
	Si no ejecuta este comando desde la ubicación en la que descargó `tvm-layer.zip`, indique la ruta correcta a `tvm-layer.zip` en el parámetro `--zip-file`.
	
	`aws lambda publish-layer-version \ --layer-name sample-token-vending-machine \ --compatible-runtimes java11 \ --zip-file fileb://tvm-layer.zip`
	
	En la línea de comandos de Windows:
	
	`aws lambda publish-layer-version ^ --layer-name sample-token-vending-machine ^ --compatible-runtimes java11 ^ --zip-file fileb://tvm-layer.zip`	

Tarea	Descripción	Habilidades requeridas
	Este comando crea una capa de Lambda que contiene la biblioteca TVM reutilizable.	

Tarea	Descripción	Habilidades requeridas
Crear la función de Lambda.	Utilice el siguiente AWS CLI comando para crear una función Lambda. Proporcione los valores de `<sample-app-function-name>`, `<AWS Account ID>`, `<AWS Region>`, `<sample-tvm-role-name>`, `<sample-app-bucket-name>` y `<sample-app-role-name>` en el comando. **Note** Si no ejecuta este comando desde la ubicación en la que descargó `s3UploadSample.jar`, indique la ruta correcta a `s3UploadSample.jar` en el parámetro `--zip-file`. `aws lambda create-function \ --function-name <sample-app-function-name> \ --timeout 30 \ --memory-size 256 \ --runtime java11 \ --role arn:aws:iam::<AWS Account`	Administrador de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	ID>:role/<sample-tvm-role-name> \ --handler com.amazon.aws.s3UploadSample.App \ --zip-file fileb://s3UploadSample.jar \ --layers arn:aws:lambda:<AWS Region>:<AWS Account ID>:layer:sample-token-vending-machine:1 \ --environment "Variables={S3_BUCKET=<sample-app-bucket-name>, ROLE=arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>}" En la línea de comandos de Windows: aws lambda create-function ^ --function-name <sample-app-function-name> ^ --timeout 30 ^ --memory-size 256 ^ --runtime java11 ^ --role arn:aws:iam::<AWS Account ID>:role/<sample-tvm-role-name> ^ --handler com.amazon.aws.s3UploadSample.App ^ --zip-file fileb://s3UploadSample.jar ^	

Tarea	Descripción	Habilidades requeridas
	`--layers arn:aws:lambda:<AWS Region>:<AWS Account ID>:layer:sample-token-vending-machine:1 ^ --environment "Variables={S3_BUCKET=<sample-app-bucket-name>,ROLE=arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>}"` Este comando crea una función de Lambda con el código de la aplicación de ejemplo y la capa de TVM adjunta. También establece dos variables de entorno: `S3_BUCKET` y `ROLE`. La aplicación de ejemplo usa estas variables para determinar el rol que debe asumir y el bucket de S3 en el que se deben cargar los documentos JSON.	

Pruebe la aplicación de muestra y TVM

Tarea	Descripción	Habilidades requeridas
Invoque la aplicación de ejemplo de Lambda.	Utilice uno de los siguientes AWS CLI comandos para iniciar la aplicación de ejemplo de Lambda con la carga útil esperada. Proporcione	Administrador de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	los valores de `<sample-app-function-name>` y `<sample-tenant-name>` en el comando.
	
	Para intérprete de comandos macOS y Linux:
	
	`aws lambda invoke \ --function <sample-app-function-name> \ --invocation-type RequestResponse \ --payload '{"tenant": "<sample-tenant-name>"}' \ --cli-binary-format raw-in-base64-out response.json`
	
	En la línea de comandos de Windows:
	
	`aws lambda invoke ^ --function <sample-app-function-name> ^ --invocation-type RequestResponse ^ --payload "{\"tenant\": \"<sample-tenant-name>\"}" ^ --cli-binary-format raw-in-base64-out response.json`
	
	Este comando llama a la función de Lambda y devuelve el resultado en un documento	

Tarea	Descripción	Habilidades requeridas
	`response.json` . En muchos sistemas basados en Unix, puede cambiar `response.json` a `/dev/stdout` para enviar los resultados directamente a su intérprete de comandos sin necesidad de crear otro archivo. **Note** Si cambia el valor de `<sample-tenant-name>` en las siguientes invocaciones de esta función de Lambda, se modificará la ubicación del documento JSON y los permisos proporcionados por el token.	

Tarea	Descripción	Habilidades requeridas
Acceda al bucket de S3 para ver los objetos creados.	Acceda al bucket de S3 (`<sample-app-bucket-name>`) que creó anteriormente. Este bucket contiene un prefijo de objeto de S3 con el valor de `<sample-tenant-name>` . Bajo ese prefijo, encontrará un documento JSON denominado con un UUID. Si invoca la aplicación de ejemplo varias veces, se añadirán más documentos JSON.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Vea los registros de la aplicación de muestra en CloudWatch Logs.	Vea los registros que están asociados a la función Lambda nombrada `<sample-app-function-name>` en CloudWatch Logs. Para obtener instrucciones, consulte Envío de registros de funciones de Lambda a CloudWatch registros en la documentación de Lambda. En estos registros puede ver la política basada en usuario generada por la TVM. Esta política dirigida al inquilino otorga permisos para la aplicación de ejemplo a Amazon S3 PutObject ,, y GetObjectDeleteObj ectListBucket APIs, pero solo para el prefijo de objeto al que está asociado. `<sample-tenant-name>` En las siguientes invocaciones de la aplicación de muestra, si cambia `<sample-tenant-name>` , la TVM actualizará la política con el ámbito de aplicación para adaptarla al inquilino proporcionado en la carga útil de invocación. Esta política generada dinámicam ente muestra cómo se puede mantener el acceso basado	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	en usuario con una TVM en aplicaciones SaaS. La funcionalidad de TVM se proporciona en una capa de Lambda. Así, es posible adjuntarla a otras funciones de Lambda usadas por una aplicación sin tener que replicar el código. Para ver un ejemplo de la política generada dinámicam ente, consulte la sección de Información adicional.	

Recursos relacionados

- Aislar a los usuarios con políticas de IAM generadas dinámicamente (publicación del blog)
- Applying Dynamically Generated Isolation Policies in SaaS Environments (entrada en el blog)
- SaaS en AWS

Información adicional

En el siguiente registro se muestra la política generada de forma dinámica y creada por el código de la TVM de este patrón. En esta captura de pantalla, `<sample-app-bucket-name>` es `DOC-EXAMPLE-BUCKET` y `<sample-tenant-name>` es `test-tenant-1`. Las credenciales de STS emitidas por esta política limitada no pueden realizar ninguna acción en los objetos del bucket de S3, excepto en aquellos objetos asociados al prefijo de clave de objeto `test-tenant-1`.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Implementar el patrón saga sin servidor mediante AWS Step Functions

Tabby Ward, Joe Kern y Rohan Mehta, Amazon Web Services

Resumen

En una arquitectura de microservicios, el objetivo principal es crear componentes disociados e independientes para promover la agilidad, la flexibilidad y reducir el tiempo de comercialización de sus aplicaciones. Como resultado del desacoplamiento, cada componente del microservicio tiene su propia capa de persistencia de datos. En una arquitectura distribuida, las transacciones comerciales pueden abarcar varios microservicios. Como estos microservicios no pueden utilizar una sola transacción de atomicidad, coherencia, aislamiento y durabilidad (ACID), es posible que acabe con transacciones parciales. En este caso, se necesita alguna lógica de control para deshacer las transacciones que ya se han procesado. El patrón saga distribuido se utiliza normalmente para este propósito.

El patrón saga es un patrón de gestión de fallos que ayuda a establecer la coherencia en las aplicaciones distribuidas y coordina las transacciones entre varios microservicios para mantener la coherencia de los datos. Si se utiliza el patrón «saga», cada servicio que realiza una transacción publica un evento que desencadena que los servicios subsiguientes realicen la siguiente transacción de la cadena. Esto continúa hasta que se complete la última transacción de la cadena. Si una transacción comercial fracasa, Saga organiza una serie de transacciones compensatorias que anulan los cambios introducidos en las transacciones anteriores.

Este patrón demuestra cómo automatizar la configuración y el despliegue de una aplicación de muestra (que gestiona las reservas de viajes) con tecnologías sin servidor, como AWS Step Functions, AWS Lambda y Amazon DynamoDB. La aplicación de ejemplo también utiliza Amazon API Gateway y Amazon Simple Notification Service (Amazon SNS) para implementar un coordinador de ejecución de saga. El patrón se puede implementar con un marco de infraestructura como código (IaC), como el AWS Cloud Development Kit (AWS CDK), el AWS Serverless Application Model (AWS Serverless Application Model SAM) o Terraform.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Permisos para crear una CloudFormation pila de AWS. Para obtener más información, consulte Controlar el acceso en la CloudFormation documentación.

- El marco de IaC de su elección (AWS CDK, AWS SAM o Terraform) se configuró con su cuenta de AWS para que pueda usar la CLI del marco para implementar la aplicación.
- NodejS, utilizado para compilar la aplicación y ejecutarla localmente.
- Un editor de código de su elección (como Visual Studio Code, Sublime o Atom).

Versiones de producto

- NodeJS versión 14
- AWS CDK versión 2.37.1
- AWS SAM versión 1.71.0
- Terraform versión 1.3.7

Limitaciones

El abastecimiento de eventos es una forma natural de implementar el patrón de orquestación de la saga en una arquitectura de microservicios en la que todos los componentes están acoplados de forma flexible y no se conocen directamente entre sí. Si su transacción incluye un número reducido de pasos (de tres a cinco), el patrón saga podría ser una buena opción. Sin embargo, la complejidad aumenta con el número de microservicios y el número de pasos.

Las pruebas y la depuración pueden resultar difíciles cuando se utiliza este diseño, ya que es necesario tener todos los servicios en ejecución para poder simular el patrón de transacciones.

Arquitectura

Arquitectura de destino

La arquitectura propuesta utiliza AWS Step Functions para crear un patrón de saga para reservar vuelos, reservar alquileres de vehículos y procesar los pagos de las vacaciones.

El siguiente diagrama de flujo de trabajo ilustra el flujo típico del sistema de reservas de viajes. El flujo de trabajo consiste en reservar un viaje en avión (» ReserveFlight «), reservar un automóvil (» ReserveCarRental «), procesar los pagos (» ProcessPayment «), confirmar las reservas de vuelos (» ConfirmFlight «) y confirmar el alquiler de vehículos (» ConfirmCarRental «), seguido de una notificación de éxito cuando se hayan completado estos pasos. Sin embargo, si el sistema detecta algún error al ejecuter alguna de estas transacciones, empezará a fallar hacia atrás. Por ejemplo, un error en el procesamiento del pago (» ProcessPayment «) desencadena un reembolso

(» RefundPayment «), que luego desencadena la cancelación del coche de alquiler y del vuelo (» CancelRentalReservation "y CancelFlightReservation «), lo que finaliza toda la transacción con un mensaje de error.

Este patrón implementa funciones Lambda independientes para cada tarea que se resalta en el diagrama, así como tres tablas de DynamoDB para vuelos, alquileres de vehículos y pagos. Cada función de Lambda crea, actualiza o elimina las filas de las tablas de DynamoDB respectivas, en función de si la transacción se confirma o se revierte. El patrón utiliza Amazon SNS para enviar mensajes de texto (SMS) a los suscriptores y notificarles las transacciones fallidas o satisfactorias.

Automatización y escala

Puede crear la configuración de esta arquitectura mediante uno de los marcos de IaC. Utilice uno de los siguientes enlaces para su iAC preferido.

- Implementar con AWS CDK
- Implementar con AWS SAM
- Implementar con Terraform

Tools (Herramientas)

Servicios de AWS

- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de AWS Lambda y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial. A través de la consola gráfica Step Functions, puede ver el flujo de trabajo de su aplicación como una serie de pasos basados en eventos.
- Amazon DynamoDB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido y predecible, así como una perfecta escalabilidad. Puede utilizar DynamoDB para crear una tabla de base de datos capaz de almacenar y recuperar cualquier cantidad de datos, así como de atender cualquier nivel de tráfico de solicitudes.
- AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- Amazon API Gateway es un servicio de AWS para crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket APIs a cualquier escala.

- Amazon Simple Notification Service (Amazon SNS) es un servicio administrado que proporciona la entrega de mensajes de los publicadores a los suscriptores.
- El AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software para definir los recursos de las aplicaciones en la nube mediante lenguajes de programación conocidos TypeScript, como Python JavaScript, Java y C#/.Net.
- AWS Serverless Application Model (AWS SAM) es un marco de código abierto que permite crear aplicaciones sin servidor. Proporciona una sintaxis abreviada para expresar funciones, bases de datos y mapeos de fuentes de APIs eventos.

Código

El código de una aplicación de ejemplo que muestra el patrón saga, incluida la plantilla IaC (AWS CDK, AWS SAM o Terraform), las funciones de Lambda y las tablas de DynamoDB, se encuentra en los siguientes enlaces. Siga las instrucciones de la primera epic para instalarlos.

- Implementar con AWS CDK
- Implementar con AWS SAM
- Implementar con Terraform

Epics

Instalar paquetes, compilar y compilar

Tarea	Descripción	Habilidades requeridas
Instalar los paquetes NPM.	Cree un directorio nuevo, navegue hasta ese directori o en una terminal y clone el GitHub repositorio que prefiera en la sección de código que aparece anteriormente en este patrón. En la carpeta raíz que contiene el archivo `package.json` , ejecute	Desarrollador, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	el siguiente comando para descargar e instalar todos los paquetes de Node Package Manager (NPM): `npm install`	
Compilar scripts.	En la carpeta raíz, ejecute el siguiente comando para indicar al TypeScript transpilador que cree todos los archivos necesarios: JavaScript `npm run build`	Desarrollador, arquitecto de la nube
Esté atento a los cambios y vuelva a compilar.	En la carpeta raíz, ejecute el siguiente comando en una ventana de terminal independiente para comprobar si hay cambios en el código y compílalo cuando lo detecte: `npm run watch`	Desarrollador, arquitecto de la nube
Ejecute pruebas unitarias (solo AWS CDK).	Si utiliza el CDK de AWS, en la carpeta raíz, ejecute el siguiente comando para realizar las pruebas unitarias de Jest: `npm run test`	Desarrollador, arquitecto de la nube

Implemente recursos en la cuenta de AWS de destino

Tarea	Descripción	Habilidades requeridas

Implemente la pila de demostración en AWS.	**Important**
	La aplicación es independiente de la región de AWS. Si utiliza un perfil, debe declarar la región de forma explícita en el perfil de la interfaz de la línea de comandos de AWS (AWS CLI) o mediante variables de entorno de la CLI de AWS.
	
	En la carpeta raíz, ejecute el siguiente comando para crear un ensamblaje de implement ación e implementarlo en la cuenta y región de AWS predeterminadas.
	
	AWS CDK:
	
	`cdk bootstrap`
	`cdk deploy`
	
	AWS SAM:
	
	`sam build`
	`sam deploy --guided`
		Desarrollador, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas

	Terraform:
	
	`terraform init`
	`terraform apply`
	
	Este paso puede tardar varios minutos en completarse. Este comando usa las credencia les predeterminadas que se configuraron para la AWS CLI.
	
	Anote la URL de API Gateway que se muestra en la consola una vez completada la implementación. Necesitará esta información para probar el flujo de ejecución de la saga.	

Tarea	Descripción	Habilidades requeridas

Compare la pila implementada con el estado actual.	En la carpeta raíz, ejecute el siguiente comando para comparar la pila implementada con el estado actual después de realizar cambios en el código fuente:
	AWS CDK:
	`cdk diff`
	AWS SAM:
	`sam deploy`
	Terraform:
	`terraform plan`
		Desarrollador, arquitecto de la nube

Pruebe el flujo de ejecución

Tarea	Descripción	Habilidades requeridas
Probar el flujo de ejecución de la saga.	Navegue hasta la URL de API Gateway que indicó en el paso anterior, cuando implementó la pila. Esta URL activa el inicio de la máquina de estados. Para obtener más información sobre cómo manipular el flujo de la máquina de estados pasando diferentes parámetro	Desarrollador, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	s de URL, consulte la sección de Información adicional. Para ver los resultados, inicie sesión en la consola de administración de AWS y vaya a la consola de Step Functions . Aquí puede ver todos los pasos de la saga State Machine. También puede ver la tabla de DynamoDB para ver los registros insertado s, actualizados o eliminado s. Si actualiza la pantalla con frecuencia, puede ver cómo el estado de la transacci ón cambia de `apending`. `confirmed` Puede suscribirse al tema de las redes sociales actualiza ndo el código del archivo `stateMachine.ts` con su número de teléfono móvil para recibir mensajes SMS cuando las reservas se hayan realizado o no se hayan realizado correctamente. Para obtener más información, consulte Amazon SNS en la sección Información adicional.	

Limpieza

Tarea	Descripción	Habilidades requeridas

Limpiar recursos.	Para limpiar los recursos desplegados para esta aplicación, puede usar uno de los siguientes comandos.
	
	AWS CDK:
	
	`cdk destroy`
	
	AWS SAM:
	
	`sam delete`
	
	Terraform:
	
	`terraform destroy`
		Desarrollador de aplicaciones, arquitecto de la nube

Recursos relacionados

Documentos técnicos

- Implementación de microservicios en AWS
- Aplicaciones sin servidor

Documentación de servicio de AWS

- Introducción a los AWS SDK
- Introducción a AWS SAM
- AWS Step Functions
- Amazon DynamoDB
- AWS Lambda

- Amazon API Gateway
- Amazon SNS

Tutoriales

- Talleres prácticos sobre informática sin servidor

Información adicional

Código

Con fines de prueba, este patrón implementa API Gateway y una función de Lambda de prueba que activa la máquina de estados Step Functions. Con Step Functions, puede controlar la funcionalidad del sistema de reservas de viajes pasando un `run_type` parámetro para imitar los errores en «ReserveFlightReserveCarRental,»»» ProcessPaymentConfirmFlight,»» y «»ConfirmCarRental.

La `saga`función de Lambda (`sagaLambda.ts`) toma la entrada de los parámetros de consulta de la URL de la API Gateway, crea el siguiente objeto JSON y lo pasa a Step Functions para su ejecución:

```
let input = {
"trip_id": tripID, //  value taken from query parameter, default is AWS request ID
"depart_city": "Detroit",
"depart_time": "2021-07-07T06:00:00.000Z",
"arrive_city": "Frankfurt",
"arrive_time": "2021-07-09T08:00:00.000Z",
"rental": "BMW",
"rental_from": "2021-07-09T00:00:00.000Z",
"rental_to": "2021-07-17T00:00:00.000Z",
"run_type": runType // value taken from query parameter, default is "success"
};
```

Puede experimentar con diferentes flujos de la máquina de estados Step Functions pasando los siguientes parámetros de URL:

- Ejecución correcta: https://{api gateway url}
- Error en la reserva del vuelo — https://{api gateway url}? Tipo de ejecución = failFlightsReservation
- Confirma el error del vuelo — https://{api gateway url}? Tipo de ejecución = failFlightsConfirmation
- Error al alquilar un coche al reservar — https://{api gateway url}? RunType = Reserva failCarRental

- Confirme que el alquiler del vehículo ha fallado – https://{api gateway url}? RunType = Confirmación failCarRental
- Error al procesar el pago: https://{api gateway url}?runType=failPayment
- Pasar un identificador de viaje: https://{api gateway url}? tripID= {de forma predeterminada, el ID de viaje será el ID de solicitud de AWS}

Plantillas de iAC

Los repositorios enlazados incluyen plantillas de IaC que puede utilizar para crear toda la aplicación de reserva de viajes de muestra.

- Implementar con AWS CDK
- Implementar con AWS SAM
- Implementar con Terraform

Tablas de DynamoDB

Estos son los modelos de datos para las tablas de vuelos, alquileres de coches y pagos.

```
Flight Data Model:
 var params = {
      TableName: process.env.TABLE_NAME,
      Item: {
        'pk' : {S: event.trip_id},
        'sk' : {S: flightReservationID},
        'trip_id' : {S: event.trip_id},
        'id': {S: flightReservationID},
        'depart_city' : {S: event.depart_city},
        'depart_time': {S: event.depart_time},
        'arrive_city': {S: event.arrive_city},
        'arrive_time': {S: event.arrive_time},
        'transaction_status': {S: 'pending'}
      }
    };

Car Rental Data Model:
var params = {
      TableName: process.env.TABLE_NAME,
      Item: {
        'pk' : {S: event.trip_id},
```

```
        'sk' : {S: carRentalReservationID},
        'trip_id' : {S: event.trip_id},
        'id': {S: carRentalReservationID},
        'rental': {S: event.rental},
        'rental_from': {S: event.rental_from},
        'rental_to': {S: event.rental_to},
        'transaction_status': {S: 'pending'}
      }
    };

Payment Data Model:
var params = {
      TableName: process.env.TABLE_NAME,
      Item: {
        'pk' : {S: event.trip_id},
        'sk' : {S: paymentID},
        'trip_id' : {S: event.trip_id},
        'id': {S: paymentID},
        'amount': {S: "750.00"}, // hard coded for simplicity as implementing any
 monetary transaction functionality is beyond the scope of this pattern
        'currency': {S: "USD"},
        'transaction_status': {S: "confirmed"}
      }
    };
```

Funciones de Lambda

Se crearán las siguientes funciones para respaldar el flujo y la ejecución de la máquina de estados en Step Functions:

- Reservar vuelos: introduzca un registro en la tabla de vuelos de DynamoDB con `transaction_status` un `pending` de para reservar un vuelo.
- Confirmar vuelo: actualiza el registro de la tabla de vuelos de DynamoDB para establecer `transaction_status` en `confirmed`, para confirmar el vuelo.
- Cancelar reserva de vuelos: elimina el registro de la tabla de vuelos de DynamoDB para cancelar el vuelo pendiente.
- Reserve vehículos de alquiler: inserta un registro en la tabla de CarRentals DynamoDB con `transaction_status` un `pending` de para reservar un alquiler de vehículos.
- Confirmar alquileres de vehículos: actualiza el registro de la tabla de CarRentals DynamoDB para `transaction_status` `confirmed` establecerlo en y confirmar el alquiler de vehículos.

- Cancelar reserva de vehículos de alquiler: elimina el registro de la tabla de CarRentals DynamoDB para cancelar el alquiler de vehículos pendiente.
- Procesar pago: inserta un registro en la tabla de pagos de DynamoDB para el pago.
- Cancelar pago: elimina el registro del pago de la tabla de pagos de DynamoDB.

Amazon SNS

La aplicación de ejemplo crea el tema y la suscripción siguientes para enviar mensajes SMS y notificar al cliente si las reservas se han realizado o no se han realizado correctamente. Si desea recibir mensajes de texto mientras prueba la aplicación de ejemplo, actualice la suscripción de SMS con su número de teléfono válido en el archivo de definición de la máquina de estados.

Fragmento de CDK de AWS (añada el número de teléfono en la segunda línea del siguiente código):

```
const topic = new  sns.Topic(this, 'Topic');
topic.addSubscription(new subscriptions.SmsSubscription('+11111111111'));
const snsNotificationFailure = new tasks.SnsPublish(this ,'SendingSMSFailure', {
topic:topic,
integrationPattern: sfn.IntegrationPattern.REQUEST_RESPONSE,
message: sfn.TaskInput.fromText('Your Travel Reservation Failed'),
});

const snsNotificationSuccess = new tasks.SnsPublish(this ,'SendingSMSSuccess', {
topic:topic,
integrationPattern: sfn.IntegrationPattern.REQUEST_RESPONSE,
message: sfn.TaskInput.fromText('Your Travel Reservation is Successful'),
});
```

Fragmento de SAM de AWS (sustituya las cadenas +1111111111 por su número de teléfono válido):

```
  StateMachineTopic11111111111:
    Type: 'AWS::SNS::Subscription'
    Properties:
      Protocol: sms
      TopicArn:
        Ref: StateMachineTopic
      Endpoint: '+11111111111'
    Metadata:
      'aws:sam:path': SamServerlessSagaStack/StateMachine/Topic/+11111111111/Resource
```

Fragmento de Terraform (sustituya la cadena +111111111 por su número de teléfono válido):

```
resource "aws_sns_topic_subscription" "sms-target" {
  topic_arn = aws_sns_topic.topic.arn
  protocol  = "sms"
  endpoint  = "+11111111111"
}
```

Reservas realizadas satisfactoriamente

En el siguiente flujo se muestra una reserva correcta con los caracteres "ReserveFlight,»ReserveCarRental,» y "" seguidos de ProcessPayment "" y ConfirmFlight "». ConfirmCarRental Se notifica al cliente que la reserva se ha realizado correctamente mediante mensajes SMS que se envían al suscriptor del tema de las redes sociales.

Reservas fallidas

Este flujo es un ejemplo de fracaso en el patrón de la saga. Si, después de reservar vuelos y alquileres de vehículos, "ProcessPayment" falla, los pasos se cancelan en orden inverso. Se cancelan las reservas y se notifica al cliente del error mediante mensajes SMS que se envían al suscriptor del tema de las redes sociales.

Gestión de las aplicaciones de contenedores en las instalaciones mediante la configuración de Amazon ECS Anywhere con AWS CDK

Dr. Rahul Sharad Gaikwad, Amazon Web Services

Resumen

Amazon ECS Anywhere es una extensión de Amazon Elastic Container Service (Amazon ECS). Puede usar ECS Anywhere para implementar tareas nativas de Amazon ECS en un entorno en las instalaciones o administrado por el cliente. Esta característica ayuda a reducir los costos y a mitigar la compleja orquestación y las operaciones de los contenedores locales. Puede usar ECS Anywhere para implementar y ejecutar aplicaciones de contenedor tanto en entornos en las instalaciones como en la nube. Evita que su equipo tenga que aprender varios dominios y conjuntos de habilidades, o administrar software complejo por su cuenta.

Este patrón muestra los pasos para configurar ECS Anywhere mediante pilas del AWS Cloud Development Kit (AWS CDK).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada. (Consulte Instalación, actualización y desinstalación de la CLI de AWS en la documentación de la CLI de AWS).
- Kit de herramientas de AWS CDK, instalado y configurado. (Consulte Kit de Herramientas CDK de AWS en la documentación de AWS CDK y siga las instrucciones para instalar la versión 2 de forma global).
- Administrador de paquetes de nodos (npm), instalado y configurado para la AWS CDK en. TypeScript (Consulte Descargar e instalar Node.js y npm en la documentación de npm).

Limitaciones

- Para ver las limitaciones y consideraciones, consulte Instancias externas (Amazon ECS Anywhere) en la documentación de Amazon ECS.

Versiones de producto

- Kit de Herramientas CDK de AWS, versión 2
- npm versión 7.20.3 o posterior
- Node.js versión 16.6.1 o posterior

Arquitectura

Pila de tecnología de destino

- AWS CloudFormation
- AWS CDK
- Amazon ECS Anywhere
- AWS Identity y Access Management (IAM)

Arquitectura de destino

El siguiente diagrama ilustra una arquitectura de sistema de alto nivel de la configuración de ECS Anywhere que utiliza la AWS CDK con TypeScript, tal como se implementa mediante este patrón.

1. Al implementar la pila de CDK de AWS, se crea una CloudFormation pila en AWS.
2. La CloudFormation pila aprovisiona un clúster de Amazon ECS y los recursos de AWS relacionados.
3. Para registrar una instancia externa en un clúster de Amazon ECS, debe instalar AWS Systems Manager Agent (SSM Agent) en su máquina virtual (VM) y registrar la VM como instancia administrada por AWS Systems Manager.
4. También debe instalar el agente de contenedores de Amazon ECS y Docker en su máquina virtual para registrarla como instancia externa en el clúster de Amazon ECS.
5. Cuando la instancia externa está ya registrada y configurada con el clúster de Amazon ECS, puede ejecutar varios contenedores en su máquina virtual, registrada como instancia externa.

Automatización y escala

El GitHub repositorio que se proporciona con este patrón utiliza la CDK de AWS como herramienta de infraestructura como código (IaC) para crear la configuración de esta arquitectura. AWS CDK le ayuda a orquestar los recursos y configurar ECS Anywhere.

Tools (Herramientas)

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.

Código

El código fuente de este patrón está disponible en el GitHub repositorio de muestras de CDK de Amazon ECS Anywhere. Para clonar y utilizar el repositorio, siga las instrucciones de la siguiente sección.

Epics

Verificar la configuración de AWS CDK

Tarea	Descripción	Habilidades requeridas
Verifique la versión de AWS CDK.	Compruebe la versión del kit de herramientas de AWS CDK mediante el siguiente comando: `cdk --version` Este patrón requiere la versión 2 de AWS CDK. Si tiene una versión anterior de AWS CDK siga las instrucciones de la documentación de AWS CDK para actualizarla.	DevOps ingeniero
Configure las credenciales de AWS.	Para configurar las credenciales, ejecute el comando `aws configure` y siga las instrucciones:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	`$aws configure`
	`AWS Access Key ID`
	` [None]: <your-access-key-ID>`
	`AWS Secret Access Key`
	` [None]: <your-secret-access-key>`
	`Default region name`
	` [None]: <your-Region-name>`
	`Default output format`
	` [None]:`	

Inicie el entorno de AWS CDK

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio de código de AWS CDK.	Clona el repositorio de GitHub código de este patrón mediante el comando: `git clone https://github.com/aws-samples/amazon-ecs-anywhere-cdk-samples.git`	DevOps ingeniero
Arranque el entorno de .	Para implementar la CloudFormation plantilla de AWS en la cuenta y la región de AWS que desee usar, ejecute el siguiente comando: `cdk bootstrap <account-number>/<Region>`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte Proceso de arranque en la documentación de AWS CDK.	

Crear e implementar el proyecto

Tarea	Descripción	Habilidades requeridas

Instale las dependencias de los paquetes y compile TypeScript los archivos.	Instale las dependencias del paquete y compile los TypeScript archivos ejecutando los siguientes comandos:
	`$cd amazon-ecs-anywhere-cdk-samples`
	`$npm install`
	`$npm fund`
	Estos comandos instalan todos los paquetes del repositorio de muestra.
	Important
	Si se muestra algún error acerca de paquetes que faltan, utilice uno de los siguientes comandos:
	`$npm ci`
	—o—
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`$npm install -g @aws-cdk/<package_name>` Para obtener más información, consulte npm ci y npm install en la documentación de npm.	
Compilar el proyecto.	Ejecute el siguiente comando para compilar el código del proyecto: `npm run build` Para obtener más informaci ón sobre la compilaci ón e implementación del proyecto, consulte Su primera aplicación de AWS CDK en la documentación de AWS CDK.	DevOps ingeniero
Implementar el proyecto.	Para implementar el código del proyecto, ejecute el comando: `cdk deploy`	DevOps ingeniero
Verifique la creación y el resultado de la pila.	Abra la CloudFormation consola de AWS en https://console.aws.amazon.com/cloudformation y elija la `EcsAnywhereStack` pila. La pestaña Salidas muestra los comandos que se deben ejecutar en su máquina virtual externa.	DevOps ingeniero

Configuración de una máquina en las instalaciones

Tarea	Descripción	Habilidades requeridas
Configure su máquina virtual mediante Vagrant.	Con fines de demostración, puede usar HashiCorp Vagrant para crear una máquina virtual. Vagrant es una utilidad de código abierto para compilar y mantener entornos de desarrollo de software virtual portátiles. Cree una máquina virtual Vagrant ejecutando el comando `vagrant up` desde el directorio raíz donde se encuentra Vagrantfile. Para obtener más información, consulte la documentación de Vagrant.	DevOps ingeniero
Registre su máquina virtual como instancia externa.	1. Inicie sesión en la máquina virtual de Vagrant mediante el comando `vagrant ssh`. Para obtener más información, consulte la documentación de Vagrant. 2. Cree un código de activación y una ID que usará para registrar su máquina virtual en AWS Systems Manager y activar su instancia externa. El resultado de este comando incluye valores `ActivationId` y `ActivationCode` :	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	`aws ssm create-activation --iam-role EcsAnywhereInstanceRole | tee ssm-activation.json`
	
	3. Exporte el ID de activación y los valores del código:
	
	`export ACTIVATION_ID=<activation-ID>`
	`export ACTIVATION_CODE=<activation-code>`
	
	4. Descargar el script de instalación en el servidor ubicado en las instalaciones o en la máquina virtual (VM):
	
	`curl -o "ecs-anywhere-install.sh" "https://amazon-ecs-agent.s3.amazonaws.com/ecs-anywhere-install-latest.sh" && sudo chmod +x ecs-anywhere-install.sh`
	
	5. Ejecute el script de instalación en el servidor ubicado en las instalaciones o en la máquina virtual (VM).
	
	`sudo ./ecs-anywhere-install.sh \`
	`--cluster test-ecs-anywhere \`	

Tarea	Descripción	Habilidades requeridas
	`--activation-id $ACTIVATION_ID \ --activation-code $ACTIVATION_CODE \ --region <Region>` Para obtener más información sobre la configuración y el registro de su máquina virtual, consulte Registrar una instancia externa en un clúster en la documentación de Amazon ECS.	
Verifique el estado de ECS Anywhere y de la máquina virtual externa.	Para verificar si su caja virtual está conectada al plano de control de Amazon ECS y en funcionamiento, utilice los siguientes comandos: `aws ssm describe-instance-information aws ecs list-container-instances --cluster $CLUSTER_NAME`	DevOps ingeniero

Limpieza

Tarea	Descripción	Habilidades requeridas
Limpie y elimine recursos.	Después de seguir este patrón, debe eliminar los recursos que ha creado para evitar incurrir en cargos adicionales. Para limpiar, ejecute el comando:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`cdk destroy`	

Recursos relacionados

- Documentación de Amazon ECS Anywhere
- Amazon ECS Anywhere Demo
- Muestras de talleres sobre Amazon ECS Anywhere

Incorporación de inquilinos en la arquitectura SaaS para el modelo de silo mediante C# y AWS CDK

Tabby Ward, Susmitha Reddy Gankidi y Vijai Anand Ramalingam, Amazon Web Services

Resumen

Las aplicaciones de software como servicio (SaaS) se pueden crear con una variedad de modelos arquitectónicos diferentes. El modelo de silo se refiere a una arquitectura en la que los inquilinos reciben recursos específicos.

Las aplicaciones SaaS se basan en un modelo sencillo para introducir nuevos inquilinos en su entorno. Esto suele requerir la orquestación de varios componentes para aprovisionar y configurar correctamente todos los elementos necesarios para crear un nuevo inquilino. Este proceso, en la arquitectura SaaS, se denomina incorporación de inquilinos. La incorporación debe automatizarse por completo en todos los entornos de SaaS y utilizar la infraestructura como código en el proceso de incorporación.

Este patrón le guía a través de un ejemplo de creación de un inquilino y aprovisionamiento de una infraestructura básica para el inquilino en Amazon Web Services (AWS). El patrón utiliza C# y el AWS Cloud Development Kit (AWS CDK).

Como este patrón crea una alarma de facturación, le recomendamos implementar la pila en la región Este de EE. UU. (Norte de Virginia) o us-east-1 de AWS. Para obtener más información, consulte la documentación de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una entidad principal de AWS Identity and Access Management (IAM) con acceso suficiente de IAM para crear recursos de AWS para este patrón. Para obtener más información, consulte Roles de IAM.
- Instale Amazon Command Line Interface (AWS CLI) y configure la CLI de AWS para realizar la implementación de la CDK de AWS.
- Visual Studio 2022 descargado o instalado o Visual Studio Code descargado o instalado.

- Configuración de AWS Toolkit para Visual Studio.
- .NET Core 3.1 o posterior (necesario para las aplicaciones de AWS CDK de C#)
- Amazon.Lambda.Tools instalado.

Limitaciones

- La CDK de AWS utiliza AWS CloudFormation, por lo que las aplicaciones de la CDK de AWS están sujetas a cuotas de CloudFormation servicio. Para obtener más información, consulte CloudFormation Cuotas de AWS.
- La CloudFormation pila de inquilinos se crea con un rol de CloudFormation servicio `infra-cloudformation-role` con caracteres comodín en las acciones (`sns* ysqs*`), pero con los recursos limitados al `tenant-cluster` prefijo. Para un caso de uso de producción, evalúe esta configuración y proporcione únicamente el acceso obligatorio a este rol de servicio. La función `InfrastructureProvision` Lambda también usa un carácter comodín (`cloudformation*`) para aprovisionar la CloudFormation pila, pero con los recursos limitados al prefijo. `tenant-cluster`
- La compilación de docker de este ejemplo de código utiliza `--platform=linux/amd64` para forzar imágenes basadas en `linux/amd64`. Esto es para garantizar que los artefactos de imagen finales sean adecuados para Lambda, que de forma predeterminada utiliza una arquitectura x86-64. Si necesita cambiar la arquitectura Lambda de destino, asegúrese de cambiar los códigos CDK de Dockerfiles y de AWS. Para obtener más información, consulte esta entrada en el blog: Migrating AWS Lambda functions to Arm-based AWS Graviton2 processors.
- El proceso de eliminación de la pila no limpiará CloudWatch los registros (grupos de registros y registros) generados por la pila. Debe limpiar los registros manualmente a través de la consola de administración de AWS, la CloudWatch consola Amazon o la API.

Este patrón se configura a modo de ejemplo. Para su uso en producción, evalúe las siguientes configuraciones y realice los cambios en función de los requisitos de su empresa:

- Para simplificar, el bucket de AWS Simple Storage Service (Amazon S3) de este ejemplo no tiene habilitado el control de versiones. Evalúe y actualice la configuración según sea necesario.
- Para simplificar, en este ejemplo se configuran los puntos de conexión de la API de REST de Amazon API Gateway sin autenticación, autorización ni limitación. Para uso en producción, recomendamos integrar el sistema con la infraestructura de seguridad empresarial. Evalúe esta configuración y añada la configuración de seguridad necesaria según sea necesario.

- Para este ejemplo de infraestructura de inquilinos, Amazon Simple Notification Service (Amazon SNS) y Amazon Simple Queue Service (Amazon SQS) solo tienen configuraciones mínimas. El AWS Key Management Service (AWS KMS) de cada inquilino permite que los servicios de Amazon CloudWatch y Amazon SNS de la cuenta los consuman según la política de claves de AWS KMS. La configuración es solo un marcador de posición de ejemplo. Ajuste las configuraciones según sea necesario en función de su caso de uso empresarial.
- Toda la configuración, que incluye, entre otros, el aprovisionamiento y la eliminación de los puntos de enlace de la API y los inquilinos de backend mediante AWS CloudFormation, cubre únicamente el caso básico de la ruta feliz. Evalúe y actualice la configuración con la lógica de reintentos necesaria, la lógica adicional de gestión de errores y la lógica de seguridad en función de las necesidades de su empresa.
- En el momento de escribir este artículo, el código de ejemplo se ha probado con up-to-date cdk-nag para comprobar si existen políticas. Es posible que se apliquen nuevas políticas en el futuro. Es posible que estas nuevas políticas requieran que modifique manualmente la pila en función de las recomendaciones antes de poder implementarla. Revise el código existente para asegurarse de que se ajusta a los requisitos de su empresa.
- El código se basa en la CDK de AWS para generar un sufijo al azar en lugar de depender de nombres físicos estáticos asignados a la mayoría de los recursos creados. Esta configuración sirve para garantizar que estos recursos sean únicos y no entren en conflicto con otras pilas. Para obtener más información, consulte la documentación de AWS CDK. Ajústelo en función de los requisitos de su empresa.
- Este código de ejemplo empaqueta artefactos .NET Lambda en imágenes basadas en Docker y se ejecuta con el Tiempo de ejecución de imágenes de contenedor proporcionado por Lambda. El tiempo de ejecución de la imagen del contenedor presenta ventajas como mecanismo estándar de transferencia y almacenamiento (registros de contenedores) y entornos de prueba locales más precisos (a través de la imagen del contenedor). Puede cambiar el proyecto para que utilice los tiempos de ejecución de .NET proporcionados por Lambda para reducir el tiempo de compilación de las imágenes de Docker, pero después tendrá que configurar los mecanismos de transferencia y almacenamiento y asegurarse de que la configuración local coincida con la configuración de Lambda. Ajuste el código para adaptarlo a los requisitos empresariales de los usuarios.

Versiones de producto

- CDK de AWS, versión 2.45.0 o posterior
- Visual Studio 2022

Arquitectura

Pila de tecnología

- Amazon API Gateway
- AWS CloudFormation
- Amazon CloudWatch
- Amazon DynamoDB
- AWS Identity y Access Management (IAM)
- AWS KMS
- AWS Lambda
- Amazon S3
- Amazon SNS
- Amazon SQS

Arquitectura

En el siguiente diagrama se muestra el flujo de creación de la pila de inquilinos. Para obtener más información sobre los paquetes de tecnología del plano de control y del inquilino, consulte la sección de Información adicional.

Flujo de creación de pilas de inquilinos

1. El usuario envía una solicitud de API POST con la carga útil del nuevo inquilino (nombre del inquilino, descripción del inquilino) en JSON a una API de REST alojada en Amazon API Gateway. La API de puerta de enlace procesa la solicitud y la reenvía a la función de Lambda backend de incorporación de inquilinos. En este ejemplo, no hay autorización ni autenticación. En una configuración de producción, esta API debe integrarse con el sistema de seguridad de la infraestructura SaaS.
2. La función de incorporación de inquilinos verifica la solicitud. A continuación, intenta almacenar el registro del inquilino, que incluye el nombre del inquilino, el identificador único universal (UUID) generado y la descripción del inquilino, en la tabla de incorporación de inquilinos de Amazon DynamoDB.
3. Una vez que DynamoDB almacena el registro, una transmisión de DynamoDB inicia la función de infraestructura de inquilinos de Lambda descendente.

4. La función de Lambda de la infraestructura de inquilino actúa en función de la transmisión de DynamoDB recibida. Si la transmisión es para el evento INSERT, la función utiliza la NewImage sección de la transmisión (registro de última actualización, campo Nombre del inquilino) CloudFormation para crear una nueva infraestructura de arrendatario utilizando la plantilla que está almacenada en el bucket de S3. La CloudFormation plantilla requiere el parámetro Tenant Name.
5. AWS CloudFormation crea la infraestructura de inquilinos en función de la CloudFormation plantilla y los parámetros de entrada.
6. Cada configuración de infraestructura arrendataria tiene una CloudWatch alarma, una alarma de facturación y un evento de alarma.
7. El evento de alarma se convierte en un mensaje dirigido a un tema de SNS, que se cifra con la clave de AWS KMS del inquilino.
8. El tema de SNS reenvía el mensaje de alarma recibido a la cola de SQS, que está cifrada por la clave de cifrado AWS KMS del inquilino.

Se pueden integrar otros sistemas con Amazon SQS para realizar acciones basadas en los mensajes en cola. En este ejemplo, para mantener el código genérico, los mensajes entrantes permanecen en cola y es necesario eliminarlos manualmente.

Flujo de eliminación de pilas de inquilinos

1. El usuario envía una solicitud de DELETE API con la carga útil del nuevo inquilino (nombre del inquilino, descripción del inquilino) en JSON a la API de REST alojada por Amazon API Gateway, que procesará la solicitud y la reenviará a la función de incorporación de inquilino. En este ejemplo, no hay autorización ni autenticación. En una configuración de producción, esta API se integrará con el sistema de seguridad de la infraestructura SaaS.
2. La función de incorporación de inquilinos verificará la solicitud y, a continuación, intentará eliminar el registro del inquilino (nombre del inquilino) de la tabla de incorporación de inquilinos.
3. Una vez que DynamoDB elimina el registro correctamente (el registro existe en la tabla y se elimina), una transmisión de DynamoDB inicia la función de infraestructura de inquilinos de Lambda descendente.
4. La función de Lambda de la infraestructura de inquilino actúa en base a la transmisión de DynamoDB recibida. Si la transmisión es para el evento REMOVE, la función utiliza la OldImage sección del registro (información del registro y campo Nombre del inquilino, antes del último cambio, que es eliminar) para iniciar la eliminación de una pila existente en función de la información de ese registro.

5. AWS CloudFormation elimina la pila de inquilinos de destino en función de la entrada.

Tools (Herramientas)

Servicios de AWS

- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket APIs a cualquier escala.
- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- Kit de herramientas de AWS CDK es un kit de desarrollo en la nube de línea de comandos que ayuda a interactuar con la aplicación AWS Cloud Development Kit (AWS CDK).
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.

- AWS Toolkit para Visual Studio es un complemento para el entorno de desarrollo integrado (IDE) de Visual Studio. El Toolkit para Visual Studio permite desarrollar, depurar e implementar aplicaciones .NET que utilizan los servicios de AWS.

Otras herramientas

- Visual Studio es un entorno de desarrollo integrado (IDE) que incluye compiladores, herramientas de finalización de código, diseñadores gráficos y otras características que facilitan el desarrollo de software.

Código

El código de este patrón se encuentra en el repositorio de Incorporación de inquilinos en la arquitectura SaaS para el modelo silo Ejemplo APG.

Epics

Configure AWS CDK

Tarea	Descripción	Habilidades requeridas
Compruebe la instalación de Node.js.	Para comprobar que Node.js esté instalado en su equipo local, ejecute el siguiente comando. `node --version`	Administrador de AWS, AWS DevOps
Instale el kit de herramientas de AWS CDK.	Para instalar el kit de herramientas de AWS CDK en su equipo local, ejecute el siguiente comando. `npm install -g aws-cdk`	Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Si npm no está instalado, puede instalarlo desde el sitio Node.js.	
Compruebe la versión del kit de herramientas de AWS CDK.	Para comprobar que la versión del kit de herramientas de AWS CDK esté instalada correctamente en su equipo, ejecute el siguiente comando. `cdk --version`	Administrador de AWS, AWS DevOps

Revise el código del plano de control de incorporación del inquilino

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Clone el repositorio y navegue hasta la carpeta `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example` . Abra la solución `\src\TenantOnboardingInfra.sln` en Visual Studio 2022. Abra el archivo `TenantOnboardingInfraStack.cs` y revise el código. Los siguientes recursos se crean como parte de esta pila: • Tabla de DynamoDB	Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• Depósito de S3 (cargue la CloudFormation plantilla en el depósito de S3). • Rol de ejecución de Lambda • Función de Lambda • API de API Gateway • Origen de eventos de la función de Lambda	
Revise la CloudFormation plantilla.	En la `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\template` carpeta`infra.yaml` , abra y revise la CloudFormation plantilla. Esta plantilla se completará con el nombre del inquilino obtenido de la tabla de DynamoDB de incorporación de inquilinos. La plantilla proporciona la infraestructura específica para cada inquilino. En este ejemplo, aprovisiona la clave AWS KMS, Amazon SNS, Amazon SQS y la alarma. CloudWatch	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Revise la función de incorporación de inquilinos.	Abra `Function.cs` y revise el código de la función de incorporación de inquilinos, que se crea con la plantilla AWS Lambda Project (.NET Core- C#) de Visual Studio con el esquema .NET 6 (Imagen contenedora). Abra `Dockerfile` y revise el código. `Dockerfile` es un archivo de texto que contiene instrucciones para crear la imagen del contenedor de Lambda. Tenga en cuenta que los siguientes NuGet paquetes se añaden como dependencias al `TenantOnboardingFunction` proyecto: • `Amazon.Lambda.APIGatewayEvents` • `AWSSDK.DynamoDBv2` • `Newtonsoft.Json`	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Revise la InfraProvisioning función Tenant.	Vaya a `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\src\InfraProvisioningFunction` . Abra `Function.cs` y revise el código de la función de aprovisionamiento de la infraestructura inquilina, que se crea con la plantilla AWS Lambda Project (.NET Core-C#) de Visual Studio con el esquema .NET 6 (Imagen contenedora). Abra `Dockerfile` y revise el código. Tenga en cuenta que los siguientes NuGet paquetes se agregan como dependencias al `InfraProvisioningFunction` proyecto: • `Amazon.Lambda.DynamoDBEvents` • `AWSSDK.DynamoDBv2` • `AWSSDK.Cloudformation`	Desarrollador de aplicaciones, AWS DevOps

Implementar recursos de AWS

Tarea	Descripción	Habilidades requeridas
Compilar la solución.	Para crear la solución, siga los pasos que se indican a continuación: 1. Abra la solución `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\src\TenantOnboardingInfra.sln` en Visual Studio 2022. 2. Abra el menú contextual (clic derecho) de la solución y elija Build solution (Compilar solución). **Note** Asegúrese de actualizar el paquete `Amazon.CDK.Lib NuGet` a la última versión del proyecto `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\src\TenantOnboardingInfra`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	antes de crear la solución.	

Inicie el entorno de AWS CDK.	Abra la línea de comandos de Windows y vaya a la carpeta raíz de la aplicación AWS CDK donde está disponibl e el archivo `cdk.json` (`\tenant-onboarding -in-saas-architect ure-for-silo-model -apg-example`). Ejecute el siguiente comando para el arranque.
	`cdk bootstrap`
	Si ha creado un perfil de AWS para las credenciales, utilice el comando con su perfil.
	`cdk bootstrap --profile <profile name>`
		Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas

Enumere las pilas de CDK de AWS.	Para obtener una lista de todas las pilas que se van a crear como parte de este proyecto, ejecute el siguiente comando.
	`cdk ls`
	`cdk ls --profile <profile name>`
	Si ha creado un perfil de AWS para las credenciales, utilice el comando con su perfil.
	`cdk ls --profile <profile name>`
		Administrador de AWS, AWS DevOps

Revise qué recursos de AWS se crearán.	Para revisar todos los recursos de AWS que se crearán como parte de este proyecto, ejecute el siguiente comando.
	`cdk diff`
	Si ha creado un perfil de AWS para las credenciales, utilice el comando con su perfil.
	`cdk diff --profile <profile name>`
		Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas

Implemente todos los recursos de AWS mediante AWS CDK.	Use el siguiente comando para implementar todos los recursos de AWS.
	`cdk deploy --all --require-approval never`
	Si ha creado un perfil de AWS para las credenciales, utilice el comando con su perfil.
	`cdk deploy --all --require-approval never --profile <profile name>`
	Una vez completada la implementación, copie la URL de la API de la sección de resultados de la línea de comandos, como se muestra en el siguiente ejemplo.
	`Outputs: TenantOnboardingInfraStack.TenantOnboardingAPIEndpoint42E526D7 = https://j2qmp8ds21i1i.execute-api.us-west-2.amazonaws.com/prod/`
		Administrador de AWS, AWS DevOps

Verificar la funcionalidad

Tarea	Descripción	Habilidades requeridas

Cree un nuevo inquilino.	Para crear el nuevo inquilino, envíe la siguiente solicitud de curl.
	`curl -X POST <TenantOnboardingAPIEndpoint* from CDK Output>tenant -d '{"Name":"Tenant123", "Description":"Stack for Tenant123"}'`
	Cambie el marcador de posición `<TenantOnboardingAPIEndpoint* from CDK Output>` por el valor real de AWS CDK, como se muestra en el siguiente ejemplo.
	`curl -X POST https://j2qmp8ds21i1i.execute-api.us-west-2.amazonaws.com/prod/tenant -d '{"Name": "Tenant123", "Description":"test12"}'`
	En el siguiente ejemplo, se muestra el resultado.
	`{"message": "A new tenant added - 5/4/2022 7:11:30 AM"}`
		Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Compruebe los detalles del inquilino recién creado en DynamoDB.	Para comprobar los detalles del inquilino recién creado en DynamoDB, siga estos pasos. 1. Abra la consola de administración de AWS y navegue hasta el servicio Amazon DynamoDB. 2. En el menú de navegación de la izquierda, elija Explorar elementos y elija la tabla `Tenant0nboarding` . **Note** El nombre del inquilino irá precedido de `tenantcluster-` . Para obtener más información, consulte la sección Additional information (Información adicional). 3. Compruebe que se ha creado un elemento nuevo con los detalles del inquilino .	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Verifique la creación de la pila para el nuevo inquilino.	Compruebe que la nueva pila se haya creado correctam ente y se haya aprovisionado con la infraestructura para el inquilino recién creado de acuerdo con la CloudForm ation plantilla. 1. Abre la CloudFormation consola. 2. En el menú de navegació n de la izquierda, elija Pilas y compruebe que se haya creado correctamente una pila con el nombre del inquilino. 3. Elija la pila de inquilinos de recién creada y, a continuac ión, elija la pestaña Resources (Recursos). Anote el recurso de alarma y el recurso de Amazon SQS. 4. Abra una nueva terminal con las credenciales de AWS configuradas y apunte a la región correcta. Para activar una alarma de prueba, introduzca el siguiente código, sustituye ndo `<alarm resource name>` por el nombre del recurso de alarma indicado en el paso 3.	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`aws cloudwatch set-alarm-state --alarm-name <alarm resource name> --state-value ALARM --state-reason 'Test setup'`
	
	En el siguiente ejemplo se muestra el código con un nombre de recurso de alarma.
	
	`aws cloudwatch set-alarm-state --alarm-name tenantcluster-tenant123-alarm --state-value ALARM --state-reason 'Test setup'`
	
	5. Abra la consola y vaya a la consola de Amazon SQS. Elija el nombre del recurso de Amazon SQS identificado en el paso 3. Siga las Instrucciones de la documentación de AWS para recibir y eliminar el mensaje de prueba de la alarma que se activó en el paso 4.	

Tarea	Descripción	Habilidades requeridas

Elimine la pila de inquilinos.	Para eliminar la nueva pila de inquilinos, envíe la siguiente solicitud de curl.
	`curl -X DELETE <TenantOnboardingAPIEndpoint* from CDK Output>tenant/<Tenant Name from previous step>`
	Cambie el marcador de posición `<TenantOnboardingAPIEndpoint* from CDK Output>` por el valor real de AWS CDK y cambie `<Tenant Name from previous step>` por el valor real del paso anterior de creación del inquilino , como se muestra en el siguiente ejemplo.
	`curl -X DELETE https://j2qmp8ds21i1i.execute-api.us-west-2.amazonaws.com/prod/tenant/Tenant123`
	En el siguiente ejemplo, se muestra el resultado.
	`{"message": "Tenant destroyed - 5/4/2022 7:14:48 AM"}`
		Desarrollador de aplicaciones, AWS DevOps, administrador de AWS

Tarea	Descripción	Habilidades requeridas
Verifique la eliminación de la pila para el inquilino existente.	Para comprobar que se ha eliminado la pila de inquilinos existente, siga estos pasos: 1. Abra la consola y navegue hasta CloudFormation ella. 2. En el panel de navegación de la izquierda, compruebe que la pila existente con el nombre del inquilino ya no esté en la CloudForm ation consola (si la consola está configurada para mostrar solo las pilas activas) o que esté en proceso de borrarse. Si la pila ya no está en la CloudFormation consola, usa la lista desplegable para cambiar la configura ción de la consola de Activa a Eliminada para ver la pila eliminada y comprobar que la pila se ha eliminado correctamente.	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Limpieza

Tarea	Descripción	Habilidades requeridas
Destruya el entorno.	Antes de limpiar la pila, asegúrese de lo siguiente:	Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• Todos los registros de DynamoDB se han eliminado mediante la operación de eliminación de inquilinos anterior o mediante la consola o la API de DynamoDB. Cada vez que se elimine un registro de inquilino, se iniciará la limpieza de su CloudFormation homólogo de AWS. • Todas las CloudFormation pilas de AWS basadas en inquilinos se limpian (en caso de que falle la lógica de limpieza del activador de DynamoDB) en la consola de AWS. CloudFormation Una vez finalizadas las pruebas, se puede usar AWS CDK para destruir todas las pilas y los recursos relacionados mediante la ejecución del siguiente comando. `cdk destroy --all;` Si ha creado un perfil de AWS para las credenciales, utilice el perfil.	

Tarea	Descripción	Habilidades requeridas
	Confirme la solicitud de eliminación de la pila para eliminarla.	
Limpia Amazon CloudWatch Logs.	El proceso de eliminación de la pila no limpiará CloudWatch los registros (grupos de registros y registros) generados por la pila. Limpie los CloudWatch recursos manualmente mediante la CloudWatch consola o la API.	Desarrollador de aplicaciones, AWS DevOps, administrador de AWS

Recursos relacionados

- Taller sobre AWS CDK .NET
- Utilización de AWS CDK en C#
- Referencia de CDK .NET

Información adicional

Conjunto de tecnologías de plano de control

El código CDK escrito en .NET se utiliza para aprovisionar la infraestructura del plano de control, que consta de los siguientes recursos:

1. API Gateway

   Sirve como punto de entrada de la API de REST para la pila del plano de control.

2. Función de Lambda de incorporación de inquilinos

   La puerta de enlace de API inicia esta función de Lambda mediante el método m.

   Una solicitud de API del método POST hace que (`tenant name`, `tenant description`) se inserte en la tabla de DynamoDB `Tenant Onboarding`.

En este ejemplo de código, el nombre del inquilino también se usa como parte del nombre de la pila de inquilinos y de los nombres de los recursos de esa pila. Esto es para facilitar la identificación de estos recursos. El nombre de este inquilino debe ser único en la configuración para evitar conflictos o errores. La configuración detallada de la validación de entradas se explica en la documentación sobre los roles de IAM y en la sección de Limitations (Limitaciones).

El proceso de persistencia en la tabla de DynamoDB solo tendrá éxito si el nombre del inquilino no se utiliza en ningún otro registro de la tabla.

En este caso, el nombre del inquilino es la clave de partición de esta tabla, ya que solo la clave de partición se puede usar como expresión de condición `PutItem`.

Si el nombre del inquilino nunca se registró antes, el registro se guardará correctamente en la tabla.

Sin embargo, si un registro existente de la tabla ya utiliza el nombre del inquilino, la operación fallará e iniciará una excepción de DynamoDB `ConditionalCheckFailedException`. La excepción se utilizará para devolver un mensaje de error (`HTTP BadRequest`) que indique que el nombre del inquilino ya existe.

Una solicitud de API de método `DELETE` eliminará el registro de un nombre de inquilino específico de la tabla `Tenant Onboardin`.

La eliminación del registro de DynamoDB en este ejemplo se realizará correctamente aunque el registro no exista.

Si el registro de destino existe y se elimina, se creará un registro de transmisión de DynamoDB. De lo contrario, no se creará ningún registro posterior.

3. Incorporación de DynamoDB por parte del inquilino, con Amazon DynamoDB Streams habilitado

   Esto registra la información de los metadatos del inquilino y cualquier registro que se guarde o elimine enviará un flujo descendente a la función de Lambda `Tenant Infrastructure`.

4. Función de Lambda de infraestructura inquilina

   Esta función de Lambda la inicia el registro de flujo de DynamoDB del paso anterior. Si el registro corresponde a un `INSERT` evento, invoca CloudFormation a AWS para crear una nueva infraestructura de inquilinos con la CloudFormation plantilla almacenada en un bucket de S3. Si

el registro es para `REMOVE`, se inicia la eliminación de una pila existente en función del campo del registro de transmisión `Tenant Name`.

5. Bucket de S3

   Esto sirve para almacenar la CloudFormation plantilla.

6. Funciones de IAM para cada función de Lambda y una función de servicio para CloudFormation

   Cada función de Lambda tiene su rol de IAM único con permisos de privilegio mínimo para realizar su tarea. Por ejemplo, la función `Tenant On-boarding` Lambda tiene read/write acceso a DynamoDB y la función `Tenant Infrastructure` Lambda solo puede leer el flujo de DynamoDB.

   Se crea un rol de CloudFormation servicio personalizado para el aprovisionamiento de la pila de inquilinos. Esta función de servicio contiene permisos adicionales para el aprovisionamiento de CloudFormation pilas (por ejemplo, la clave de AWS KMS). Esto divide las funciones entre Lambda y CloudFormation evita todos los permisos en una sola función (función de Infraestructura Lambda).

   Los permisos que permiten realizar acciones poderosas (como crear y eliminar CloudFormation pilas) están bloqueados y solo se permiten en los recursos que comienzan con. `tenantcluster-` La excepción es AWS KMS, debido a su convención de nomenclatura de recursos. El nombre del inquilino introducido por la API irá precedido de `tenantcluster-` así como otras comprobaciones de validación (alfanuméricas solo con guiones y limitadas a menos de 30 caracteres para que quepan en la mayoría de los nombres de los recursos de AWS). Esto garantiza que el nombre del inquilino no provoque una interrupción accidental de los recursos o las pilas de la infraestructura principal.

Pila de tecnología para inquilinos

La CloudFormation plantilla se almacena en el depósito de S3. La plantilla proporciona la clave de AWS KMS específica del inquilino, una CloudWatch alarma, un tema de SNS, una cola de SQS y una política de SQS.

Amazon SNS y Amazon SQS utilizan la clave de AWS KMS para el cifrado de datos de sus mensajes. Las prácticas de seguridad para AwsSolutions(SNS2 y AwsSolutions) SQS2 recomiendan configurar Amazon SNS y Amazon SQS con cifrado. Sin embargo, CloudWatch las alarmas no funcionan con Amazon SNS cuando se utiliza una clave gestionada por AWS, por lo que debe utilizar

una clave gestionada por el cliente en este caso. Para obtener más información, consulte el Centro de conocimientos de AWS.

La política de SQS se utiliza en la cola de Amazon SQS para permitir que el tema de SNS creado entregue el mensaje a la cola. Sin la política SQS, se denegará el acceso. Para obtener más información, consulte la documentación de Amazon SNS.

Descomponga monolitos en microservicios mediante CQRS y abastecimiento de eventos

Rodolfo Jr. Cerrada, Dmitry Gulin y Tabby Ward, Amazon Web Services

Resumen

Este patrón combina dos patrones y emplea tanto el patrón de división de responsabilidad por consultas de comandos (CQRS) como el patrón de abastecimiento de eventos. El patrón CQRS divide las responsabilidades de los modelos de comando y consulta. El patrón de abastecimiento de eventos aprovecha la comunicación asincrónica basada en eventos para mejorar la experiencia general del usuario.

Puede usar servicios de CQRS y Amazon Web Services (AWS) para mantener y escalar cada modelo de datos de forma independiente y, al mismo tiempo, refactorizar su aplicación monolítica en una arquitectura de microservicios. Después, puede usar el patrón de abastecimiento de eventos para sincronizar los datos de la base de datos de comandos con la base de datos de consultas.

Este patrón emplea un código de ejemplo que incluye un archivo de solución (*.sln) que puede abrir con la versión más reciente de Visual Studio. El ejemplo contiene el código de la API Reward para mostrar el funcionamiento de CQRS y el abastecimiento de eventos en aplicaciones de AWS sin servidor y aplicaciones tradicionales o en las instalaciones.

Para obtener más información sobre CQRS y el abastecimiento de eventos, consulte la sección de Información adicional.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Amazon CloudWatch
- Tablas de Amazon DynamoDB
- Amazon DynamoDB Streams
- Clave de acceso y clave secreta de AWS Identity and Access Management (IAM); para obtener más información, consulte el video de la sección de Recursos relacionados
- AWS Lambda
- Familiaridad con Visual Studio

- Familiaridad con el kit de herramientas de AWS para Visual Studio; para obtener más información, consulte el video de demostración del Kit de herramientas de AWS para Visual Studio en la sección de Recursos relacionados

Versiones de producto

- Microsoft Visual Studio 2019 Community Edition.
- AWS Toolkit para Visual Studio 2019.
- .NET Core 3.1. Este componente es una opción de la instalación de Visual Studio. Para incluir .NET Core durante la instalación, seleccione desarrollo multiplataforma de NET Core.

Limitaciones

- El código de ejemplo de aplicación tradicional en las instalaciones (ASP.NET Core Web API y objetos de acceso a datos) no incluye base de datos. Sin embargo, incluye el objeto en memoria `CustomerData`, que actúa como base de datos simulada. El código proporcionado es suficiente para probar el patrón.

Arquitectura

Pila de tecnología de origen

- Proyecto ASP.NET Core Web API
- Servidor web IIS
- Objeto de acceso a datos
- Modelo CRUD

Arquitectura de origen

En la arquitectura de origen, el modelo CRUD contiene interfaces de comandos y consultas en una sola aplicación. Para ver un código de ejemplo, consulte `CustomerDA0.cs` (adjunto).

Pila de tecnología de destino

- Amazon DynamoDB

- Amazon DynamoDB Streams
- AWS Lambda
- (Opcional) Amazon API Gateway
- (Opcional) Amazon Simple Notification Service (Amazon SNS)

Arquitectura de destino

En la arquitectura de destino, las interfaces de comando y consulta están separadas. La arquitectura que se muestra en el siguiente diagrama se puede ampliar con puerta de enlace API y Amazon SNS. Para obtener más información, consulte la sección Información adicional.

1. Las funciones de comandos de Lambda realizan operaciones de escritura, como crear, actualizar o eliminar, en la base de datos.
2. Las funciones de consulta de Lambda realizan operaciones de lectura, como obtener o seleccionar, en la base de datos.
3. Esta función de Lambda procesa los flujos de DynamoDB de la base de datos de comandos y actualiza la base de datos de consultas con los cambios.

Tools (Herramientas)

Herramientas

- Amazon DynamoDB: Amazon DynamoDB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido y predecible, así como una perfecta escalabilidad.
- Amazon DynamoDB Streams: DynamoDB Streams captura una secuencia en orden cronológico de las modificaciones de los elementos en una tabla de DynamoDB. Este servicio posteriormente almacena esta información en un registro durante un máximo de 24 horas. El cifrado en reposo cifra los datos en DynamoDB streams.
- AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.

- La consola de administración de AWS: la consola de administración de AWS es una aplicación web que engloba y hace referencia a un amplio conjunto de consolas de servicios para la administración de recursos de AWS.
- Visual Studio 2019 Community Edition: Visual Studio 2019 es un entorno de desarrollo integrado (IDE). La Community Edition es gratuita para colaboradores de código abierto. En este patrón usará Visual Studio 2019 Community Edition para abrir, compilar y ejecutar código de ejemplo. Solo con fines de visualización, puede usar cualquier editor de texto o Visual Studio Code.
- AWS Toolkit para Visual Studio: el AWS Toolkit para Visual Studio es un complemento para el IDE de Visual Studio. El AWS Toolkit para Visual Studio facilita el desarrollo, la depuración y la implementación de aplicaciones .NET que utilizan servicios de AWS.

Código

Se adjunta el código de ejemplo. Para obtener más instrucciones sobre cómo implementar el código de ejemplo, consulta la sección Epics.

Epics

Abra y cree la solución

Tarea	Descripción	Habilidades requeridas
Abra la solución.	1. Descargue el código fuente de ejemplo (`CQRS-ES Code.zip`) de la sección de Adjuntos y extraiga los archivos. 2. En el IDE de Visual Studio, seleccione Archivo, Abrir, Solución de proyecto, y navegue hasta la carpeta en la que extrajo el código fuente. 3. Seleccione AWS.APG.CQRSES.sln y seleccione	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	Abrir. La solución completa se carga en Visual Studio.	
Cree la solución.	Abra el menú contextual (clic derecho) de la solución y elija Compilar solución. Esto generará y compilará todos los proyectos de la solución. La compilación debería realizarse correctamente. Visual Studio Solution Explorer mostrará la estructura de directorios. • `CQRS On-Premises Code Sample` contiene un ejemplo del uso de CQRS en las instalaciones. • `CQRS AWS Serverless` contiene todo el código de ejemplo de CQRS y de abastecimiento de eventos mediante servicios sin servidor de AWS.	Desarrollador de aplicaciones

Cree tablas de DynamoDB

Tarea	Descripción	Habilidades requeridas
Proporcionar credenciales.	Si aún no tiene una clave de acceso, consulte el video de la sección de Recursos relacionados.	Desarrollador de aplicaciones, ingeniero de datos, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	1. En Solution Explorer, expanda CQRS AWS Serverless y, a continuación, expanda la carpeta Compilar solución. 2. Expanda el proyecto AwS.APG.CQRSES.Build y visualice el archivo `Program.cs` . 3. Desplácese hasta la parte superior de `Program.cs` y busque `Program()` . 4. Sustituya `YOUR ACCESS KEY` por su clave de acceso a la cuenta y sustituya `YOUR SECRET KEY` por la clave secreta de la cuenta. Tenga en cuenta que, en un entorno de producción, no debería codificar sus claves de forma rígida. En su lugar, puede usar AWS Secrets Manager para almacenar y recuperar las credenciales.	
Compilar el proyecto.	Para compilar el proyecto, abra el menú contextual (clic derecho) del proyecto AwS.APG.CQRSES.Build y seleccione Compilar.	Desarrollador de aplicaciones, ingeniero de datos, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree y rellene las tablas.	Para compilar las tablas y rellenarlas con datos iniciales , abra el menú contextual (clic derecho) del proyecto AwS.APG.CQRSES.Build y seleccione Depurar, Iniciar nueva instancia.	Desarrollador de aplicaciones, ingeniero de datos, administr ador de base de datos
Verifique la construcción de la tabla y los datos.	Para comprobarlo, acceda al Explorador de AWS y expanda Amazon DynamoDB. Se mostrarán las tablas. Abra cada tabla para mostrar los datos de ejemplo.	Desarrollador de aplicaciones, ingeniero de datos, administr ador de base de datos

Ejecute pruebas locales

Tarea	Descripción	Habilidades requeridas
Crear el proyecto CQRS.	1. Abra la solución y vaya a la carpeta de Services/CQRS/ Tests soluciones AWS de CQRS. 2. En el archivo AWS.APG.C QRSES. CQRSLambd a.Tests del proyecto, abra BaseFunctionTest.cs y sustituya AccessKeyy SecretKeypor las claves de IAM que haya creado. 3. Guarde los cambios. 4. Para compilar y crear el proyecto de prueba, abra el menú contextual (clic	Desarrollador de aplicaciones, ingeniero de pruebas

Tarea	Descripción	Habilidades requeridas
	derecho) del proyecto y seleccione Crear.	
Cree el proyecto de abastecimiento de eventos.	1. Navegue hasta la carpeta de soluciones AWS Services/Event Source/Tests de CQRS. 2. En AWS.APG.CQRSES.EventSourceLambda.Tests del proyecto, abra BaseFunctionTest.cs y sustituya AccessKeyy SecretKeypor las claves de IAM que haya creado. 3. Guarde los cambios. 4. Para compilar y crear el proyecto de prueba, abra el menú contextual (clic derecho) del proyecto y seleccione Crear.	Desarrollador de aplicaciones, ingeniero de pruebas
Ejecutar las pruebas.	Para ejecutar todas las pruebas, seleccione Ver, Explorador de pruebas y, a continuación, seleccione Ejecutar todas las pruebas a la vista. Todas las pruebas resultarán correctas. El sistema lo indicará con un icono de marca de verificación verde.	Desarrollador de aplicaciones, ingeniero de pruebas

Publique las funciones de Lambda de CQRS en AWS

Tarea	Descripción	Habilidades requeridas
Publica la primera función de Lambda.	1. En el Explorador de soluciones, abra el menú contextual (haga clic con el botón derecho) del AWS.APG.CQRSES. CommandCreateLambd a proyecto y, a continuac ión, elija Publicar en AWS Lambda. 2. Seleccione el perfil que desee usar, la región de AWS en la que desee implementar la función de Lambda y el nombre de la función. 3. Para los campos restantes , mantenga los valores predeterminados y seleccione Next (Siguiente). 4. En la lista desplegable del nombre del rol, seleccione. AWSLambdaFullAccess 5. Para proporcionar las claves de su cuenta, seleccione Agregar e introdúzca `AcessKey` como variable y su clave de acceso como valor. A continuación, vuelva a seleccionar Agregar, introduzca `SecretKey`	Desarrollador de aplicaciones, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	como variable y su clave secreta como valor. 6. Para los campos restantes , mantenga los valores predeterminados y seleccione Upload (Cargar). Una vez cargada la función de prueba de Lambda, aparecerá automáticamente en Visual Studio. 7. Repita los pasos 1 a 6 para los siguientes proyectos: • AWS.APG.CARSES. CommandDeleteLambda • AWS.APG.CARSES. CommandUpdateLambda • AWS.APG.CARSES. CommandAddRewardLa mbda • AWS.APG.CARSES. CommandRedeemRewar dLambda • AWS.APG.CARSES. QueryCustomerListL ambda • AWS.APG.CARSES. QueryRewqardLambda	

Tarea	Descripción	Habilidades requeridas
Verifique la carga de la función.	(Opcional) Para comprobar que la función se ha cargado correctamente, acceda al Explorador de AWS y expanda AWS Lambda. Para abrir la ventana de prueba, seleccione la función de Lambda (doble clic).	Desarrollador de aplicaciones, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Pruebe la función de Lambda.	1. Introduzca los datos de la solicitud o copie los datos de la solicitud de ejemplo Datos de prueba, en la sección Información adicional. Asegúrese de seleccionar los datos correctos para la función que está probando. 2. Para ejecutar la prueba, elija Invoke (Invocar). La respuesta y cualquier error se muestran en el cuadro de texto Respuesta, y los registros se muestran en el cuadro de texto Registros o en CloudWatch Registros. 3. Para verificar los datos, en el Explorador de AWS, seleccione la tabla de DynamoDB (doble clic). Todos los proyectos Lambda de CQRS se encuentran en las carpetas de soluciones `CQRS AWS Serverless\CQRS\Command Microservice` y `CQRS AWS Serverless\CQRS\Command Microservice`. Para ver el directorio de soluciones y los proyectos, consulte el Directorio de	Desarrollador de aplicaciones, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	códigos fuente en la sección de Información adicional.	
Publique las funciones restantes.	Repita los pasos previos para los siguientes proyectos: • AWS.APG.CARSES.CommandDeleteLambda • AWS.APG.CARSES.CommandUpdateLambda • AWS.APG.CARSES.CommandAddRewardLambda • AWS.APG.CARSES.CommandRedeemRewardLambda • AWS.APG.CARSES.QueryCustomerListLambda • AWS.APG.CARSES.QueryRewqardLambda	Desarrollador de aplicaciones, DevOps ingeniero

Configure la función de Lambda como oyente de eventos

Tarea	Descripción	Habilidades requeridas
Publique los controladores de eventos Customer y Reward Lambda.	Para publicar cada controlador de eventos, siga los pasos de la épica anterior. Los proyectos se encuentran en las carpetas de soluciones `CQRS AWS Serverless\Event Source\Customer Event` y `CQRS`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`AWS Serverless\Event Source\Reward Event` . Para obtener más información, consulte Directorio de código fuente en la sección Información adicional.	

Tarea	Descripción	Habilidades requeridas
Adjunte el oyente de Lambda detector de eventos.	1. Inicie sesión en la consola de administración de AWS con la misma cuenta que usó para publicar los proyectos de Lambda. 2. En Región, seleccione US East 1 o la región en la que implementó las funciones de Lambda en la épica anterior. 3. Navegue hasta el servicio Lambda. 4. Seleccione el `EventSourceCustomer` función de Lambda. 5. Elija Add trigger (Añadir disparador). 6. En la lista desplegable Configuración de desencadenante, seleccione DynamoDB. 7. En la lista desplegable de tablas de DynamoDB, seleccione. cqrses-customer-cmd 8. En la lista desplegable Posición inicial, seleccione Recortar horizonte desde. Recortar el horizonte significa que el desencadenante de DynamoDB empezará a leer en el último registro de transmisi	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	ón (sin recortar), que es el registro más antiguo del fragmento. 9. Seleccione la casilla Enable trigger (Habilitar disparador). 10. Deje los valores predeterminados en los demás campos y seleccione Add (Agregar). Una vez que el oyente se haya adjuntado correctamente a la tabla de DynamoDB, se mostrará en la página del diseñador de Lambda.	
Publique y adjunte la EventSourceReward función Lambda.	Para publicar y adjuntar la función `EventSourceReward` Lambda, repita los pasos de las dos historias anteriores y selecciónela en la lista desplegable cqrses-reward-cmdde tablas de DynamoDB.	Desarrollador de aplicaciones

Pruebe y valide los flujos de DynamoDB y el desencadenante de Lambda

Tarea	Descripción	Habilidades requeridas
Pruebe la transmisión y el desencadenante de Lambda.	1. En Visual Studio, acceda al Explorador de AWS. 2. Amplíe AWS Lambda y elija la CommandRedeemRewar	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	dfunción (haga doble clic). Se abrirá una ventana de funciones en la que podrá probar la función. 3. En el cuadro de texto de la solicitud, introduzca los datos de la solicitud en formato de notación de JavaScript objetos (JSON). Para ver un ejemplo de solicitud, consulte Datos de prueba en la sección Información adicional. 4. Elija Invocación de .	
Valide usando la tabla de consultas de recompensas de DynamodDB.	1. Abre la cqrses-reward-queryytabla. 2. Compruebe los puntos del cliente que canjeó la recompensa. Los puntos canjeados deben restarse del total de puntos agregados del cliente.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Valide mediante CloudWatch registros.	1. Navegue hasta los grupos de registros CloudWatch y selecciónelos. 2. El grupo de aws/lambda/EventSourceReward registros/contiene los registros del `EventSourceReward` desencadenador. Se registrarán todas las llamadas de Lambda, incluidos los mensajes que ha incluido en `context.Logger.LogLine` y `Console.Writeline` dentro del código de Lambda.	Desarrollador de aplicaciones
Valide el EventSourceCustomer disparador.	Para validar el `EventSourceCustomer` disparador, repite los pasos de esta epopeya utilizando la tabla de clientes y los CloudWatch registros respectivos del `EventSourceCustomer` disparador.	Desarrollador de aplicaciones

Recursos relacionados

Referencias

- Descargas de Visual Studio 2019 Community Edition
- Descargar AWS Toolkit para Visual Studio
- Guía del usuario de AWS Toolkit para Visual Studio
- Sin servidor en AWS

- Casos de uso y patrones de diseño de DynamoDB
- CQRS Martin Fowler
- Aprovisionamiento de eventos Martin Fowler

Videos

- Demo de AWS Toolkit para Visual Studio
- ¿Cómo creo una ID de clave de acceso para un nuevo usuario de IAM?

Información adicional

CQRS y abastecimiento de eventos

CQRS

El patrón CQRS separa un único modelo de operaciones conceptual, como un modelo CRUD (creación, lectura, actualización, eliminación) único de objetos de acceso a datos, en modelos de operaciones de comando y consulta. El modelo de comandos hace referencia a cualquier operación, como crear, actualizar o eliminar, que cambia el estado. El modelo de consulta hace referencia a cualquier operación que devuelva un valor.

1. El modelo CRUD del cliente incluye las siguientes interfaces:
   - `Create Customer()`
   - `UpdateCustomer()`
   - `DeleteCustomer()`
   - `AddPoints()`
   - `RedeemPoints()`
   - `GetVIPCustomers()`
   - `GetCustomerList()`
   - `GetCustomerPoints()`

Cuando sus necesidades sean más complejas, podrá superar este enfoque de modelo único. El CQRS emplea un modelo de comandos y un modelo de consulta para separar las responsabilidades de escribir y leer los datos. De esta forma, los datos se pueden mantener y gestionar de forma

independiente. Con una clara separación de responsabilidades, las mejoras de cada modelo no afectan al otro. Esta separación mejora el mantenimiento y el rendimiento, y reduce la complejidad de la aplicación a medida que crece.

1. Interfaces en el modelo de comandos del cliente:
   - `Create Customer()`
   - `UpdateCustomer()`
   - `DeleteCustomer()`
   - `AddPoints()`
   - `RedeemPoints()`
2. Interfaces en el modelo de consultas del cliente:
   - `GetVIPCustomers()`
   - `GetCustomerList()`
   - `GetCustomerPoints()`
   - `GetMonthlyStatement()`

Para ver código de ejemplo, consulte el Directorio de códigos fuente.

A continuación, el patrón CQRS desacopla la base de datos. Esta disociación posibilita la independencia total de cada servicio, que es el ingrediente principal de la arquitectura de microservicios.

Al usar CQRS en la nube de AWS, puede optimizar aún más cada servicio. Por ejemplo, puede establecer diferentes configuraciones informáticas, o elegir entre un microservicio sin servidor o uno basado en contenedores. Puedes sustituir el almacenamiento en caché local por Amazon. ElastiCache Si tiene una publish/subscribe mensajería local, puede sustituirla por Amazon Simple Notification Service (Amazon SNS). Además, puede aprovechar los pay-as-you-go precios y la amplia gama de servicios de AWS, que solo paga por lo que utiliza.

CQRS ofrece los siguientes beneficios:

- Escalado independiente: la estrategia de escalado de cada modelo se puede adaptar para satisfacer los requisitos y la demanda del servicio. Al igual que en las aplicaciones de alto

rendimiento, separar la lectura y la escritura permite escalar el modelo de forma independiente para satisfacer cada demanda. También puede agregar o reducir recursos de cómputo para satisfacer la demanda de escalabilidad de un modelo sin afectar al otro.

- Mantenimiento independiente: la separación de los modelos de consulta y comando mejora la capacidad de mantenimiento de los modelos. Puede realizar cambios en el código y mejoras en un modelo sin que ello afecte al otro.
- Seguridad: es más fácil aplicar los permisos y las políticas a modelos separados para lectura y escritura.
- Lecturas optimizadas: puede definir un esquema optimizado para las consultas. Por ejemplo, puede definir un esquema para datos agregados y un esquema independiente para tablas de hechos.
- Integración: CQRS se adapta bien a los modelos de programación basados en eventos.
- Complejidad gestionada: la separación en modelos de consulta y comando es adecuada para dominios complejos.

Al utilizar CQRS, tenga en cuenta lo siguiente:

- El patrón de CQRS se aplica solo a una parte específica de una aplicación, y no a su conjunto. La implementación en un dominio inadecuado para el patrón puede reducir la productividad, aumentar el riesgo e introducir complejidad.
- El patrón funciona mejor en modelos de uso frecuente que presentan un desequilibrio en las operaciones de lectura y escritura.
- En el caso de aplicaciones de lectura intensiva, como informes de gran tamaño que tardan en procesarse, CQRS le ofrece la opción de seleccionar la base de datos adecuada y crear un esquema para almacenar los datos agregados. Esto mejora el tiempo de respuesta en la lectura y visualización del informe, ya que procesa los datos del informe solo una vez y los coloca en la tabla agregada.
- En el caso de las aplicaciones de escritura intensiva, puede configurar la base de datos para operaciones de escritura y permitir que el microservicio de comandos se escale de forma independiente cuando aumente la demanda de escritura. Para ver ejemplos, consulte los microservicios `AWS.APG.CQRSES.CommandRedeemRewardLambda` y `AWS.APG.CQRSES.CommandAddRewardLambda`.

Aprovisionamiento de eventos

El siguiente paso consiste en usar el abastecimiento de eventos para sincronizar la base de datos de consultas cuando se ejecuta un comando. Por ejemplo, considere los siguientes eventos:

- Al añadir un punto de recompensa, es necesario actualizar sus puntos de recompensa totales o agregados en la base de datos de consultas.
- El apellido del cliente se actualiza en la base de datos de comandos, y es necesario actualizar la información del cliente en la base de datos de consultas.

En un modelo CRUD tradicional, se garantiza la coherencia de los datos al bloquearlos hasta que finalice la transacción. En el abastecimiento de eventos, los datos se sincronizan publicando una serie de eventos que el suscriptor utilizará para actualizar sus datos respectivos.

El patrón de abastecimiento de eventos garantiza y registra una serie completa de acciones realizadas con los datos, y las publica a través de una secuencia de eventos. Estos eventos representan un conjunto de cambios en los datos que los suscriptores de ese evento deben procesar para mantener su registro actualizado. El suscriptor consume estos eventos y sincroniza los datos en la base de datos del suscriptor. En este caso, es la base de datos de consultas.

El siguiente diagrama muestra el abastecimiento de eventos con CQRS en AWS.

1. Las funciones de comandos de Lambda realizan operaciones de escritura, como crear, actualizar o eliminar, en la base de datos.
2. Las funciones de consulta de Lambda realizan operaciones de lectura, como obtener o seleccionar, en la base de datos.
3. Esta función de Lambda procesa los flujos de DynamoDB de la base de datos de comandos y actualiza la base de datos de consultas con los cambios. También puede usar esta función para publicar un mensaje en Amazon SNS y que los suscriptores puedan procesar los datos.
4. (Opcional) El suscriptor del evento de Lambda procesa el mensaje publicado por Amazon SNS y actualiza la base de datos de consultas.
5. (Opcional) Amazon SNS envía una notificación por correo electrónico de la operación de escritura.

En AWS, DynamoDB Streams puede sincronizar la base de datos de consultas. DynamoDB captura una secuencia en orden cronológico de las modificaciones de los elementos en la tabla de DynamoDB en tiempo casi real y almacena la información de forma duradera en un plazo máximo de 24 horas.

La activación de DynamoDB Streams permite a la base de datos publicar una secuencia de eventos que posibilita el patrón de abastecimiento de eventos. El patrón de abastecimiento de eventos añade al suscriptor del evento. La aplicación del suscriptor del evento consume el evento y lo procesa en función de la responsabilidad del suscriptor. En el diagrama anterior, el suscriptor del evento envía los cambios a la base de datos de Query DynamoDB para mantener los datos sincronizados. El uso de Amazon SNS, el agente de mensajes y la aplicación de suscripción de eventos mantiene la arquitectura desacoplada.

El abastecimiento de eventos ofrece los siguientes beneficios:

- Coherencia de los datos transaccionales
- Un registro de auditoría fiable y un historial de las acciones que permite supervisar las medidas adoptadas en los datos
- Las aplicaciones distribuidas, como los microservicios, pueden sincronizar sus datos en todo el entorno
- Publicación fiable de los eventos siempre que cambie el estado
- Reconstrucción o reproducción de estados anteriores
- Entidades con acoplamiento flexible que intercambian eventos para migrar de una aplicación monolítica a microservicios
- Reducción de los conflictos causados por actualizaciones simultáneas; el abastecimiento de eventos evita la necesidad de actualizar los objetos directamente en el almacén de datos
- Flexibilidad y extensibilidad, ya que la tarea se desvincula del evento
- Actualizaciones externas del sistema
- Gestión de múltiples tareas en un solo evento

Cuando use abastecimiento de eventos, tenga en cuenta los siguientes puntos:

- Como existe cierto retardo en la actualización de los datos entre las bases de datos de suscriptor de origen, la única forma de deshacer un cambio es añadir un evento de compensación al almacén de eventos.
- La implementación del abastecimiento de eventos tiene cierta curva de aprendizaje, ya que su estilo de programación es diferente.

Datos de prueba

Use los siguientes datos de prueba para probar la función de Lambda tras una implementación correcta.

CommandCreate Cliente

```
{  "Id":1501,  "Firstname":"John",  "Lastname":"Done",  "CompanyName":"AnyCompany",
 "Address": "USA",  "VIP":true }
```

CommandUpdate Cliente

```
{  "Id":1501,  "Firstname":"John",  "Lastname":"Doe",  "CompanyName":"Example Corp.",
 "Address": "Seattle, USA",  "VIP":true }
```

CommandDelete Cliente

Introduzca la ID del cliente como dato de solicitud. Por ejemplo, si la ID de cliente es 151, introduzca 151 como dato de solicitud.

```
151
```

QueryCustomerList

Está en blanco. Cuando se invoca, devuelve a todos los clientes.

CommandAddReward

Añade 40 puntos al cliente con la ID 1 (Richard).

```
{
  "Id":10101,
  "CustomerId":1,
  "Points":40
}
```

CommandRedeemReward

Esto reducirá 15 puntos al cliente con la ID 1 (Richard).

```
{
  "Id":10110,
  "CustomerId":1,
```

```
  "Points":15
}
```

QueryReward

Introduzca la ID del cliente. Por ejemplo, introduzca 1 para Richard, 2 para Arnav y 3 para Shirley.

```
2
```

Directorio de códigos fuente

Use la siguiente tabla como guía de estructura de directorios de la solución de Visual Studio.

Ejemplo de código de muestra de directorio CQRS en las instalaciones

Modelo CRUD de cliente

Proyecto CQRS On-Premises Code Sample\CRUD Model\AWS.APG.CQRSES.DAL

Versión CQRS del modelo CRUD del cliente

- Comando del cliente: proyecto `CQRS On-Premises Code Sample\CQRS Model\Command Microservice\AWS.APG.CQRSES.Command`
- Consulta del cliente: proyecto `CQRS On-Premises Code Sample\CQRS Model\Query Microservice\AWS.APG.CQRSES.Query`

Microservicios de comando y consulta

El microservicio de comandos se encuentra en la carpeta de soluciones `CQRS On-Premises Code Sample\CQRS Model\Command Microservice`:

- El proyecto de API ASP.NET Core `AWS.APG.CQRSES.CommandMicroservice` actúa como punto de entrada desde el que los consumidores interactúan con el servicio.
- El proyecto .NET Core `AWS.APG.CQRSES.Command` es un objeto que aloja objetos e interfaces relacionados con comandos.

El microservicio de consultas se encuentra en la carpeta de soluciones `CQRS On-Premises Code Sample\CQRS Model\Query Microservice`:

- El proyecto de API ASP.NET Core `AWS.APG.CQRSES.QueryMicroservice` actúa como punto de entrada desde el que los consumidores interactúan con el servicio.
- El proyecto .NET Core `AWS.APG.CQRSES.Query` es un objeto que aloja objetos e interfaces relacionados con consultas.

Directorio de soluciones de código CQRS AWS sin servidor

Este código es la versión de AWS del código en las instalaciones que emplea los servicios sin servidor de AWS.

En C# .NET Core, cada función de Lambda está representada por un proyecto .NET Core. En el código de ejemplo de este patrón, hay un proyecto independiente para cada interfaz en los modelos de comandos y consultas.

Uso de los servicios de AWS por CQRS

Puede encontrar el directorio raíz de soluciones para CQRS con servicios sin servidor de AWS en la carpeta `CQRS AWS Serverless\CQRS`. El ejemplo incluye dos modelos: Customer y Reward.

El comando de funciones de Lambda para Customer y Reward se encuentra en las carpetas `CQRS \Command Microservice\Customer` y `CQRS\Command Microservice\Reward`. Contienen los siguientes proyectos de Lambda:

- Comando Customer: `CommandCreateLambda`, `CommandDeleteLambda` y `CommandUpdateLambda`
- Comando Reward: `CommandAddRewardLambda` y `CommandRedeemRewardLambda`

Las funciones de Lambda de consulta para Customer y Reward se encuentra en las carpetas `CQRS \Query Microservice\Customer` y `CQRS\QueryMicroservice\Reward`. Contienen los proyectos de Lambda `QueryCustomerListLambda` and `QueryRewardLambda`.

Proyecto de prueba de CQRS

El proyecto de prueba se encuentra en la carpeta `CQRS\Tests`. Este proyecto contiene un script de prueba para automatizar las pruebas de las funciones de Lambda de CQRS.

Abastecimiento de eventos mediante servicios de AWS

Las transmisiones de DynamoDB Customer y Reward inician los siguientes controladores de eventos de Lambda para procesar y sincronizar los datos de las tablas de consultas.

- La función de Lambda `EventSourceCustomer` se asigna al flujo de DynamoDB de la tabla Customer (`cqrses-customer-cmd`).
- La función de Lambda `EventSourceReward` se asigna al flujo de DynamoDB de la tabla Customer (`cqrses-reward-cmd`).

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Más patrones

- Acceda a aplicaciones de contenedores de forma privada en Amazon EKS mediante AWS PrivateLink y un Network Load Balancer
- Automatice la adición o actualización de entradas de registro de Windows con AWS Systems Manager
- Automatización de la conmutación por error y la conmutación por recuperación entre regiones mediante DR Orchestrator Framework
- Cree e implemente automáticamente una aplicación Java en Amazon EKS mediante una CI/CD canalización
- Cree CI/CD canalizaciones y clústeres de Amazon ECS de forma automática para microservicios mediante AWS CDK
- Copia de seguridad y archivo de datos de mainframe en Amazon S3 mediante BMC AMI Cloud Data
- Cree un PAC de servidor empresarial Micro Focus con Amazon EC2 Auto Scaling y Systems Manager
- Cree una malla de datos empresarial con Amazon DataZone y AWS CDK AWS CloudFormation
- Almacenamiento en contenedores de las cargas de trabajo de mainframe que Blu Age ha modernizado
- Convierta y desempaquete datos EBCDIC a ASCII en AWS mediante Python
- Convertir archivos de datos de mainframe con diseños de registros complejos mediante Micro Focus
- Cree un portal para microinterfaces mediante Angular AWS Amplify y Module Federation
- Implementar contenedores mediante Elastic Beanstalk
- Emule Oracle DR mediante una base de datos global de Aurora compatible con PostgreSQL
- Genere información de datos mediante AWS Mainframe Modernization Amazon Q en Quick Sight
- Genere información sobre z/OS datos de Db2 mediante AWS Mainframe Modernization Amazon Q en Quick Sight
- Identificación automática de las imágenes de contenedor duplicadas al migrar a un repositorio de Amazon ECR
- Implementación de diagnósticos y solución de problemas de Kubernetes con tecnología de IA con la integración de K8sGPT y Amazon Bedrock

- Implemente la autenticación basada en Microsoft Entra ID en una aplicación de mainframe modernizada de AWS Blu Age
- Implementación del control de versiones de API basado en rutas mediante dominios personalizados en Amazon API Gateway
- Migración gradual de Amazon RDS para Oracle a Amazon RDS para PostgreSQL con Oracle SQL Developer y AWS SCT
- Integrar el controlador universal Stonebranch con AWS Mainframe Modernization
- Administre los productos de AWS Service Catalog en varias cuentas y regiones de AWS
- Migrar una cuenta de AWS miembro de AWS Organizations a AWS Control Tower
- Migración y réplica de archivos VSAM a Amazon RDS o Amazon MSK mediante Connect de Precisely
- Migración de SAP ASE a Amazon RDS para SQL Server utilizando AWS DMS
- Migración de tablas externas de Oracle a Amazon Aurora compatible con PostgreSQL
- Modernice la aplicación de CardDemo mainframe mediante AWS Transform
- Modernice e implemente aplicaciones de mainframe con Terraform AWS Transform
- Modernice las cargas de trabajo de impresión por lotes de mainframe AWS mediante Rocket Enterprise Server y LRS VPSX/MFI
- Modernizar las cargas de trabajo de impresión en línea de mainframe en AWS mediante Micro Focus Enterprise Server y LRS VPSX/MFI
- Modernice la administración de la producción del mainframe AWS mediante Rocket Enterprise Server y LRS X PageCenter
- Mover los archivos de mainframe directamente a Amazon S3 mediante Transfer Family
- Optimice las implementaciones sin servidor con varias cuentas mediante los flujos de trabajo y Actions AWS CDK GitHub
- Optimice el rendimiento de su aplicación modernizada AWS Blu Age
- Automatice blue/green las implementaciones de las bases de datos globales de Amazon Aurora mediante los principios de la IaC
- Replicar bases de datos de unidades centrales en AWS mediante Precisely Connect
- Ejecute tareas de Amazon ECS en Amazon WorkSpaces con Amazon ECS Anywhere
- Envíe datos de telemetría desde y AWS Lambda OpenSearch para análisis y visualización en tiempo real

- Configure la detección de CloudFormation desviaciones en una organización multirregional y multicuenta
- Estructure un proyecto de Python en una arquitectura hexagonal con AWS Lambda
- Pruebe AWS la infraestructura mediante LocalStack Terraform Tests
- Transforma Easytrieve a lenguajes modernos usando AWS Transform personalizado
- Actualice los clústeres de SAP Pacemaker de a ENSA1 ENSA2
- Uso de Amazon Q Developer como asistente de codificación para aumentar la productividad
- Validar Account Factory para el código Terraform (AFT) localmente

Unidades centrales

Temas

- Acceda Servicios de AWS desde IBM z/OS instalando el AWS CLI
- Copia de seguridad y archivo de datos de mainframe en Amazon S3 mediante BMC AMI Cloud Data
- Cree programas COBOL Db2 mediante y AWS Mainframe Modernization AWS CodeBuild
- Cree un PAC de servidor empresarial Micro Focus con Amazon EC2 Auto Scaling y Systems Manager
- Cree un visor de archivos de unidad central avanzada en la nube de AWS
- Almacenamiento en contenedores de las cargas de trabajo de mainframe que Blu Age ha modernizado
- Convierta y desempaquete datos EBCDIC a ASCII en AWS mediante Python
- Convierta archivos de mainframe del formato EBCDIC al formato ASCII delimitado por caracteres en Amazon S3 mediante AWS Lambda
- Convertir archivos de datos de mainframe con diseños de registros complejos mediante Micro Focus
- Implementar un entorno para aplicaciones de Blu Age en contenedores mediante Terraform
- Genere información sobre z/OS datos de Db2 mediante AWS Mainframe Modernization Amazon Q en Quick Sight
- Genere información de datos mediante AWS Mainframe Modernization Amazon Q en Quick Sight
- Implemente la autenticación basada en Microsoft Entra ID en una aplicación de mainframe modernizada de AWS Blu Age
- Integrar el controlador universal Stonebranch con AWS Mainframe Modernization
- Migración y réplica de archivos VSAM a Amazon RDS o Amazon MSK mediante Connect de Precisely
- Modernice la aplicación de CardDemo mainframe mediante AWS Transform
- Modernice e implemente aplicaciones de mainframe con Terraform AWS Transform
- Modernice la administración de la producción del mainframe AWS mediante Rocket Enterprise Server y LRS X PageCenter
- Modernice las cargas de trabajo de impresión por lotes de mainframe AWS mediante Rocket Enterprise Server y LRS VPSX/MFI

- Modernización del mainframe: DevOps adelante AWS con Rocket Software Enterprise Suite
- Modernizar las cargas de trabajo de impresión en línea de mainframe en AWS mediante Micro Focus Enterprise Server y LRS VPSX/MFI
- Mover los archivos de mainframe directamente a Amazon S3 mediante Transfer Family
- Optimice el rendimiento de su aplicación modernizada AWS Blu Age
- Proteja y optimice el acceso de los usuarios a una base de datos de federación DB2 en AWS mediante contextos de confianza
- Transfiera z/OS datos de Db2 a gran escala a Amazon S3 en archivos CSV
- Transforma Easytrieve a lenguajes modernos usando AWS Transform personalizado
- Más patrones

Acceda Servicios de AWS desde IBM z/OS instalando el AWS CLI

Souma Ghosh, Paulo Vitor Pereira y Phil de Valence, Amazon Web Services

Resumen

The AWS Command Line Interface (AWS CLI) es una herramienta de código abierto para gestionar varios AWS servicios mediante comandos en una consola de línea de comandos. Con una configuración mínima, puede ejecutar comandos desde sesiones de línea de comandos, como el símbolo del sistema, la terminal y el intérprete de comandos bash para implementar una funcionalidad equivalente a la proporcionada por Consola de administración de AWS basada en el navegador.

Todas las funciones de administración, gestión y acceso de la AWS infraestructura como servicio (IaaS) Consola de administración de AWS están disponibles en la AWS API y. AWS CLI Puede instalarlas AWS CLI en un z/OS mainframe de IBM para acceder, gestionar e interactuar directamente con ellas Servicios de AWS desde z/OS. AWS CLI Esto permite a los usuarios y las aplicaciones realizar diversas tareas, como:

- Transferencia de archivos o conjuntos de datos entre z/OS un almacenamiento de objetos del Amazon Simple Storage Service (Amazon S3) y visualización del contenido de los buckets
- Iniciar y detener diferentes AWS recursos; por ejemplo, iniciar un trabajo por lotes en un entorno AWS Mainframe Modernization
- Llamar a una AWS Lambda función para implementar una lógica empresarial común
- Integración con inteligencia artificial y machine learning (IA y ML) y servicios de análisis

Este patrón describe cómo instalar, configurar y usar la función AWS CLI en z/OS. You can install it globally, so it's available to all z/OS los usuarios o a nivel de usuario. El patrón también detalla cómo usarlo AWS CLI en una sesión de línea de comandos interactiva desde z/OS Unix System Services (USS) o como un trabajo por lotes.

Requisitos previos y limitaciones

Requisitos previos

- Comunicación de red de a z/OS AWS

  De forma predeterminada, AWS CLI envía las solicitudes Servicios de AWS mediante HTTPS en el puerto TCP 443. Para usarlo AWS CLI correctamente, debe poder realizar conexiones salientes en

el puerto TCP 443. Puede usar cualquiera de los siguientes comandos z/OS USS (es posible que algunos de ellos no estén instalados en su entorno) para probar la conectividad de la red desde z/OS hasta AWS:

```
ping amazonaws.com
dig amazonaws.com
traceroute amazonaws.com
curl -k https://docs.aws.amazon.com/cli/v1/userguide/cli-chap-welcome.html
```

- AWS credenciales

  Para poder comunicarse con Nube de AWS los servicios de z/OS, es AWS CLI necesario configurar algunas credenciales con privilegios para acceder al destino. Cuenta de AWS Para los comandos programáticos AWS, puede utilizar las teclas de acceso, que consisten en un identificador de clave de acceso y una clave de acceso secreta. Si no tiene claves de acceso, puede crearlas desde la Consola de administración de AWS. Como práctica recomendada, no utilice las claves de acceso del usuario Cuenta de AWS raíz para ninguna tarea a menos que se requiera el usuario raíz. En su lugar, cree un nuevo usuario administrador de IAM y prepárese para los permisos con privilegios mínimos para configurar el usuario con claves de acceso. Tras crear el usuario, puede crear un ID de clave de acceso y una clave de acceso secreta para este usuario.

  > **Warning**
  >
  > AWS Identity and Access Management Los usuarios (IAM) tienen credenciales de larga duración que representan un riesgo para la seguridad. Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten.

- IBM Python para z/OS

  AWS CLI Requiere Python 3.8 o posterior. IBM ha permitido que Python se ejecute z/OS con IBM Open Enterprise Python for z/OS. IBM Open Enterprise Python está disponible de forma gratuita a través de Shopz SMP/E, o puede descargar el archivo PAX desde el sitio web de IBM. Para obtener instrucciones, consulte la documentación de instalación y configuración de IBM Open Enterprise Python para z/OS.

Limitaciones

- Las instrucciones de instalación que se proporcionan en este patrón se aplican únicamente a la versión 1 de la AWS CLI . La última versión de AWS CLI es la versión 2. Sin embargo, este patrón usa la versión anterior porque los métodos de instalación son diferentes para la versión 2 y los ejecutables binarios disponibles para la versión 2 no son compatibles con el z/OS sistema.

Versiones de producto

- AWS CLI versión 1
- Python 3.8 o posterior

Arquitectura

Pila de tecnología

- Mainframe que ejecuta z/OS
- Servicios de sistemas z/OS UNIX para mainframe (USS)
- Mainframe Open MVS (OMVS): z/OS interfaz de comandos del entorno shell de UNIX
- Disco de mainframe, como un dispositivo de almacenamiento de acceso directo (DASD)
- AWS CLI

Arquitectura de destino

El siguiente diagrama muestra un AWS CLI despliegue en IBM z/OS. Puede invocarla AWS CLI desde una sesión de usuario interactiva, como una sesión de SSH o una sesión de telnet. También puede invocarlo desde un trabajo por lotes mediante el lenguaje de control de tareas (JCL) o desde cualquier programa que pueda llamar a un comando de shell de Unix. z/OS

AWS CLI Se comunica con los Servicio de AWS puntos finales a través de una TCP/IP red. Esta conexión de red puede realizarse a través de Internet o mediante una AWS Direct Connect conexión privada desde el centro de datos del cliente a los centros de Nube de AWS datos. La comunicación se autentica con AWS credenciales y se cifra.

Automatización y escala

Puede explorar las capacidades de AWS CLI y desarrollar scripts Servicio de AWS de shell USS para gestionar sus AWS recursos desde z/OS. También puede ejecutar AWS CLI comandos y

scripts de shell desde el entorno z/OS por lotes, y puede automatizar los trabajos por lotes para que se ejecuten según un cronograma específico mediante la integración con los programadores de mainframe. AWS CLI Los comandos o scripts se pueden codificar dentro de los parámetros (PARMs) y los procedimientos (PROCs), y se pueden escalar siguiendo el enfoque estándar de llamar al PARM o al PROC desde diferentes trabajos por lotes con diferentes parámetros.

Tools (Herramientas)

- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que te ayuda a interactuar Servicios de AWS mediante los comandos de tu consola de línea de comandos.

Prácticas recomendadas

- Por motivos de seguridad, restrinja los permisos de acceso al directorio USS donde se almacenan los detalles de las claves de AWS acceso. Permita el acceso únicamente a los usuarios o programas que usen la AWS CLI.
- No utilice las claves de acceso del usuario Cuenta de AWS root para ninguna tarea. Por el contrario, cree un nuevo usuario administrador de IAM con las claves de acceso correspondientes y que sea para usted.

> **Warning**
>
> Los usuarios de IAM tienen credenciales de larga duración, lo que supone un riesgo de seguridad. Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten.

Epics

Instale AWS CLI la versión 1 en z/OS USS

Tarea	Descripción	Habilidades requeridas
Instale Python 3.8 o posterior.	1. Inicie sesión en la interfaz de línea de comandos del z/	Administrador de mainframe z/OS

Tarea	Descripción	Habilidades requeridas
	OS USS mediante uno de estos métodos: • Utilice un comando OMVS de la Opción de tiempo compartido (TSO) desde el panel Instalación de Sistema Interactivo de Productividad (ISPF), o • Utilice SSH o telnet para conectarse a la IP de la partición lógica del mainframe (LPAR). Este patrón supone que `cliuser` es el ID de usuario que se usa para iniciar sesión en el entorno USS y que `/u/cliuser/` es el directorio principal del usuario. Puede configurar el directorio principal del usuario de forma diferente en su z/OS entorno en función de los requisitos de instalación. 2. Siga la guía de instalación de IBM Open Enterprise Python para z/OS para instalar Python 3.8 o una versión posterior si aún no lo tiene instalado.	

Tarea	Descripción	Habilidades requeridas

Configure las variables de entorno de USS.	Agregue variables de entorno al perfil. Puede añadirlas al archivo `/u/cliuser/.profile` de un usuario individual (`cliuser`) o al archivo `/etc/profile` de todos los usuarios.
	
	Note
	Este patrón asume que Python se ha instalado en el directorio `/u/awscli/python`. Si el directorio de instalación es diferente, actualice el código en consecuencia.
	
	`# Python configuration`
	`export BPXKAUTOC`
	`VT='ON'`
	`export CEERUNOPT`
	`S='FILETAG(AUTOCVT`
	`,AUTOTAG) POSIX(ON)'`
	`export TAGREDIR_ERR=txt`
	`export TAGREDIR_IN=txt`
	`export TAGREDIR_`
	`OUT=txt`
	
	`# AWS CLI configura`
	`tion`
	`export PATH=/u/c`
	`liuser/python/bin:`
	`$PATH`
		Administrador de mainframe z/OS

Tarea	Descripción	Habilidades requeridas
	`export PYTHONPATH=/u/cliuser/python:$PYTHONPATH`	
Pruebe la instalación de Python.	Ejecute el comando python: `python --version` El resultado debe confirmar que Python 3.8 o posterior está instalado correctamente.	Administrador de mainframe z/OS

Verifique o instale pip.	1. El comando pip normalmente se instala automáticamente al instalar Python desde el sitio web de IBM. Para comprobar esto, ejecute el comando:
	`pip —-version`
	Si pip está instalado, este comando debería mostrar la versión instalada.
	2. Si no encuentra el comando pip, instale pip ejecutando el siguiente comando:
	`python -m ensurepip --upgrade`
	Para ver más opciones de instalación, consulte la documentación de pip.
		Administrador de mainframe z/OS

Tarea	Descripción	Habilidades requeridas

Instale la AWS CLI versión 1.	1. Para instalar el AWS CLI, ejecute el comando:
	`python -m pip install awscli`
	El resultado debería ser similar al siguiente.
	`Successfully installed PyYAML-6.0.1 awscli-1.32.23 botocore-1.34.23 colorama-0.4.4 docutils-0.16 jmespath-1.0.1 pyasn1-0.5.1 python-dateutil-2.8.2 rsa-4.7.2 s3transfer-0.10.0 urllib3-2.0.7`
	2. Cambie el permiso del ejecutable de aws ejecutando el siguiente comando. Asegúrese de actualizar el directorio de marcadores de posición `<python_installation_dir>` con la ruta de instalación de Python.
	`chmod 744 <python_installation_dir>/bin/aws`
		Administrador de mainframe z/OS

Tarea	Descripción	Habilidades requeridas

	3. Ejecute el siguiente comando para probar la AWS CLI instalación:
	`aws --version`
	El resultado debería mostrar las versiones de Python y botocore, de forma similar a la siguiente. AWS CLI
	`aws-cli/1.32.3`
	`Python/3.9.5`
	`OS/390/27.00`
	`botocore/1.34.3`	

Configure el AWS CLI acceso desde z/OS

Tarea	Descripción	Habilidades requeridas
Configure las claves de AWS acceso, la región predeterm inada y la salida.	La AWS CLI documenta ción describe diferentes opciones para configurar el AWS acceso. Puede elegir una configuración de acuerdo con los estándares de su organización. En este ejemplo, se utiliza la configuración de credenciales a corto plazo. 1. Configure la AWS CLI mediante el comando siguiente:	Administrador de AWS, administrador de mainframe , z/OS desarrollador de mainframe z/OS

Tarea	Descripción	Habilidades requeridas

	`aws configure`
	2. Proporcione los detalles de los siguientes elementos cuando se le solicite. El identificador de la clave de acceso y los valores de la clave de acceso secreta provienen de las claves que se obtuvieron al configura r AWS las credenciales en los pasos de los requisitos previos.
	`AWS Access Key ID [None]: ASIAIOSFO DNN7EXAMPLE`
	`AWS Secret Access Key [None]: wJalrXUtn FEMI/K7MDENG/bPxRf iCYEXAMPLEKEY`
	`Default region name [None]: us-east-1`
	`Default output format [None]:`
	`aws configure set aws_session_token IQoJb3JpZ2luX2IQoJ b3JpZ2luX2IQoJb3Jp Z2luX2IQoJb3JpZ2lu X2IQoJb3JpZVERYLON GSTRINGEXAMPLE`
	Esta configuración, incluidas las claves de acceso, se almacena en la carpeta `/u/cliuse`	

Tarea	Descripción	Habilidades requeridas
	`r/.aws` . Por motivos de seguridad, restrinja esta carpeta para permitir el acceso únicamente a los usuarios o programas que utilizan la AWS CLI.	

Tarea	Descripción	Habilidades requeridas
Pruebe el. AWS CLI	1. Ejecute el siguiente comando en la línea de comandos para AWS CLI probarlo con un comando sencillo: `aws s3 ls` El resultado debería enumerar todos los depósitos S3 configurados Cuenta de AWS sin ningún error. 2. Siga las instrucciones de las dos secciones siguiente s para transferir datos de USS a Amazon S3. Puede elegir una de estas dos opciones: • Opción 1 (siguiente sección): transfiera de forma interactiva un archivo EBCDIC con valores separados por comas (CSV) a Amazon S3 y consulte el archivo desde Amazon Athena. • Opción 2: transfiera un conjunto de datos EBCDIC de longitud fija a Amazon S3 como un trabajo por lotes.	z/OS Administrador de mainframe, desarrollador de mainframe z/OS

Opción 1: transferencia de datos de USS a Amazon S3 de forma interactiva desde una sesión de USS

Tarea	Descripción	Habilidades requeridas
Descargue y transfiera el archivo CSV de muestra.	1. Descargue `sales-records.csv` desde la sección Archivos adjuntos. Este archivo proporciona un ejemplo de archivo CSV con registros de ventas. 2. Transfiera el archivo a USS. z/OS 3. Compruebe que el archivo `/u/cliuser/sales-records.csv` se puede leer en formato EBCDIC en USS mediante el editor de texto que desee.	Desarrollador de aplicaciones, desarrollador de mainframe z/OS

Cree un bucket de S3 y cargue el archivo CSV.	1. Cree un bucket de S3 para almacenar el archivo CSV.
	`aws s3 mb s3://<s3_bucket_name>`
	donde `<s3_bucket_name>` es el nombre exclusivo de un bucket; por ejemplo:
	`aws s3 mb s3://DOC-EXAMPLE-BUCKET1`
	2. Cargue el archivo CSV de z/OS USS al bucket de S3:
		Desarrollador de aplicaciones, desarrollador de mainframe z/OS

Tarea	Descripción	Habilidades requeridas

	`aws s3 cp <csv_file _path> s3://<s3_ bucket_name>`
	
	Por ejemplo:
	
	`aws s3 cp /u/cliuser/ sales-records.csv s3://DOC-EXAMPLE-B UCKET1`
	
	3. Enumere el contenido del bucket de S3 y confirme que incluye el archivo cargado:
	
	`aws s3 ls s3://<s3_ bucket_name>`
	
	Por ejemplo:
	
	`aws s3 ls s3://DOC-EXAMPLE-BUCKET1`	

Tarea	Descripción	Habilidades requeridas
Consulte el bucket de S3 y el archivo cargado.	1. Inicie sesión en la consola Amazon S3 Consola de administración de AWS y ábrala. 2. Navegue al lugar correspondiente para ver el nuevo bucket de S3 y el objeto cargado. Para más información sobre la carga de objetos, consulte Introducción a Amazon S3 en la documentación de Amazon S3.	AWS general

Tarea	Descripción	Habilidades requeridas

Ejecute una consulta SQL en una tabla de Amazon Athena.	1. Abra la consola de Amazon Athena.
	2. Cree una tabla nueva (por ejemplo, `DOC-EXAMPLE-BUCKET`) con los datos CSV de Amazon S3. Para más información, consulte Consultas del inventario de Amazon S3 con Amazon Athena en la documentación de Amazon S3.
	3. Ejecute la consulta `SELECT` en la tabla para ver los datos.
	`SELECT * FROM <table_name>;`
	Por ejemplo:
	`SELECT * FROM DOC-EXAMPLE-BUCKET;`
	El resultado de la consulta SQL mostrará el contenido del archivo CSV.
		AWS general, desarrollador de aplicaciones

Opción 2: transferencia de datos de USS a Amazon S3 mediante JCL por lotes

Tarea	Descripción	Habilidades requeridas
Cargue el archivo de muestra.	1. Descargue `sales-records-fixed.txt`	Desarrollador de mainframes z/OS

Tarea	Descripción	Habilidades requeridas
	desde la sección Archivos adjuntos. Este es un archivo de muestra con registros de ventas. Cambie el nombre del archivo de texto; por ejemplo, a `USER.DATA.FIXED` . 2. Transfiera el archivo a un z/OS conjunto de datos secuencial físico (PS) de 256 registros (LRECL) y con bloques fijos (FB). 3. Utilice la utilidad de lista de conjuntos de datos para comprobar que el conjunto de datos de `USER.DATA .FIXED` es legible en formato EBCDIC según la opción 3.4 del ISPF. Para obtener ejemplos, consulte la sección Información adicional.	

Tarea	Descripción	Habilidades requeridas

Cree JCL por lotes.	Codifique JCL del lote de la siguiente manera para crear el bucket de S3 de destino, cargar el conjunto de datos y enumerar el contenido del depósito. Asegúrese de reemplazar el nombre del directorio, los nombres de los archivos y el nombre del bucket por sus propios valores.
	
	`//AWSCLICP JOB`
	`ACTINFO1,'IBMUSER'`
	`,CLASS=A,MSGCLASS=`
	`H,MSGLEVEL=(1,1),`
	`// NOTIFY=&SYSUID,TIM`
	`E=1440`
	`//*--------------`
	`------------------`
	`------------------`
	`-------`
	`//* Sample job for AWS`
	`CLI`
	`//*--------------`
	`------------------`
	`------------------`
	`-------`
	`//USSCMD EXEC PGM=BPXBA`
	`TCH`
	`//STDERR DD SYSOUT=*`
	`//STDOUT DD SYSOUT=*`
	`//STDENV DD *`
	`export PATH=/u/c`
	`liuser/python/bin:`
	`$PATH`
	`//STDPARM DD *`
	`SH`
		Desarrollador de mainframe z/OS

Tarea	Descripción	Habilidades requeridas
	`export _BPXK_AUTOCVT=ON; aws s3 mb s3://DOC-EXAMPLE-BUCKET2; cp "//'USER.DATA.FIXED'" /tmp/tmpfile; aws s3 cp /tmp/tmpfile s3://DOC-EXAMPLE-BUCKET2/USER.DATA.FIXED; rm /tmp/tmpfile; aws s3 ls s3://DOC-EXAMPLE-BUCKET2; /*`	
Envíe el trabajo de JCL por lotes.	1. Envíe el trabajo de JCL que codificó en el paso anterior. 2. Compruebe el estado del trabajo en la función de visualización y búsqueda del sistema (SDSF). Si se ejecuta correctamente, el trabajo debería finalizar con el código de retorno 0. 3. El resultado estándar (STDOUT) del registro de trabajos muestra la creación correcta del bucket, la carga del conjunto de datos y la lista del contenido del bucket. Para ver una ilustración en la pantalla, consulte la sección de Información adicional.	Desarrollador de mainframe z/OS

Tarea	Descripción	Habilidades requeridas
Vea el conjunto de datos cargado en el bucket de S3.	1. Inicie sesión en la consola Amazon S3 Consola de administración de AWS y ábrala. 2. Navegue al lugar apropiado para ver el archivo cargado en el bucket de prueba. 3. Puede seguir procesando el archivo `USER.DATA.FIXED` o analizarlo mediante servicios de análisis como Amazon Redshift.	AWS general

Recursos relacionados

- AWS CLI documentación de la versión 1
- AWS Mainframe Modernization Referencia de los comandos de la CLI
- AWS Mainframe Modernization

Información adicional

USER.DATA.FIXED en la opción 3.4 del ISPF (utilidad de lista de conjuntos de datos)

SYSOUT del trabajo por lotes enviado

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Copia de seguridad y archivo de datos de mainframe en Amazon S3 mediante BMC AMI Cloud Data

Santosh Kumar Singh, Gilberto Biondo y Maggie Li, Amazon Web Services

Mikhael Liberman, Model9 Mainframe Software

Resumen

Este patrón muestra cómo hacer copias de seguridad y archivar los datos del mainframe directamente en Amazon Simple Storage Service (Amazon S3) y, a continuación, recuperar y restaurar esos datos en el mainframe mediante BMC AMI Cloud Data (antes conocido como Model9 Manager). Si busca una forma de modernizar su solución de copia de seguridad y archivado como parte de su proceso de modernización del mainframe o de cumplir con los requisitos de conformidad, este patrón puede ayudarle a cumplir esos objetivos.

Por lo general, las organizaciones que ejecutan aplicaciones empresariales principales en mainframes utilizan una biblioteca de cintas virtuales (VTL) para hacer copias de seguridad de los almacenes de datos, como archivos y registros. Este método puede resultar caro porque consume MIPS facturables y no se puede acceder a los datos almacenados en cintas fuera del ordenador central. Para evitar estos problemas, puede utilizar BMC AMI Cloud Data para transferir de forma rápida y rentable los datos operativos e históricos del mainframe directamente a Amazon S3. Puede utilizar AMI Cloud Data de BMC para realizar copias de seguridad y archivar datos y, TCP/IP al AWS mismo tiempo, aprovechar los motores del procesador de información integrado (zIIP) de IBM z para reducir los costes, el paralelismo y los tiempos de transferencia.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- BMC AMI Cloud Data con una clave de licencia válida
- Conectividad TCP/IP entre el mainframe y AWS
- Una función AWS Identity and Access Management (IAM) para acceder a un bucket de S3 read/write
- Se ha establecido el acceso al producto de seguridad de mainframe (RACF) para ejecutar los procesos de BMC AMI Cloud

- Un z/OS agente AMI Cloud de BMC (Java versión 8 de 64 bits SR5 FP16 o posterior) que tenga puertos de red disponibles, reglas de firewall que permitan el acceso a los depósitos de S3 y un sistema de archivos dedicado z/FS
- Requisitos cumplidos para el servidor de administración BMC AMI Cloud

Limitaciones

- BMC AMI Cloud Data almacena sus datos operativos en una base de datos PostgreSQL que se ejecuta como un contenedor de Docker en la misma instancia de Amazon Elastic Compute Cloud (EC2Amazon) que el servidor de administración. Actualmente, Amazon Relational Database Service (Amazon RDS) no admite actualmente como backend para BMC AMI Cloud Data. Para obtener más información sobre las últimas actualizaciones de los productos, consulte Novedades en la documentación de BMC.
- Este patrón solo realiza copias de seguridad y z/OS archiva los datos del mainframe. BMC AMI Cloud Data solo realiza copias de seguridad y archiva los archivos del mainframe.
- Este patrón no convierte los datos a formatos abiertos estándar, como JSON o CSV. Utilice un servicio de transformación adicional como BMC AMI Cloud Analytics (anteriormente conocido como Model9 Gravity) para convertir los datos a formatos abiertos estándar. Las aplicaciones nativas en la nube y las herramientas de análisis de datos pueden acceder a los datos una vez que estos se hayan escrito en la nube.

Versiones de producto

- BMC AMI Cloud Data, versión 2.x

Arquitectura

Pila de tecnología de origen

- Mainframe que ejecuta z/OS
- Archivos de mainframe, como conjuntos de datos y archivos de z/OS UNIX System Services (USS)
- Disco de mainframe, como un dispositivo de almacenamiento de acceso directo (DASD)
- Cinta de mainframe (biblioteca de cintas físicas o virtuales)

Pila de tecnología de destino

- Amazon S3
- EC2 Instancia de Amazon en una nube privada virtual (VPC)
- AWS Direct Connect
- Amazon Elastic File System (Amazon EFS)

Arquitectura de destino

El siguiente diagrama muestra una arquitectura de referencia en la que los agentes de software BMC AMI Cloud Data de un mainframe controlan los procesos de archivado y respaldo de datos heredados que almacenan los datos en Amazon S3.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Los agentes de software AMI Cloud Data de BMC se ejecutan en particiones lógicas de mainframe ()LPARs. Los agentes de software leen y escriben datos del mainframe desde el DASD o graban directamente en Amazon S3 a través de TCP/IP.
2. AWS Direct Connect configura una conexión física y aislada entre la red local y. AWS Para mejorar la seguridad, ejecute una site-to-site VPN sobre ella Direct Connect para cifrar los datos en tránsito.
3. El bucket de S3 almacena los archivos del mainframe como datos de almacenamiento de objetos y los agentes de BMC AMI Cloud Data se comunican directamente con los buckets de S3. Los certificados se utilizan para el cifrado HTTPS de todas las comunicaciones entre el agente y Amazon S3. El cifrado de datos de Amazon S3 se utiliza para cifrar y proteger los datos en reposo.
4. Los servidores de administración de datos AMI Cloud de BMC se ejecutan como contenedores Docker en las EC2 instancias. Las instancias se comunican con los agentes que se ejecutan en el mainframe LPARs y en los buckets S3.
5. Amazon EFS se monta en EC2 instancias activas y pasivas para compartir el almacenamiento del Network File System (NFS). Esto garantiza que los metadatos relacionados con una política creada en el servidor de administración no se pierdan en caso de una conmutación por error. En caso de una conmutación por error por parte del servidor activo, puede acceder al servidor pasivo sin pérdida de datos. Si el servidor pasivo devuelve un error, también podrá acceder al servidor activo sin perder ningún dato.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática escalable en el Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Elastic File System (Amazon EFS) permite crear y configurar sistemas de archivos compartidos en la Nube de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar casi cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.
- AWS Direct Connectconecta su red interna a una AWS Direct Connect ubicación a través de un cable Ethernet de fibra óptica estándar. Con esta conexión, puede crear interfaces virtuales directamente con los AWS servicios públicos y, al mismo tiempo, omitir a los proveedores de servicios de Internet en su ruta de red.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.

Herramientas de BMC

- El servidor de administración BMC AMI Cloud es una aplicación GUI que se ejecuta como un contenedor Docker en una Amazon Machine Image (AMI) de Amazon Linux para Amazon. EC2 El servidor de administración proporciona la funcionalidad necesaria para gestionar las actividades de BMC AMI Cloud, como la elaboración de informes, la creación y administración de políticas, la ejecución de archivos y la realización de copias de seguridad, recuperaciones y restauraciones.
- El agente de BMC AMI Cloud se ejecuta en un LPAR de mainframe en las instalaciones que lee y escribe archivos directamente en el almacenamiento de objetos mediante TCP/IP. Una tarea iniciada se ejecuta en un LPAR de mainframe y es responsable de leer y escribir los datos de copia de seguridad y archivar en Amazon S3 y desde este.
- La interfaz de línea de comandos (M9CLI) de BMC AMI Cloud Mainframe le proporciona un conjunto de comandos para realizar acciones de BMC AMI Cloud directamente desde TSO/E o en operaciones por lotes, sin depender del servidor de administración.

Epics

Creación de un bucket de S3 y una política de IAM

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Cree un bucket de S3 para almacenar los archivos y volúmenes de los que desee realizar copias de seguridad y archivar desde su entorno de mainframe.	AWS general
Cree una política de IAM.	Todos los servidores de administración y agentes de BMC AMI Cloud requieren acceso al bucket de S3 que creó en el paso anterior. Para conceder el acceso necesario, cree la siguiente política de IAM: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "Listfolder", "Action": [ "s3:ListBucket", "s3:GetBucketLocation", "s3:ListBucketVersions" ],`	AWS general

Tarea	Descripción	Habilidades requeridas
	"Effect": "Allow", "Resource": ["arn:aws:s3:::<Bucket Name>"] }, { "Sid": "Objectaccess", "Effect": "Allow", "Action": ["s3:PutObject", "s3:GetObjectAcl", "s3:GetObject", "s3:DeleteObjectVersion", "s3:DeleteObject", "s3:PutObjectAcl", "s3:GetObjectVersion"], "Resource": ["arn:aws:s3:::<Bucket Name>/*"] }] }	

Obtenga la licencia del software BMC AMI Cloud y descárguelo

Tarea	Descripción	Habilidades requeridas
Obtenga una licencia de software de BMC AMI Cloud.	Para obtener una clave de licencia de software, póngase en contacto con el equipo de BMC AMI Cloud. El resultado del z/OS `D M=CPU` comando es necesario para generar una licencia.	Responsable de compilación
Descarga de la clave de licencia y el software BMC AMI Cloud	Puede obtener los archivos de instalación y la clave de licencia si sigue las instrucciones de la documentación de BMC.	Administrador de la infraestructura de mainframe

Instalación del agente de software BMC AMI Cloud en el mainframe

Tarea	Descripción	Habilidades requeridas
Instalación del agente de software BMC AMI Cloud	1. Antes de iniciar el proceso de instalación, compruebe que cumple los requisitos mínimos de software y hardware para el agente. 2. Para instalar el agente, siga las instrucciones de la documentación de BMC. 3. Cuando el agente comience a ejecutarse en el LPAR del mainframe, compruebe si aparece el mensaje `ZM91000I MODEL9 BACKUP AGENT`	Administrador de la infraestructura de mainframe

Tarea	Descripción	Habilidades requeridas
	`INITIALIZED` en la cola Compruebe que la conectividad entre el agente y el bucket de S3 se ha establecido correctamente buscando el mensaje `Object store connectivity has been established successfully` en el STDOUT del agente.	

Configurar un servidor de administración AMI Cloud de BMC en una instancia EC2

Tarea	Descripción	Habilidades requeridas
Cree instancias de Amazon EC2 Linux 2.	Lance dos instancias de Amazon EC2 Linux 2 en distintas zonas de disponibilidad siguiendo las instrucciones del paso 1: lanzar una instancia de la EC2 documentación de Amazon. Su instancia debe cumplir los siguientes requisitos de hardware y software recomendados: • CPU: 4 núcleos como mínimo • RAM: 8 GB como mínimo • Unidad: 40 GB	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	• EC2 Instancia recomenda da: C5.xlarge • Sistema operativo: Linux • Software: Docker, unzip, VI/ vim • Ancho de banda de la red mínimo de 1 GB Para obtener más información, consulte la Documentación de BMC.	
Crear un sistema de archivos de Amazon EFS.	Cree un sistema de archivos Amazon EFS siguiendo las instrucciones del Paso 1: Cree su sistema de archivos Amazon EFS en la documenta ción de Amazon EFS. Al crear el sistema de archivos, haga lo siguiente: • Elija la clase de almacenam iento estándar. • Elija la misma VPC que utilizó para lanzar las instancias EC2 .	Administrador de la nube, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas

Instale Docker y configure el servidor de administración.	Conéctese a sus EC2 instancias:
	
	Conéctate a tus EC2 instancias siguiendo las instrucciones de Connect to your Linux en la EC2 documentación de Amazon.
	
	Configura tus EC2 instancias:
	
	Para cada EC2 instancia, haz lo siguiente:
	
	1. Para instalar Docker, ejecute el comando:
	
	`sudo yum install docker`
	
	2. Para iniciar Docker, ejecute el comando:
	
	`sudo service docker start`
	
	3. Para validar el estado de Docker, ejecute el comando:
	
	`sudo service docker status`
	
	4. En la carpeta `/etc/selinux` , cambie el archivo `config` a `SELINUX=permissive` .
		Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas

	5. Sube los `VerificationScripts.zip` archivos `model9-v2.x.y_build_build-id-server.zip` y (que descargaste anteriormente) a una carpeta temporal de una de las EC2 instancias (por ejemplo, a la `/var/tmp` carpeta de tu instancia).
	6. Para ir a la carpeta `tmp`, ejecute el comando:
	`cd/var/tmp`
	7. Para descomprimir el script de verificación, ejecute el comando:
	`unzip VerificationScripts.zip`
	8. Para cambiar el directorio, ejecute el comando:
	`cd /var/tmp/sysutils/PrereqsScripts`
	9. Para ejecutar el script de verificación, ejecute el comando:
	`./M9VerifyPrereqs.sh`	

Tarea	Descripción	Habilidades requeridas
	10. Cuando el script de verificación le pida que introduzca información, introduzca la URL y el número de puerto de Amazon S3. A continuación, introduce la z/OS IP/DNS y el número de puerto. **Note** El script comprueba que la EC2 instancia se puede conectar con el bucket y el agente de S3 que se están ejecutando en el mainframe. Si se establece una conexión, aparece un mensaje de confirmación.	

Tarea	Descripción	Habilidades requeridas

Instale el software del servidor de administración.	1. Crea una carpeta y una subcarpeta en el directorio raíz (por ejemplo `/data/model9`) en el EC2 caso de que planees convertir el servidor activo.
	2. Para instalar el paquete `amazon-efs-utils` y montar el sistema de archivos Amazon EFS que creó anteriormente, ejecute los siguientes comandos:
	`sudo yum install -y amazon-efs-utils`
	`sudo mount -t efs -o tls <File System ID>:/ /data/model9`
	3. Para actualizar el `/etc/fstab` archivo de la EC2 instancia con una entrada para el sistema de archivos Amazon EFS (de modo que Amazon EFS se vuelva a montar automáticamente cuando Amazon se EC2 reinicie), ejecuta el comando:
	`<Amazon-EFS-file-system-id>:/ /data/model9 efs defaults,_netdev 0 0`
		Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas

	4. Para definir la ruta a los archivos de instalación de BMC AMI Cloud y la ubicación de instalación de destino, ejecute los siguientes comandos para exportar las variables:
	`export MODEL9_HOME=/data/model9`
	`export M9INSTALL=/var/tmp`
	Note
	Le recomendamos que añada estos comandos de exportación a su script `.bashrc`.
	5. Para cambiar el directorio, ejecute el comando `cd $MODEL9_HOME` y, a continuación, cree otro subdirectorio ejecutando el comando `mkdir diag`.
	6. Para descomprimir el archivo de instalación, ejecute el comando:
	`unzip $M9INSTALL/model9-<v2.x.y>_build_<build-id>-server.zip`	

Tarea	Descripción	Habilidades requeridas

	Note
	Sustituya `x.y` (la versión) y `build-id` por sus valores.
	7. Para implementar la aplicación, ejecute los siguientes comandos:
	`docker load -i $MODEL9_HOME/model9-<v2.x.y>_build_<build-id>.docker`
	`docker load -i $MODEL9_HOME/postgres-12.10-x86.docker.gz`
	Note
	Sustituya `v2.x.y` (la versión) y `build-id` por sus valores.
	8. En la carpeta `$MODEL9_HOME/conf` , actualice el archivo `model9-local.yml` .
	Note
	Algunos de los parámetros tienen valores predeterm	

Tarea	Descripción	Habilidades requeridas

	inados y otros se pueden actualiza r según sea necesario. Para más informaci ón, consulte las instrucciones en el archivo `model9-lo cal.yml` .
	9. Cree un archivo denominad o `$MODEL9_HOME/conf` y, a continuación, añada los siguientes parámetros al archivo:
	`TZ=America/New_York`
	`EXTRA_JVM_ARGS=-Xmx2048m`
	10. Para crear un puente de red Docker, ejecute el comando:
	`docker network create -d bridge model9network`
	11. Para iniciar el contenedo r de base de datos PostgreSQL de BMC AMI Cloud, ejecute el siguiente comando:
	`docker run -p 127.0.0.1:5432:5432 \`	

Tarea	Descripción	Habilidades requeridas

	`-v $MODEL9_HOME/db/data:/var/lib/postgresql/data:z \`
	`--name model9db --restart unless-stopped \`
	`--network model9network \`
	`-e POSTGRES_PASSWORD=model9 -e POSTGRES_DB=model9 -d postgres:12.10`
	
	12. Una vez que se inicie la ejecución del contenedor de PostgreSQL, ejecute el siguiente comando para iniciar el servidor de aplicaciones:
	
	`docker run -d -p 0.0.0.0:443:443 -p 0.0.0.0:80:80 \`
	`--sysctl net.ipv4.tcp_keepalive_time=600 \`
	`--sysctl net.ipv4.tcp_keepalive_intvl=30 \`
	`--sysctl net.ipv4.tcp_keepalive_probes=10 \`
	`-v $MODEL9_HOME:/model9:z -h $(hostname) --restart unless-stopped \`
	`--env-file $MODEL9_HOME/conf/model9.env \`
	`--network model9network \`	

Tarea	Descripción	Habilidades requeridas

	`--name model9-v2.x.y model9:<v2.x.y>.<build-id>`
	
	Note
	Sustituya `v2.x.y` (la versión) y `build-id` por sus valores.
	
	13. Para comprobar el estado de ambos contenedores, ejecute el comando:
	
	`docker ps -a`
	
	14. Para instalar un servidor de administración en las EC2 instancias pasivas, repita los pasos 1 a 4, 7 y 10 a 13.
	
	Note
	Para solucionar problemas, vaya a los registros almacenados en la carpeta `/data/model9/logs/` . Para obtener más información, consulte la Documentación de BMC.	

Incorporación de un agente y defina una política de copia de seguridad o archivado en el servidor de administración de BMC AMI Cloud

Tarea	Descripción	Habilidades requeridas
Añada un nuevo agente.	Antes de añadir un nuevo agente, confirme lo siguiente: • Se está ejecutando un agente de BMC AMI Cloud en el LPAR del mainframe y se ha inicializado por completo. Para identificar al agente, busque el mensaje de inicialización `ZM91000I MODEL9 BACKUP AGENT INITIALIZED` en la cola. • Un contenedor de Docker del servidor de administración está completamente inicializado y en ejecución. Debe crear un agente en el servidor de administración antes de definir cualquier política de copia de seguridad y archivado. Para crear el agente, haga lo siguiente: 1. Usa un navegador web para acceder al servidor de administración que está desplegado en tu EC2 máquina Amazon y, a continuación, inicia sesión con tus credenciales de mainframe.	Desarrollador o administrador de almacenamiento de mainframe

Tarea	Descripción	Habilidades requeridas
	2. Elija la pestaña AGENTES y, a continuación, AGREGAR NUEVO AGENTE. 3. En Nombre, escriba el nombre del agente. 4. En el campo Nombre de host/dirección IP, introduzca el nombre de host o la dirección IP de su mainframe. 5. En Puerto, escriba su número de puerto. 6. Elija PROBAR CONEXIÓN. Si la conectividad se ha establecido correctamente, verá un mensaje de confirmación. 7. Seleccione CREAR. Una vez creado el agente, puede ver el estado Conectado en comparación con el agente de almacenamiento de objetos y el agente de mainframe en una nueva ventana que aparece en la tabla.	

Tarea	Descripción	Habilidades requeridas
Cree una política de copia de seguridad o archivado.	1. Elija POLÍTICAS. 2. Elija CREAR POLÍTICA. 3. En la página CREAR UNA NUEVA POLÍTICA, introduzca las especific aciones de su política. **Note** Para obtener más información sobre las especific aciones disponibles, consulte Creación de una nueva política en la documentación de BMC. 4. Seleccione Finalizar. 5. La nueva política ahora aparece en forma de tabla. Para ver esta tabla, seleccione la pestaña POLÍTICAS.	Desarrollador o administr ador de almacenamiento de mainframe

Ejecute la política de copia de seguridad o archivado desde el servidor de administración

Tarea	Descripción	Habilidades requeridas
Ejecute la política de copia de seguridad o archivado.	Ejecute la política de copia de seguridad o archivado de datos que creó anteriorm ente desde el servidor de	Desarrollador o administr ador de almacenamiento de mainframe

Tarea	Descripción	Habilidades requeridas
	administración de forma manual o automática (según una programación). Para ejecutar la política manualmente: 1. En el menú de navegación, elija la pestaña POLÍTICAS. 2. A la derecha de la tabla de la política que desea ejecutar, elija el menú de tres puntos. 3. Seleccione Ejecutar ahora. 4. En la ventana de confirmación emergente, elija SÍ, EJECUTAR LA POLÍTICA AHORA. 5. Una vez ejecutada la política, compruebe el estado de ejecución en la sección de actividad de la política. 6. En la política que se ejecutó, seleccione el menú de tres puntos y, a continuación, seleccione Ver registro de ejecución para ver los registros. 7. Para comprobar que se ha creado la copia de seguridad, compruebe el bucket de S3.	

Tarea	Descripción	Habilidades requeridas
Restaure la copia de seguridad o la política de archivos.	1. En el menú de navegación, elija la pestaña POLÍTICAS. 2. Elija la política en la que desea ejecutar el proceso de restauración. Esto le mostrará todas las actividades de copia de seguridad o archivado que se ejecutaron en el pasado para esa política específica. 3. Para seleccionar las copias de seguridad que desea restaurar, elija la columna Fecha y hora. El nombre del grupo `file/Volume/Storage` muestra los detalles de ejecución de la política. 4. A la derecha de la tabla, seleccione el menú de tres puntos y, a continuación, seleccione RESTAURAR. 5. En la ventana emergente, introduzca el nombre, el volumen y el grupo de almacenamiento de destino y, a continuación, elija RESTAURAR. 6. Introduzca las credenciales de su mainframe y, a continuación, vuelva a seleccionar RESTAURAR.	Desarrollador o administrador de almacenamiento de mainframe

Tarea	Descripción	Habilidades requeridas
	7. Para comprobar que la restauración se ha realizado correctamente, compruebe los registros o el mainframe.	

Ejecute la política de copia de seguridad o archivado desde el mainframe

Tarea	Descripción	Habilidades requeridas
Ejecute la política de copia de seguridad o de archivo mediante M9CLI.	Utilice la M9CLI para realizar procesos de copia de seguridad y restauración desde TSO/E, REXX o incluso JCLs sin configurar reglas en el servidor de administración AMI Cloud de BMC. Uso de TSO/E: Si usa TSO/E, asegúrese de que `M9CLI REXX` esté concatenado a `TSO`. Para hacer una copia de seguridad de un conjunto de datos mediante TSO/E, utilice el comando `TSO M9CLI BACKDSN <DSNAME>`. **Note** Para obtener más información sobre los comandos M9CLI, consulte la referenci	Desarrollador o administrador de almacenamiento de mainframe

Tarea	Descripción	Habilidades requeridas

	a de CLI en la documentación de BMC.
	
	Uso JCLs de:
	
	Para ejecutar la política de copia de seguridad y archivado mediante JCLs, ejecute el `M9CLI` comando.
	
	Uso de operaciones por lotes:
	
	En el siguiente ejemplo se muestra cómo archivar un conjunto de datos mediante la ejecución del comando `M9CLI` por lotes:
	
	`//JOBNAME JOB …`
	`//M9CLI EXEC PGM=IKJEF T01`
	`//STEPLIB DD DISP=SHR, DSN=<MODEL9 LOADLIB>`
	`//SYSEXEC DD DISP=SHR, DSN=<MODEL9 EXEC LIB>`
	`//SYSTSPRT DD SYSOUT=*`
	`//SYSPRINT DD SYSOUT=*`
	`//SYSTSIN DD TSO M9CLI`
	` ARCHIVE`
	` M9CLI ARCHIVE <DSNNAME`
	` OR DSN PATTERN>`
	`/`	

Tarea	Descripción	Habilidades requeridas
Ejecute la política de copia de seguridad o de archivo en el lote JCL.	BMC AMI Cloud proporcio na un ejemplo de rutina JCL llamada M9SAPIJ. Puede personalizar M9SAPIJ para que ejecute una política específica creada en el servidor de administración con un JCL. Este trabajo también puede formar parte de un programador de lotes para ejecutar automáticamente los procesos de copia de seguridad y restauración. El trabajo por lotes espera los siguientes valores obligatorios: • address/host Nombre IP del servidor de administración • Número de puerto • ID de política o nombre de política (que se crea en el servidor de administración) **Note** También puede cambiar otros valores según las instrucci ones del trabajo de ejemplo.	Desarrollador o administr ador de almacenamiento de mainframe

Recursos relacionados

- Modernización del mainframe con AWS (documentación de AWS)
- How Cloud Backup for Mainframes Cuts Costs with Model9 and AWS (blog AWS Partner Network)
- How to Enable Mainframe Data Analytics on AWS Using Model9 (blog AWS Partner Network)
- Recomendaciones de resiliencia de AWS Direct Connect (documentación de AWS)
- Documentación de BMC AMI Cloud (sitio web de BMC)

Cree programas COBOL Db2 mediante y AWS Mainframe Modernization AWS CodeBuild

Luis Gustavo Dantas y Eduardo Zimelewicz, Amazon Web Services

Resumen

> **Note**
>
> AWS Mainframe Modernization El servicio (experiencia de entorno de ejecución gestionado) ya no está abierto a nuevos clientes. Para obtener funcionalidades similares a las AWS Mainframe Modernization de Service (experiencia en entornos de ejecución gestionados), explore AWS Mainframe Modernization Service (experiencia autogestionada). Los clientes existentes pueden seguir utilizando el servicio con normalidad. Para obtener más información, consulte Cambio en la disponibilidad de AWS Mainframe Modernization.

Este patrón explica cómo crear un AWS CodeBuild proyecto sencillo para precompilar y vincular programas de COBOL Db2 mediante las herramientas Replatform. AWS Mainframe Modernization Esto permite el despliegue y la ejecución de estos programas en el entorno de ejecución de Replatform. AWS Mainframe Modernization

COBOL, un lenguaje de programación orientado a los negocios, potencia muchas aplicaciones críticas debido a su fiabilidad y legibilidad. IBM Db2, un sistema de gestión de bases de datos relacionales, gestiona grandes volúmenes de datos de manera eficiente y se integra con los programas COBOL a través de SQL. COBOL y Db2 forman juntos la columna vertebral de las operaciones de misión crítica en sectores como las finanzas y el gobierno, a pesar de la aparición de nuevas tecnologías.

La migración de los componentes COBOL y Db2 del entorno de mainframe a otras plataformas plantea desafíos como la compatibilidad de las plataformas, la complejidad de la integración, la migración de datos y la optimización del rendimiento. El traslado de estos componentes críticos requiere una planificación cuidadosa, experiencia técnica y recursos para garantizar una migración fluida y, al mismo tiempo, mantener la fiabilidad y la funcionalidad.

El AWS Mainframe Modernization servicio proporciona herramientas y recursos para cambiar la plataforma de las aplicaciones y bases de datos de mainframe para que se ejecuten en la AWS infraestructura, como las instancias de Amazon Elastic Compute Cloud EC2 (Amazon). Esto implica

trasladar las cargas de trabajo del mainframe a la nube sin tener que hacer cambios importantes en el código.

El proceso de compilación previo y enlace de Db2 es esencial para optimizar el rendimiento y la fiabilidad de las aplicaciones de bases de datos. La compilación previa transforma las instrucciones de SQL incrustadas en código ejecutable, lo que reduce la sobrecarga del tiempo de ejecución y mejora la eficiencia. El proceso de enlace vincula el código compilado previamente con las estructuras de la base de datos, lo que facilita las rutas de acceso y la optimización de las consultas. Este proceso garantiza la integridad de los datos, mejora la capacidad de respuesta de las aplicaciones y protege contra las vulnerabilidades de seguridad. Las aplicaciones compiladas previamente y enlazadas correctamente minimizan el consumo de recursos, mejoran la escalabilidad y mitigan los riesgos de los ataques de inyección de código SQL.

Requisitos previos y limitaciones

Requisitos previos

- Acceso a una Cuenta de AWS consola de nivel administrativo.
- Un sistema de base de datos IBM Db2, como IBM Db2 for z/OS o Db2 para Linux, Unix y Windows (LUW).
- El software IBM Data Server Client, está disponible para su descarga en el sitio web de IBM. Para obtener más información, consulte los tipos de IBM Data Server Client y Data Server Driver.
- Un programa COBOL Db2 para compilar y vincular. Como alternativa, este patrón proporciona un programa de ejemplo básico que puede utilizar.
- Una nube privada virtual (VPC) conectada a una AWS red privada. Para más información sobre la creación de VPC, consulte la documentación de Amazon Virtual Private Cloud (Amazon VPC).
- Un repositorio de control de código fuente, como GitHub o GitLab.

Limitaciones

- Para conocer AWS CodeBuild las cuotas, consulte Cuotas para AWS CodeBuild.
- Algunas Servicios de AWS no están disponibles en todas Regiones de AWS. Para conocer la disponibilidad de las regiones, consulte Servicios de AWS by Region. Para los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

Pila de tecnología de origen

La pila de orígenes incluye:

- Programas COBOL que utilizan una base de datos Db2 para almacenar datos
- Compilador IBM COBOL y Db2 para precompilador z/OS
- Otras partes de la configuración del mainframe, como el sistema de archivos, el administrador de transacciones y el spool

Pila de tecnología de destino

El enfoque de este patrón funciona con dos opciones: mover datos de Db2 for a Db2 para LUW o z/OS permanecer en Db2 para z/OS. La arquitectura de destino incluye:

- Programas COBOL que utilizan una base de datos Db2 para almacenar datos
- AWS Mainframe Modernization Cambie la plataforma de las herramientas de compilación
- AWS CodeBuild como infraestructura para crear la aplicación
- Otros Nube de AWS recursos, como Amazon Linux

Arquitectura de destino

En el siguiente diagrama se ilustra lo siguiente:

1. El usuario carga su código en un repositorio de control de código fuente, como GitHub o GitLab.
2. AWS CodePipeline nota el cambio y obtiene el código del repositorio.
3. CodePipeline inicia AWS CodeBuild y envía el código.
4. CodeBuild sigue las instrucciones de la `buildspec.yml` plantilla (que se proporcionan en la sección de información adicional) para:
   a. Obtener IBM Data Server Client de un bucket de Amazon Simple Storage Service (Amazon S3).
   b. Instalar y configurar IBM Data Server Client.
   c. Recupere las credenciales de Db2 de AWS Secrets Manager.
   d. Conexión al servidor Db2.

e. Precompilar, compilar y vincular el programa COBOL.

f. Guarde los productos terminados en un depósito de S3 AWS CodeDeploy para su uso.

5. CodePipeline comienza CodeDeploy.
6. CodeDeploy coordina sus agentes, que ya están instalados en los entornos de ejecución. Los agentes obtienen la aplicación de Amazon S3 y la instalan según las instrucciones que se indican en `appspec.yml`.

Para simplificar las cosas y centrarlas en la compilación, las instrucciones de este patrón abarcan los pasos 1 a 4, pero no incluyen la implementación del programa COBOL Db2.

Automatización y escala

Para mayor simplicidad, este patrón describe cómo aprovisionar los recursos de forma manual. Sin embargo, existen numerosas opciones de automatización disponibles, como CloudFormation AWS Cloud Development Kit (AWS CDK), y HashiCorp Terraform, que automatizan estas tareas. Para obtener más información, consulte la documentación de CloudFormation y AWS CDK.

Tools (Herramientas)

Servicios de AWS

- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- AWS CodeDeployautomatiza las implementaciones en instancias, AWS Lambda funciones EC2 o servicios de Amazon Elastic Container Service (Amazon ECS) o en instancias locales.
- AWS CodePipeline permite diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software y automatizar los pasos necesarios para lanzar los cambios en el software de manera continua.
- AWS Mainframe Modernizationproporciona herramientas y recursos que le ayudan a planificar e implementar la migración y la modernización de los mainframes a AWS entornos de tiempo de ejecución gestionados.

Otras herramientas

- Imagen de Amazon ECR para las herramientas de AWS Mainframe Modernization Replatform. Para compilar una aplicación COBOL, tendrá que empezar CodeBuild con una imagen de Amazon

Elastic Container Registry (Amazon ECR) que contenga las herramientas de Replatform: AWS Mainframe Modernization

`673918848628.dkr.ecr.<your-region>.amazonaws.com/m2-enterprise-build-tools:9.0.7.R1`

Para obtener más información sobre la imagen de ECR disponible, consulte el tutorial de la Guía del usuario de AWS Mainframe Modernization .

- El software IBM Data Server Client es esencial para precompilar y vincular los programas COBOL Db2. CodeBuild Actúa como puente entre el compilador COBOL y Db2.

Prácticas recomendadas

- No todos los programas COBOL utilizan Db2 como capa de persistencia de datos. Asegúrese de que las directivas de compilación para acceder a Db2 se apliquen únicamente a los programas COBOL diseñados específicamente para interactuar con Db2. Implemente una lógica para distinguir entre los programas COBOL Db2 y los programas COBOL que no utilizan Db2.
- Se recomienda evitar compilar programas que no hayan sido modificados. Implemente un proceso para identificar qué programas deben compilarse.

Epics

Creación de la infraestructura en la nube

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3 para alojar IBM Data Server Client y los artefactos de canalizac ión.	Debe configurar un bucket de S3 para (a) cargar IBM Data Server Client, (b) almacenar el código del repositorio y (c) almacenar los resultados del proceso de creación. 1. Inicie sesión en la Consola de administración de AWSconsola Amazon S3 y ábrala.	AWS general

Tarea	Descripción	Habilidades requeridas
	2. Utilice un bucket de S3 existente, o bien cree un bucket nuevo. Anote el nombre de recurso de Amazon (ARN) del bucket para utilizarlo más adelante. Para ver más maneras de crear un bucket de S3, consulte la documentación de Amazon S3.	

Tarea	Descripción	Habilidades requeridas
Cargue IBM Data Server Client en el bucket de S3.	1. En la consola de Amazon S3, elija el bucket que quiere abrir. 2. Elija Crear carpeta, especifique su nombre como cliente y, a continuación, elija Crear carpeta. 3. Abra la carpeta del cliente, seleccione Cargar y Añadir archivos. 4. Elija el archivo IBM Data Server Client que descargó previamente del sitio web de IBM a su sistema de archivos local. El nombre del archivo debe ser similar a `v11.5.8_linuxx64_client.tar.gz` o `v11.5.9_linuxx64_client.tar.gz`. 5. Seleccione Abrir, Cargar y espere a que se complete la carga. 6. En la pestaña Archivos y carpetas, elija Data Server Client y anote su URI de S3.	AWS general

Tarea	Descripción	Habilidades requeridas
Cree un AWS Secrets Manager secreto para sus credenciales de Db2.	Para crear un secreto para almacenar sus DB2 credencia les de forma segura: 1. En la consolade Secrets Manager, seleccione Almacenar un nuevo secreto. 2. En el panel Elegir un tipo de secreto, elija Otro tipo de secreto y Texto sin formato. 3. En el cuadro de texto sin formato, escriba sus credenciales de Db2 mediante la siguiente estructura JSON. `{ "username": "<your-db2-user-name>", "password": "<your-db2-password>", "db2node": "db2dev", "db2host": "<your-db2-hostname-or-IP>", "db2port": <your-db2-port>, "db2name": "<your-db2-location>", "qualifier": "<your-db2-qualifier>"`	AWS general

Tarea	Descripción	Habilidades requeridas
	`}` 4. Seleccione Siguiente y asigne al secreto un nombre como `dev-db2-cred` . 5. Seleccione Siguiente, Siguiente y Almacenar. Para más información sobre la creación de secretos, consulte la documentación de Secrets Manager.	

Tarea	Descripción	Habilidades requeridas
Compruebe que Db2 sea accesible desde la subred de la VPC.	AWS CodeBuild necesita una conexión al servidor Db2 para que el cliente del servidor de datos pueda realizar operaciones de precompil ación y enlace. Asegúrese de que CodeBuild puede acceder al servidor Db2 a través de una conexión segura. 1. Abra la Consola de Amazon VPC. 2. En el panel de navegació n, elija Subredes y anote las IDs subredes privadas en IPv4 CIDRslas que CodeBuild funcionarán. 3. Actualice la configuración actual de control de acceso a la red de su sistema Db2 mediante una regla de entrada. Esta regla debería permitir el acceso TCP personalizado al puerto Db2 exclusivamente desde la subred CIDRs asociada al proyecto. CodeBuild	Administrador de red, AWS general

Creación de los artefactos de la aplicación

Tarea	Descripción	Habilidades requeridas
Cree el activo COBOL Db2.	1. Si desea utilizar un ejemplo sencillo de COBOL Db2,	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	guarde el siguiente código fuente como `CDB2SMP.cbl` . O bien, puede sustituir este ejemplo por un programa que ya tenga. `IDENTIFICATION DIVISION. PROGRAM-ID. CDB2SMP. DATA DIVISION. WORKING-STORAGE SECTION. 01 WS-NAME PIC X(100). PROCEDURE DIVISION. EXEC SQL SELECT NAME INTO :WS-NAME FROM SYSIBM.SYSTABLES END-EXEC GOBACK.` 2. Confirme los cambios y envíe el proyecto a su repositorio.	

Tarea	Descripción	Habilidades requeridas
Creación del archivo `buildspec.yml` .	1. Genere el archivo `buildspec.yml` según el ejemplo que se proporciona en la sección Información adicional. 2. Confirme los cambios y envíe el proyecto a su repositorio.	AWS DevOps
Conecta tu repositorio a CodePipeline.	1. Abra la consola de herramientas para desarrolladores de AWS. 2. En el panel de navegación, seleccione Configuración, conexiones. 3. Siga las instrucciones de la documentación de la consola de Herramientas para desarrolladores y elija el proveedor de código fuente que prefiera. Necesitará el nombre del recurso de Amazon (ARN) para la conexión cuando cree la política AWS Identity and Access Management (IAM) para un paso CodePipeline posterior.	AWS DevOps

Configuración de permisos

Tarea	Descripción	Habilidades requeridas
Cree una política de IAM para CodeBuild.	El CodeBuild proyecto requiere acceso a algunos recursos, como Secrets Manager y Amazon S3. Para configurar los permisos necesarios: 1. Abra la consola de IAM. 2. En el panel de navegación, elija Políticas, Crear política y, a continuación, seleccione el CodeBuild servicio. 3. Cambie el formato de Visual a JSON y copie la CodeBuild política que se proporciona en la sección Información adicional en el campo del editor de políticas. 4. Asigne un nombre a esta política y guárdela para consultarla en el siguiente paso. Para obtener más información sobre la creación de políticas de IAM, consulte la documentación de IAM.	AWS general
Cree un rol de IAM para CodeBuild.	Para que las políticas de seguridad estén disponibles	AWS general

Tarea	Descripción	Habilidades requeridas
	CodeBuild, debe configurar un rol de IAM. Para crear el rol: 1. En el panel de navegación de la consola de IAM, seleccione Roles, Crear rol. 3. En Tipo de entidad de confianza, mantenga la selección predeterminada de Servicio de AWS. 4. En Caso de uso, seleccione el CodeBuild servicio y, a continuación, elija Siguiente. 4. En la lista de políticas de IAM disponibles, busque la política para la que creó y CodeBuild, a continuación, seleccione Siguiente para asociarla al rol. 5. Especifique un nombre para el rol y elija Crear rol para guardarlo para consultarlo en el futuro CodeBuild. Para obtener más información sobre la creación de un rol de IAM para un Servicio de AWS, consulte la documentación de IAM.	

Tarea	Descripción	Habilidades requeridas
Cree una política de IAM para. CodePipeline	La AWS CodePipeline canalización requiere acceso a algunos recursos, incluidos su repositorio de código y Amazon S3. Repita los pasos indicados anteriormente CodeBuild para crear una política de IAM CodePipeline (en el paso 2, elija en CodePipelinelugar de CodeBuild).	AWS DevOps

Tarea	Descripción	Habilidades requeridas

Cree un rol de IAM para CodePipeline.	Para que las políticas de seguridad estén disponibles CodePipeline, debe configurar un rol de IAM.
	
	Para crear el rol:
	
	1. En la consola de IAM, seleccione Roles y, a continuación, Crear rol.
	2. En Tipo de entidad de confianza, elija Política de confianza personalizada.
	
	Aparecerá una política con un elemento `Principal` vacío.
	3. En la línea `Principal` , entre las llaves, añada lo siguiente:
	
	`"Service": "codepipeline.amazonaws.com"`
	
	La política de confianza tendrá el siguiente aspecto:
	
	`{ "Version": "2012-10-17", "Statement": [ { "Sid": "Statement1", "Effect": "Allow", "Principal": {`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	<pre>"Service": "codepipeline.amazonaws.com" }, "Action": "sts:AssumeRole" }] }</pre> 4. Elija Siguiente. 5. En la lista de políticas de IAM disponibles, busque la política para la que creó y CodePipeline, a continuación, seleccione Siguiente para asociarla a la función. 6. Especifique un nombre para el rol y elija Crear rol para guardarlo para consultarlo en el futuro CodePipeline.	

Compilación y enlace del programa COBOL Db2

Tarea	Descripción	Habilidades requeridas
Cree una CodePipeline canalización y un CodeBuild proyecto.	Para crear una CodePipeline canalización y el CodeBuild proyecto que compila y enlaza el programa COBOL Db2: 1. Abre la CodePipeline consola y selecciona Crear canalización, Construir canalización personalizada.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	2. Escriba un nombre para la canalización. 3. En Función de servicio, elija Función de servicio existente y, a continuación, especifique el ARN de la función de IAM para la que la creó. CodePipeline 4. Expanda la configura ción avanzada, elija una ubicación personalizada, elija el bucket de S3 que creó anteriormente y, a continuación, elija Siguiente . 5. En el proveedor de origen, seleccione su proveedor de origen externo y proporcio ne la información relevante del proveedor: a. En Conexión, seleccione la conexión que se creó para el proveedor de origen. b. En Nombre del repositor io, elija un repositorio. c. En la rama predeterm inada, seleccione la rama que almacena el programa COBOL y `buildspec.yml` . d. Elija Siguiente.	

Tarea	Descripción	Habilidades requeridas
	6. En Proveedor de compilación, elija Otros proveedores de compilación y, a continuación, AWS CodeBuild. 7. En Nombre del proyecto, seleccione Crear proyecto. La consola muestra una CodeBuild ventana en la que puede crear un proyecto de compilación. En esta ventana: a. Escriba un nombre para el proyecto. b. En Environment image (Imagen de entorno), elija Custom image (Imagen personalizada). c. En Tipo de entorno, elija Contenedor de Linux. d. En Cuenta de ECR, elija Mi cuenta de ECR. e. En la URI del repositorio Amazon ECR, introduzca `673918848628.dkr.ecr.<your-region>.amazonaws.com/m2-enterprise-build-tools:8.0.9.R1` .	

Tarea	Descripción	Habilidades requeridas
	f. En Función de servicio, elija Función de servicio existente y seleccione la función para la que la creó CodeBuild. g. Amplíe la sección Configuración adicional y, a continuación, elija la VPC, las subredes privadas y el grupo de seguridad para este proyecto. h. En Especificaciones de la compilación, elija Utilizar un archivo de especificación de compilación. i. Al final de la ventana, selecciona Continuar aCodePipeline. La CodeBuild ventana se cerrará para que puedas volver a la CodePipeline consola. 8. De vuelta a la CodePipel ine consola, selecciona Siguiente. 9. En el panel Añadir fase de implementación, seleccion e Omitir fase de implement ación y confirme la opción.	

Tarea	Descripción	Habilidades requeridas
	10. Revise los parámetros de la canalización y, a continuación, elija Crear canalización.	
Revise la salida.	Compruebe el éxito de la compilación revisando los registros de CodePipeline compilación.	AWS DevOps

Tarea	Descripción	Habilidades requeridas

Compruebe los resultados en Db2.	Compruebe la versión del paquete en la tabla SYSPLAN.
	
	`select CAST(NAME AS VARCHAR(10)) as name, VALIDATE, LAST_BIND_TIME, LASTUSED, CAST(PKGVERSION AS VARCHAR(10)) as PKGVERSION from SYSIBM.SYSPLAN where NAME = 'CDB2SMP' order by LAST_BIND_TIME desc`
	
	La versión debe coincidir con el ID de CodeBuild compilación, que se muestra `CDB2SMP` en nuestro ejemplo:
	
	`NAME VALIDATE LAST_BIND_TIME LASTUSED PKGVERSION ---------- -------- ------------------ -------- ---------- CDB2SMP B 2024-05-18-11.53.11.503738 01/01/0001 19`	

Resolución de problemas

Problema	Solución
Ocasionalmente, la AWS consola cambia de región cuando te mueves de un servicio a otro.	Asegúrese de verificar lo seleccionado Región de AWS cada vez que cambie de un servicio a otro. El Región de AWS selector está en la esquina superior derecha de la ventana de la consola.
Puede resultar difícil identificar los problemas de conectividad de Db2 desde. CodeBuild	Para solucionar problemas de conectividad, añada el siguiente comando de DB2 conexión al `buildspec.yml` archivo. Esta adición lo ayudará a depurar y resolver los problemas de conectividad. `db2 connect to $DB_NAME user $DB2USER using $DB2PASS`
En ocasiones, el panel de roles de la consola de IAM no muestra inmediatamente la política de IAM que ha creado.	Si se produce un retraso, actualice la pantalla para mostrar la información más reciente.

Recursos relacionados

Documentación de IBM

- Tipos de controladores y IBM Data Server Client
- Descarga de tipos de controladores y IBM Data Server Client

AWS documentación

- Guía del usuario de Amazon S3
- AWS CodeBuild Guía del usuario
- AWS Mainframe Modernization Guía del usuario

- AWS Secrets Manager Guía del usuario
- AWS CodePipeline Guía del usuario
- AWS CodeDeploy Guía del usuario

Información adicional

CodeBuild política

Sustituya los marcadores de posición <RegionID>, <AccountID>, <SubnetARN>, <BucketARN> y <DB2CredSecretARN> por sus propios valores.

```
{"Version": "2012-10-17",
    "Statement": [
        {"Action": "ecr:GetAuthorizationToken", "Effect": "Allow", "Resource": "*" },
        {"Action": ["ecr:GetDownloadUrlForLayer", "ecr:BatchGetImage",
                    "ecr:BatchCheckLayerAvailability"],
         "Effect": "Allow",
         "Resource": "arn:aws:ecr:*:673918848628:repository/m2-enterprise-build-
tools"},
        {"Action": "s3:PutObject", "Effect": "Allow", "Resource": "arn:aws:s3:::aws-m2-
repo-*/*"},
        {"Action": ["logs:PutLogEvents", "logs:CreateLogStream",
 "logs:CreateLogGroup"],
         "Effect": "Allow", "Resource": "arn:aws:logs:<RegionId>:<AccountId>:*"},
        {"Action": ["ec2:DescribeVpcs", "ec2:DescribeSubnets",
                    "ec2:DescribeSecurityGroups", "ec2:DescribeNetworkInterfaces",
                    "ec2:DescribeDhcpOptions", "ec2:DeleteNetworkInterface",
                    "ec2:CreateNetworkInterface"],
         "Effect": "Allow", "Resource": "*"},
        {"Action": "ec2:CreateNetworkInterfacePermission",
         "Effect": "Allow", "Resource": ["<SubnetARN>"]},
        {"Action": "s3:*", "Effect": "Allow", "Resource": ["<BucketARN>/
*","<BucketARN>"]},
        {"Action": "secretsmanager:GetSecretValue",
         "Effect": "Allow", "Resource": "<DB2CredSecretARN>"}
    ]
}
```

CodePipeline política

Sustituya los marcadores de posición <BucketARN> y <ConnectionARN> por sus propios valores.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {"Action": ["s3:List*", "s3:GetObjectVersion", "s3:GetObject",
 "s3:GetBucketVersioning" ],
        "Effect": "Allow",
        "Resource": ["<BucketARN>/*", "<BucketARN>"]},
        {"Action": ["codebuild:StartBuild", "codebuild:BatchGetBuilds"],
         "Effect": "Allow", "Resource": "*"},
        {"Action": ["codestar-connections:UseConnection"],
         "Effect": "Allow", "Resource": "<ConnectionARN>"}
        ]
}
```

`buildspec.yml`

Sustituya el marcador de posición <your-bucket-name> con el nombre real de su bucket de S3.

```
version: 0.2
phases:
  pre_build:
    commands:
      - /var/microfocuslicensing/bin/mfcesd -no > /var/microfocuslicensing/logs/
mfcesd_startup.log 2>&1 &
      - |
        mkdir $CODEBUILD_SRC_DIR/db2client
        aws s3 cp s3://<your-bucket-name>/v11.5.8_linuxx64_client.tar.gz
 $CODEBUILD_SRC_DIR/db2client/ >> /dev/null 2>&1
        tar -xf $CODEBUILD_SRC_DIR/db2client/v11.5.8_linuxx64_client.tar.gz -C
 $CODEBUILD_SRC_DIR/db2client/
        cd $CODEBUILD_SRC_DIR/db2client/
        ./client/db2_install -f sysreq -y -b /opt/ibm/db2/V11.5 >> /dev/null 2>&1

        useradd db2cli
        /opt/ibm/db2/V11.5/instance/db2icrt -s client -u db2cli db2cli
        DB2CRED=$(aws secretsmanager get-secret-value --secret-id dev-db2-cred | jq -r
 '.SecretString | fromjson')
        read -r DB2USER DB2PASS DB_NODE DB_HOST DB_PORT DB_NAME DB_QUAL <<<$(echo
 $DB2CRED | jq -r
 '.username, .password, .db2node, .db2host, .db2port, .db2name, .qualifier')
        . /home/db2cli/sqllib/db2profile
        db2 catalog tcpip node $DB_NODE remote $DB_HOST server $DB_PORT
        db2 catalog db $DB_NAME as $DB_NAME at node $DB_NODE authentication server
```

```
  build:
    commands:
      - |
        revision=$CODEBUILD_SRC_DIR/loadlib
        mkdir -p $revision; cd $revision
        . /opt/microfocus/EnterpriseDeveloper/bin/cobsetenv
        cob -zU $CODEBUILD_SRC_DIR/CDB2SMP.cbl -C "DB2(DB==${DB_NAME} PASS==${DB2USER}.
${DB2PASS} VERSION==${CODEBUILD_BUILD_NUMBER} COLLECTION==DB2AWSDB"
artifacts:
  files:
    - "**/*"
  base-directory: $revision
```

Cree un PAC de servidor empresarial Micro Focus con Amazon EC2 Auto Scaling y Systems Manager

Kevin Yung y Krithika Palani Selvam, Amazon Web Services

Peter Woods, ninguno

Abraham Rondon, Micro Focus

Resumen

Este patrón introduce una arquitectura escalable para aplicaciones de mainframe que utilizan Micro Focus Enterprise Server en Scale-Out Performance and Availability Cluster (PAC) y un grupo de EC2 Auto Scaling de Amazon Elastic Compute Cloud (Amazon) en Amazon Web Services ().AWS La solución está totalmente automatizada con AWS Systems Manager los ganchos de ciclo de vida EC2 de Amazon Auto Scaling. Al usar este patrón, puede configurar sus aplicaciones de mainframe en línea y por lotes para lograr una alta resiliencia escalando vertical y horizontalmente de forma automática en función de sus demandas de capacidad.

> **Note**
>
> Este patrón se probó con la versión 6.0 de Micro Focus Enterprise Server. Para la versión 8, consulte Configurar Micro Focus Runtime (en Amazon EC2).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Software y licencia de Micro Focus Enterprise Server. Para obtener más información, contacte con el departamento de ventas de Micro Focus.
- Comprender el concepto de reconstrucción y entrega de una aplicación de mainframe a ejecutar en Micro Focus Enterprise Server. Para obtener información general, consulte Hoja de datos de Micro Focus Enterprise Server.
- Comprender los conceptos de clúster de rendimiento y disponibilidad escalable horizontalmente de Micro Focus Enterprise Server. Para más información, consulte la documentación de Micro Focus Enterprise Server.

- Comprensión del concepto general de aplicación de mainframe DevOps con integración continua (CI). Para ver un patrón de orientación AWS prescriptiva desarrollado por AWS Micro Focus, consulte Modernización de mainframe: puesta DevOps en marcha AWS con Micro Focus.

> **Note**
>
> Este patrón se probó con la versión 6 de Micro Focus Enterprise Server. Para la versión 8, consulte Configurar Micro Focus Runtime (en Amazon EC2).

Limitaciones

- Para obtener una lista de las plataformas compatibles con Micro Focus Enterprise Server, consulte la hoja de datos de Micro Focus Enterprise Server.
- Los scripts y las pruebas utilizados en este patrón se basan en Amazon EC2 Windows Server 2019; no se probaron otras versiones y sistemas operativos de Windows Server para este patrón.
- El patrón se basa en Micro Focus Enterprise Server 6.0 para Windows; no se han probado versiones anteriores o posteriores para desarrollar este patrón.

Versiones de producto

- Micro Focus Enterprise Server 6.0
- Windows Server 2019

Arquitectura

En un entorno de mainframe convencional, debe aprovisionar el hardware para alojar las aplicaciones y los datos corporativos. Para hacer frente a los picos de demanda estacionales, mensuales, trimestrales o incluso imprevistos o sin precedentes, los usuarios de mainframe deben escalar horizontalmente sus capacidades adquiriendo capacidad de almacenamiento y procesamiento adicionales. El aumento de la cantidad de recursos de almacenamiento y capacidad de cómputo mejora el rendimiento general, pero el escalado no es lineal.

Este no es el caso cuando comienza a adoptar un modelo de consumo bajo demanda en AWS mediante los servidores Amazon EC2 Auto Scaling y Micro Focus Enterprise. En las siguientes secciones se explica en detalle cómo crear una arquitectura de aplicaciones de mainframe escalable

y totalmente automatizada mediante el clúster de rendimiento y disponibilidad escalable (PAC) de Micro Focus Enterprise Server con un grupo de Amazon EC2 Auto Scaling.

Arquitectura de escalado automático de Micro Focus Enterprise Server

En primer lugar, es importante conocer los conceptos básicos de Micro Focus Enterprise Server. Este entorno proporciona un entorno de implementación x86 compatible con mainframe para aplicaciones que tradicionalmente se ejecutaban en el mainframe de IBM. Ofrece ejecuciones en línea y por lotes, así como un entorno de transacciones compatible con:

- IBM COBOL
- IBM PL/I
- Trabajos por lotes en IBM JCL
- Transacciones de IBM CICS e IMS TM
- Servicios web
- Utilidades de procesamiento por lotes comunes, incluida SORT

Micro Focus Enterprise Server permite la ejecución de aplicaciones de mainframe con cambios mínimos. Las cargas de trabajo de mainframe existentes se pueden trasladar a plataformas x86 y modernizarse para aprovechar las extensiones nativas en la nube de AWS y así expandirse rápidamente a nuevos mercados o geografías.

El patrón AWS Prescriptive Guidance Modernization: DevOps on AWS with Micro Focus introdujo la arquitectura para acelerar el desarrollo y las pruebas de aplicaciones de mainframe en AWS mediante Micro Focus Enterprise Developer y Enterprise Test Server con AWS y AWS CodePipeline . CodeBuild Este patrón se centra en la implementación de aplicaciones de mainframe en el entorno de producción de AWS para lograr una alta disponibilidad y resiliencia.

En un entorno de producción de mainframe, es posible que haya configurado IBM Parallel Sysplex en el mainframe para lograr un alto rendimiento y una alta disponibilidad. Para crear una arquitectura escalable similar a Sysplex, Micro Focus introdujo el clúster de rendimiento y disponibilidad (PAC) en Enterprise Server. PACs admiten la implementación de aplicaciones de mainframe en múltiples regiones de Enterprise Server administradas como una sola imagen y escaladas en instancias de Amazon EC2 . PACs también permiten un rendimiento predecible de las aplicaciones y del sistema bajo demanda.

En un PAC, varias instancias de Enterprise Server funcionan juntas como una sola entidad lógica. Por lo tanto, el fallo de una instancia de Enterprise Server no interrumpirá la continuidad del negocio,

ya que la capacidad se comparte con otras regiones, mientras que las nuevas instancias se inician automáticamente con la funcionalidad estándar del sector, como un grupo de Amazon EC2 Auto Scaling. Esto elimina los puntos únicos de fallo y mejora la resiliencia ante problemas de hardware, red y aplicaciones. Las instancias de Enterprise Server ampliadas se pueden operar y administrar mediante la administración web común de servidores empresariales (ESCWA) APIs, lo que simplifica el mantenimiento operativo y la facilidad de servicio de los servidores empresariales.

> **Note**
>
> Micro Focus recomienda que el clúster de rendimiento y disponibilidad (PAC) esté formado por, al menos, tres regiones de Enterprise Server. Así, la disponibilidad no se verá comprometida en caso de que una región de Enterprise Server falle o requiera mantenimiento.

La configuración del PAC requiere un servicio de administración de base de datos relacional (RDBMS) compatible para administrar la base de datos regional, una base de datos interregional y las bases de datos de almacenes de datos opcionales. Es necesario usar una base de datos de almacén de datos para gestionar los archivos de Virtual Storage Access Method (VSAM). La compatibilidad con el gestor de archivos de base de datos de Micro Focus mejora la disponibilidad y la escalabilidad. Entre las opciones admitidas se incluyen las siguientes: RDBMSs

- Microsoft SQL Server 2009 o posterior
- PostgreSQL 10.x, incluida la edición compatible con PostgreSQL de Amazon Aurora
- DB2 10.4 y versiones posteriores

Para obtener más información sobre los requisitos de RDBMS y PAC compatibles, consulte Micro Focus Enterprise Server: requisitos previos y Micro Focus Enterprise Server: configuración de PAC recomendada.

El siguiente diagrama muestra una configuración de arquitectura de AWS típica para un PAC de Micro Focus.

component	Descripción

1	Grupo de escalado automático de instancias de Enterprise Server	Configure un grupo de escalado automático implementado con las instancias de Enterpris e Server en un PAC. Las CloudWatch alarmas de Amazon pueden aumentar o activar el número de instancia s mediante CloudWatch métricas.
2	Grupo de escalado automático de instancias ESCWA de Enterprise Server	Configure un grupo de escalado automático implementado con Enterpris e Server Common Web Administration (ESCWA). La CESPAO se encarga de la gestión de clústeres . APIs Los servidores de ESCWA actúan como plano de control para añadir o eliminar Enterprise Server e iniciar o detener las regiones de Enterprise Server en el PAC durante los eventos de escalado automático de la instancia de Enterprise Server. Como la instancia de ESCWA se usa únicamente para la gestión del PAC, su patrón de tráfico es predecibl e. y su escalado. automátic o (el requisito de capacidad deseado se puede establecer en 1).

3	Instancia de Amazon Aurora en una configuración Multi-AZ	Configure un sistema de administración de base de datos relacional (RDBMS) para alojar los archivos de datos de los usuarios y del sistema y compartirlos entre las instancias de Enterprise Server.
4	Instancia y réplica de Amazon ElastiCache (Redis OSS)	Configure una instancia principal ElastiCache (Redis OSS) y al menos una réplica para alojar los datos de los usuarios y actuar como un repositorio escalable (SOR) para las instancias de Enterprise Server. Puede configurar uno o más repositorios escalables horizontalmente para almacenar tipos específicos de datos de usuario. Enterprise Server emplea una base de datos NoSQL de Redis como SOR, requisito fundamental para mantener la integridad del PAC.
5	Equilibrador de carga de red	Configure un equilibrador de carga que proporcione un nombre de host para que las aplicaciones se conecten a los servicios proporcionados por las instancias de Enterprise Server (por ejemplo, acceder a la aplicación a través de un emulador 3270).

Estos componentes conforman el requisito mínimo para un clúster PAC de Micro Focus Enterprise Server. La siguiente sección trata sobre la automatización de la administración de clústeres.

Uso de Automatización de AWS Systems Manager para escalar

Una vez implementado el clúster PAC en AWS, el PAC se administra a través de Enterprise Server Common Web Administration (ESCWA) APIs.

Para automatizar las tareas de administración de clústeres durante los eventos de escalado automático, puede utilizar los manuales de automatización de Systems Manager y Amazon EC2 Auto Scaling with Amazon EventBridge. La arquitectura de estas automatizaciones se muestra en el siguiente diagrama.

	Componente	Descripción
1	Enlace de ciclo de vida de escalado automático	Configura enlaces de ciclo de vida de escalado automátic o y envía notificaciones a Amazon EventBridge cuando se lancen nuevas instancia s y las instancias existente s finalicen en el grupo de escalado automático.
2	Amazon EventBridge	Configure una EventBridge regla de Amazon para enrutar los eventos de escalado automático a los objetivos del runbook de Systems Manager Automation.
3	Manuales de procedimientos de Automation	Configure los manuales de automatización de Systems Manager para ejecutar PowerShell scripts de Windows e invoque a la CESPAO APIs para administr

		ar el PAC. Para ver más ejemplos, consulte la sección Información adicional.
4	Instancia ESCWA de Enterprise Server en un grupo de escalado automático	Configurar una instancia ESCWA de Enterprise Server en un grupo de escalado automático. La instancia de la CESPAO permite APIs gestionar el PAC.

Tools (Herramientas)

- Micro Focus Enterprise Server: Micro Focus Enterprise Server proporciona el entorno de ejecución para aplicaciones creadas con cualquier variante de entorno de desarrollo integrado (IDE) de Enterprise Developer.
- Amazon EC2 Auto Scaling: Amazon EC2 Auto Scaling le ayuda a garantizar que dispone del número correcto de EC2 instancias de Amazon disponibles para gestionar la carga de su aplicación. Puede crear colecciones de EC2 instancias, denominadas grupos de Auto Scaling, y especificar un número mínimo y máximo de instancias.
- Amazon ElastiCache (Redis OSS): Amazon ElastiCache es un servicio web para configurar, administrar y escalar un almacén de datos en memoria distribuido o un entorno de caché en la nube. Proporciona una capacidad de almacenamiento en caché de alto rendimiento, escalable y rentable.
- Amazon RDS: Amazon Relational Database Service (Amazon RDS) es un servicio web que facilita la configuración, el funcionamiento y el escalado de una base de datos relacional en la nube de AWS. Proporciona una capacidad rentable y de tamaño ajustable para una base de datos relacional y se ocupa de las tareas comunes de administración de bases de datos.
- AWS Systems Manager: AWS Systems Manager es un servicio que puede utilizar para ver y controlar su infraestructura en AWS. Mediante la consola de Systems Manager, puede ver los datos operativos de varios servicios de AWS y automatizar las tareas operativas en sus recursos de AWS. Systems Manager le ayuda a mantener la seguridad y la conformidad mediante el análisis de sus instancias administradas y el informe sobre las infracciones de las políticas que detecte o la toma de medidas correctivas con respecto a estas.

Epics

Crear una instancia de Amazon Aurora

Tarea	Descripción	Habilidades requeridas
Cree una CloudFormation plantilla de AWS para una instancia de Amazon Aurora.	Utilice el fragmento de código de ejemplo de AWS para crear una CloudFormation plantilla que cree una instancia de Amazon Aurora compatible con PostgreSQL Edition.	Arquitecto de la nube
Implemente una CloudFormation pila para crear la instancia de Amazon Aurora.	Use la CloudFormation plantilla para crear una instancia compatible con Aurora PostgreSQL que tenga habilitada la replicación Multi-AZ para las cargas de trabajo de producción.	Arquitecto de la nube
Configure los ajustes de conexión a la base de datos para Enterprise Server.	Siga las instrucciones de la documentación de Micro Focus para preparar las cadenas de conexión y la configuración de la base de datos para Micro Focus Enterprise Server.	DevOps Ingeniero de datos, ingeniero

Crear un ElastiCache clúster de Amazon para la instancia de Redis

Tarea	Descripción	Habilidades requeridas
Crea una CloudFormation plantilla para el ElastiCache clúster de Amazon para la instancia de Redis.	Utilice el fragmento de código de ejemplo de AWS para crear una CloudFormation plantilla que cree un ElastiCac	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	he clúster de Amazon para la instancia de Redis.	
Implemente la CloudFormation pila para crear un ElastiCac he clúster de Amazon para la instancia de Redis.	Cree el ElastiCache clúster de Amazon para la instancia de Redis que tiene habilitad a la replicación Multi-AZ para las cargas de trabajo de producción.	Arquitecto de la nube
Configure los ajustes de conexión de Enterprise Server PSOR.	Siga las instrucciones de la documentación de Micro Focus para preparar la configuración de la conexión del repositorio Scale-Out PAC (PSOR) para Micro Focus Enterprise Server PAC.	DevOps ingeniero

Cree un grupo de escalado automático de ESCWA para Micro Focus Enterprise Server

Tarea	Descripción	Habilidades requeridas
Cree una AMI de Micro Focus Enterprise Server.	Cree una instancia de Amazon EC2 Windows Server e instale el binario de Micro Focus Enterprise Server en la EC2 instancia. Cree una Amazon Machine Image (AMI) de la EC2 instancia. Para más información, consulte la documentación de instalación de Enterprise Server.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Cree una CloudFormation plantilla para Enterprise Server ESCWA.	Use el fragmento de código de ejemplo de AWS para crear una plantilla de una pila personalizada de Enterprise Server ESCWA en un grupo de escalado automático.	Arquitecto de la nube
Implemente la CloudFormation pila para crear un grupo de EC2 escalado de Amazon para Enterprise Server ESCWA.	Utilice la CloudFormation plantilla para implementar el grupo de escalado automático con la AMI de la CESPAO de Micro Focus Enterprise Server creada en la historia anterior.	Arquitecto de la nube

Cree de un manual de procedimientos de Automatización de AWS Systems Manager

Tarea	Descripción	Habilidades requeridas
Cree una CloudFormation plantilla para un manual de automatización de Systems Manager.	Utilice los fragmentos de código de ejemplo de la sección de información adicional para crear una CloudFormation plantilla que cree un manual de automatización de Systems Manager para automatizar la creación de PAC, la ampliación de Enterprise Server y la ampliación horizontal de Enterprise Server.	Arquitecto de la nube
Implemente la CloudFormation pila que contiene el manual de ejecución de Systems Manager Automation.	Utilice la CloudFormation plantilla para implementar una pila que contenga el manual de automatización	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	para la creación de PAC, el escalado de Enterprise Server y el escalado de Enterprise Server.	

Cree un grupo de escalado automático para Micro Focus Enterprise Server

Tarea	Descripción	Habilidades requeridas
Cree una CloudFormation plantilla para configurar un grupo de escalado automátic o para Micro Focus Enterprise Server.	Utilice el fragmento de código de ejemplo de AWS para crear una CloudFormation plantilla que cree un grupo de escalado automático. Esta plantilla reutilizará la misma AMI que se creó para la instancia de Micro Focus Enterprise Server ESCWA. A continuación, utilice un fragmento de código de ejemplo de AWS para crear el evento del ciclo de vida de escalado automático y configure Amazon EventBrid ge para filtrar los eventos de escalado horizontal y horizontal en la misma plantilla . CloudFormation	Arquitecto de la nube
Implemente la CloudFormation pila para el grupo de escalado automático de los servidores empresariales Micro Focus.	Implemente la CloudFormation pila que contiene el grupo de escalado automático para los servidores Micro Focus Enterprise.	Arquitecto de la nube

Recursos relacionados

- Clúster de rendimiento y disponibilidad (PAC) de Micro Focus Enterprise Server
- Ganchos del ciclo de vida de Amazon EC2 Auto Scaling
- Ejecutar automatizaciones con activadores mediante EventBridge

Información adicional

Los siguientes escenarios deben automatizarse para reducir o escalar horizontalmente los clústeres de PAC.

Automatización para iniciar o recrear un PAC

Al inicio de un clúster de PAC, Enterprise Server requiere que la CESPAO lo invoque APIs para crear una configuración de PAC. Esta acción inicia y agrega regiones de Enterprise Server al PAC. Para crear o volver a crear un PAC, siga estos pasos:

1. Configure un repositorio escalable horizontalmente de PAC (PSOR) en ESCWA con un nombre determinado.

```
POST /server/v1/config/groups/sors
```

2. Cree un PAC con un nombre determinado y adjúntele el PSOR.

```
POST /server/v1/config/groups/pacs
```

3. Configure la base de datos regional y la base de datos interregional si es la primera vez que configura un PAC.

> **Note**
>
> En este paso se usan consultas SQL y la herramienta dbhfhadmin de la línea de comandos de Micro Focus Enterprise Suite para crear la base de datos e importar los datos iniciales.

4. Instale la definición de PAC en las regiones de Enterprise Server.

```
POST /server/v1/config/mfds
POST /native/v1/config/groups/pacs/${pac_uid}/install
```

5. Inicie las regiones de Enterprise Server en el PAC.

```
POST /native/v1/regions/${host_ip}/${port}/${region_name}/start
```

Los pasos anteriores se pueden implementar mediante un script de Windows PowerShell .

En los pasos siguientes se explica cómo crear una automatización para crear un PAC mediante la reutilización del PowerShell script de Windows.

1. Crea una plantilla de EC2 lanzamiento de Amazon que descargue o cree el PowerShell script de Windows como parte del proceso de arranque. Por ejemplo, puede utilizar los datos EC2 del usuario para descargar el script desde un bucket de Amazon Simple Storage Service (Amazon S3).
2. Cree un runbook de AWS Systems Manager Automation para invocar el script de Windows PowerShell .
3. Asocie el manual de procedimientos a la instancia de ESCWA mediante la etiqueta de instancia.
4. Cree un grupo de escalado automático ESCWA utilizando la plantilla de lanzamiento.

Puede usar el siguiente CloudFormation fragmento de AWS de ejemplo para crear el runbook de automatización.

CloudFormation Fragmento de ejemplo de un manual de automatización de Systems Manager utilizado para la creación de un PAC

```
PACInitDocument:
   Type: AWS::SSM::Document
   Properties:
     DocumentType: Command
     Content:
       schemaVersion: '2.2'
       description: Operation Runbook to create Enterprise Server PAC
       mainSteps:
       - action: aws:runPowerShellScript
         name: CreatePAC
         inputs:
           onFailure: Abort
           timeoutSeconds: "1200"
           runCommand:
```

```
            - |
              C:\Scripts\PAC-Init.ps1
  PacInitAutomation:
     Type: AWS::SSM::Document
     Properties:
       DocumentType: Automation
       Content:
         description: Prepare Micro Focus PAC Cluster via ESCWA Server
         schemaVersion: '0.3'
         assumeRole: !GetAtt SsmAssumeRole.Arn
         mainSteps:
           - name: RunPACInitDocument
             action: aws:runCommand
             timeoutSeconds: 300
             onFailure: Abort
             inputs:
               DocumentName: !Ref PACInitDocument
               Targets:
                 - Key: tag:Enterprise Server - ESCWA
                   Values:
                     - "true"
   PacInitDocumentAssociation:
     Type: AWS::SSM::Association
     Properties:
       DocumentVersion: "$LATEST"
       Name: !Ref PACInitDocument
       Targets:
         - Key: tag:Enterprise Server - ESCWA
           Values:
             - "true"
```

Para obtener más información, consulte Micro Focus Enterprise Server: Configuración de un PAC.

Automatización para escalado horizontal con una nueva instancia de Enterprise Server

Cuando una instancia de Enterprise Server se escala horizontalmente, su región de Enterprise Server debe añadirse al PAC. En los siguientes pasos se explica cómo invocar a la CESPAO APIs y añadir la región de Enterprise Server al PAC.

1. Instale la definición de PAC en las regiones de Enterprise Server.

```
POST '/server/v1/config/mfds'
POST /native/v1/config/groups/pacs/${pac_uid}/install
```

2. Inicie en caliente la región en el PAC.

```
POST /native/v1/regions/${host_ip}/${port}/${region_name}/start
```

3. Agregue la instancia de Enterprise Server al equilibrador de carga asociando el grupo de escalado automático al equilibrador de carga.

Los pasos anteriores se pueden implementar mediante un script de Windows PowerShell . Para obtener más información, consulte Micro Focus Enterprise Server: Configuración de un PAC.

Los siguientes pasos se pueden utilizar para crear una automatización basada en eventos que permita añadir una instancia de Enterprise Server recién lanzada a un PAC reutilizando el PowerShell script de Windows.

1. Cree una plantilla de EC2 lanzamiento de Amazon para una instancia de Enterprise Server que aprovisione una región de Enterprise Server durante su arranque. Por ejemplo, puede usar el comando mfds de Micro Focus Enterprise Server para importar una configuración regional. Para obtener más detalles y ver las opciones disponibles para este comando, consulte la referencia de Enterprise Server.
2. Cree un grupo de escalado automático de Enterprise Server que emplee la plantilla de lanzamiento creada en el paso anterior.
3. Cree un manual de automatización de Systems Manager para invocar el script de Windows PowerShell .
4. Asocie el manual de procedimientos a la instancia de ESCWA mediante la etiqueta de instancia.
5. Cree una EventBridge regla de Amazon para filtrar el evento EC2 Instance Launch Successful para el grupo de escalado automático de Enterprise Server y cree el objetivo para usar el manual de automatización.

Puede usar el siguiente CloudFormation fragmento de ejemplo para crear el manual de automatización y la regla. EventBridge

CloudFormation Fragmento de ejemplo de Systems Manager utilizado para escalar instancias de Enterprise Server

```
ScaleOutDocument:
   Type: AWS::SSM::Document
   Properties:
     DocumentType: Command
```

```
      Content:
        schemaVersion: '2.2'
        description: Operation Runbook to Adding MFDS Server into an existing PAC
        parameters:
          MfdsPort:
            type: String
          InstanceIpAddress:
            type: String
            default: "Not-Available"
          InstanceId:
            type: String
            default: "Not-Available"
        mainSteps:
        - action: aws:runPowerShellScript
          name: Add_MFDS
          inputs:
            onFailure: Abort
            timeoutSeconds: "300"
            runCommand:
            - |
              $ip = "{{InstanceIpAddress}}"
              if ( ${ip} -eq "Not-Available" ) {
                $ip = aws ec2 describe-instances --instance-id {{InstanceId}} --output
text --query "Reservations[0].Instances[0].PrivateIpAddress"
              }
              C:\Scripts\Scale-Out.ps1 -host_ip ${ip} -port {{MfdsPort}}

  PacScaleOutAutomation:
    Type: AWS::SSM::Document
    Properties:
      DocumentType: Automation
      Content:
        parameters:
          MfdsPort:
            type: String
          InstanceIpAddress:
            type: String
            default: "Not-Available"
          InstanceId:
            type: String
            default: "Not-Available"
        description: Scale Out 1 New Server in Micro Focus PAC Cluster via ESCWA
Server
        schemaVersion: '0.3'
```

```
        assumeRole: !GetAtt SsmAssumeRole.Arn
        mainSteps:
          - name: RunScaleOutCommand
            action: aws:runCommand
            timeoutSeconds: 300
            onFailure: Abort
            inputs:
              DocumentName: !Ref ScaleOutDocument
              Parameters:
                InstanceIpAddress: "{{InstanceIpAddress}}"
                InstanceId: "{{InstanceId}}"
                MfdsPort: "{{MfdsPort}}"
              Targets:
                - Key: tag:Enterprise Server - ESCWA
                  Values:
                    - "true"
```

Automatización para reducir horizontalmente una instancia de Enterprise Server

Al igual que con la ampliación horizontal, cuando se amplía una instancia de Enterprise Server, se inicia la acción de finalización del ciclo de vida EC2 de la instancia, y se necesitan las siguientes llamadas al proceso y a la API para eliminar una instancia de Micro Focus Enterprise Server del PAC.

1. Detenga la región de la instancia de Enterprise Server que está finalizando.

```
POST "/native/v1/regions/${host_ip}/${port}/${region_name}/stop"
```

2. Elimine la instancia de Enterprise Server del PAC.

```
DELETE "/server/v1/config/mfds/${uid}"
```

3. Envíe una señal para continuar con la finalización de la instancia de Enterprise Server.

Los pasos anteriores se pueden implementar en un script de Windows. PowerShell Para obtener más información sobre este proceso, consulte el documento de Micro Focus Enterprise Server: Administración de un PAC.

En los siguientes pasos se explica cómo crear una automatización basada en eventos para cerrar una instancia de Enterprise Server desde un PAC mediante la reutilización del script de Windows. PowerShell

1. Cree un manual de automatización de Systems Manager para invocar el script de Windows PowerShell .
2. Asocie el manual de procedimientos a la instancia de ESCWA mediante la etiqueta de instancia.
3. Cree un enlace automático para el ciclo de vida de un grupo de escalado, por EC2 ejemplo, la terminación.
4. Cree una EventBridge regla de Amazon para filtrar el evento de acción del ciclo EC2 de vida de finalización de la instancia para el grupo de escalado automático de Enterprise Server y cree el objetivo para usar el manual de automatización.

Puede utilizar la siguiente CloudFormation plantilla de ejemplo para crear un manual, un enlace de ciclo de vida y una EventBridge regla de Systems Manager Automation.

CloudFormation Fragmento de ejemplo de un manual de automatización de Systems Manager utilizado para escalar en una instancia de Enterprise Server

```
ScaleInDocument:
   Type: AWS::SSM::Document
   Properties:
     DocumentType: Command
     Content:
       schemaVersion: '2.2'
       description: Operation Runbook to Remove MFDS Server from PAC
       parameters:
         MfdsPort:
           type: String
         InstanceIpAddress:
           type: String
           default: "Not-Available"
         InstanceId:
           type: String
           default: "Not-Available"
       mainSteps:
       - action: aws:runPowerShellScript
         name: Remove_MFDS
         inputs:
           onFailure: Abort
           runCommand:
           - |
             $ip = "{{InstanceIpAddress}}"
             if ( ${ip} -eq "Not-Available" ) {
```

```
                $ip = aws ec2 describe-instances --instance-id {{InstanceId}} --output
text --query "Reservations[0].Instances[0].PrivateIpAddress"
              }
              C:\Scripts\Scale-In.ps1 -host_ip ${ip} -port {{MfdsPort}}

  PacScaleInAutomation:
    Type: AWS::SSM::Document
    Properties:
      DocumentType: Automation
      Content:
        parameters:
          MfdsPort:
            type: String
          InstanceIpAddress:
            type: String
            default: "Not-Available"
          InstanceId:
            type: String
            default: "Not-Available"
        description: Scale In 1 New Server in Micro Focus PAC Cluster via ESCWA Server
        schemaVersion: '0.3'
        assumeRole: !GetAtt SsmAssumeRole.Arn
        mainSteps:
          - name: RunScaleInCommand
            action: aws:runCommand
            timeoutSeconds: "600"
            onFailure: Abort
            inputs:
              DocumentName: !Ref ScaleInDocument
              Parameters:
                InstanceIpAddress: "{{InstanceIpAddress}}"
                MfdsPort: "{{MfdsPort}}"
                InstanceId: "{{InstanceId}}"
              Targets:
                - Key: tag:Enterprise Server - ESCWA
                  Values:
                    - "true"
          - name: TerminateTheInstance
            action: aws:executeAwsApi
            inputs:
              Service: autoscaling
              Api: CompleteLifecycleAction
              AutoScalingGroupName: !Ref AutoScalingGroup
              InstanceId: "{{ InstanceId }}"
```

```
                LifecycleActionResult: CONTINUE
                LifecycleHookName: !Ref ScaleInLifeCycleHook
```

Automatización para un activador de escalado EC2 automático de Amazon

El proceso de configuración de una política de escalado para instancias de Enterprise Server requiere comprender el comportamiento de la aplicación. En la mayoría de los casos, puede establecer políticas de escalado de seguimiento de objetivos. Por ejemplo, puedes usar el uso promedio de la CPU como CloudWatch métrica de Amazon para configurar la política de escalado automático. Para obtener más información, consulte Políticas de escalado de seguimiento de Target para Amazon EC2 Auto Scaling. Para aplicaciones con patrones de tráfico regulares, considere la posibilidad de usar una política de escalado predictivo. Para obtener más información, consulte Escalado predictivo para Amazon EC2 Auto Scaling.

Cree un visor de archivos de unidad central avanzada en la nube de AWS

Boopathy GOPALSAMY y Jeremiah O'Connor, Amazon Web Services

Resumen

Este patrón proporciona ejemplos de código y pasos para ayudarlo a crear una herramienta avanzada para buscar y revisar los archivos de formato fijo de su unidad central mediante los servicios sin servidor de AWS. El patrón proporciona un ejemplo de cómo convertir un archivo de entrada de mainframe en un documento de Amazon OpenSearch Service para navegar y buscar. La herramienta de visualización de archivos puede ayudarle a lograr lo siguiente:

- Conservar la misma estructura y diseño de archivos de unidad central para mantener la coherencia en su entorno de migración de AWS objetivo (por ejemplo, puede mantener el mismo diseño para los archivos en una aplicación por lotes que transmite archivos a terceros)
- Acelerar el desarrollo y las pruebas durante la migración de su unidad central
- Dar soporte a las actividades de mantenimiento después de la migración

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una nube privada virtual (VPC) con una subred a la que pueda acceder la plataforma antigua
-

> **Note**
>
> Un archivo de entrada y su correspondiente cuaderno de texto en lenguaje común orientado a los negocios (COBOL) (: Para ver ejemplos de archivos de entrada y cuadernos de texto COBOL, consulte en el repositorio. gfs-mainframe-solutions GitHub Para obtener más información sobre los cuadernos de COBOL, consulte la Guía de programación empresarial de COBOL para z/OS 6.3 en el sitio web de IBM.)

Limitaciones

- El análisis de los copybook está limitado a no más de dos niveles anidados (SE PRODUCE)

Arquitectura

Pila de tecnología de origen

- Archivos de entrada en formato FB (bloqueado fijo)
- Diseño de copybook de COBOL

Pila de tecnología de destino

- Amazon Athena
- OpenSearch Servicio Amazon
- Amazon Simple Storage Service (Amazon S3)
- AWS Lambda
- AWS Step Functions

Arquitectura de destino

El siguiente diagrama muestra el proceso de analizar y convertir un archivo de entrada del ordenador central en un documento de OpenSearch servicio para su navegación y búsqueda.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario administrador o una aplicación envía los archivos de entrada a un bucket de S3 y los copybook de COBOL a otro bucket de S3.
2.
> **Note**
>
> El bucket de S3 con los archivos de entrada invoca una función de Lambda que inicia un flujo de trabajo de Step Functions sin servidor. : El uso de un activador de eventos de S3 y una función de Lambda para impulsar el flujo de trabajo de Step Functions en este patrón es opcional. Los ejemplos de GitHub código de este patrón no incluyen el uso de estos servicios, pero puede usarlos según sus necesidades.

3. El flujo de trabajo de Step Functions coordina todos los procesos por lotes de las siguientes funciones de Lambda:

- La función `s3copybookparser.py` analiza el diseño del copybook y extrae los atributos de los campos, los tipos de datos y las compensaciones (necesarios para el procesamiento de los datos de entrada).
- La función `s3toathena.py` crea un diseño de tabla de Athena. Athena analiza los datos de entrada que procesa la función `s3toathena.py` y los convierte en un archivo CSV.
- La `s3toelasticsearch.py` función ingiere el archivo de resultados del bucket de S3 y lo envía a OpenSearch Service.

4. Los usuarios acceden a los OpenSearch paneles con OpenSearch Service para recuperar los datos en varios formatos de tablas y columnas y, a continuación, ejecutar consultas con los datos indexados.

Tools (Herramientas)

Servicios de AWS

- Amazon Athena es un servicio interactivo de consultas que le permite analizar datos directamente en Amazon Simple Storage Service (Amazon S3) usando SQL estándar.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice. En este patrón, se utiliza Lambda para implementar la lógica principal, como analizar archivos, convertir datos y cargar datos en OpenSearch Service para un acceso interactivo a los archivos.
- Amazon OpenSearch Service es un servicio gestionado que le ayuda a implementar, operar y escalar clústeres de OpenSearch servicios en la nube de AWS. En este patrón, utiliza OpenSearch Service para indexar los archivos convertidos y proporcionar capacidades de búsqueda interactiva a los usuarios.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.

- AWS Step Functions es un servicio de orquestación sin servidor que le ayuda a combinar funciones de Lambda y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial. En este patrón, se utilizan Step Functions para orquestar las funciones de Lambda.

Otras herramientas

- GitHubes un servicio de alojamiento de código que proporciona herramientas de colaboración y control de versiones.
- Python es un lenguaje de programación de alto nivel.

Código

El código de este patrón está disponible en el GitHub gfs-mainframe-patternsrepositorio.

Epics

Prepare el entorno de destino

Tarea	Descripción	Habilidades requeridas
Cree el bucket de S3.	Cree un bucket de S3 para almacenar los copybooks , los archivos de entrada y los archivos de salida. Recomendamos la siguiente estructura de carpetas para su bucket de S3: • `copybook/` • `input/` • `output/` • `query/` • `results/`	AWS general
Cree la función s3copyboo kparser.	1. Cree una función Lambda llamada `s3copyboo`	AWS general

Tarea	Descripción	Habilidades requeridas
	`kparser` y cargue el código fuente (`s3copybookparser.py` y `ycopybook.py`) desde el GitHubrepositorio. 2. Adjunte la política de IAM `S3ReadOnly` a la función de Lambda.	
Cree la función s3toathena.	1. Cree una función Lambda llamada `s3toathena` y cargue el código fuente (`s3toathena.py`) desde el GitHubrepositorio. Configure el tiempo de espera de Lambda en > 60 segundos. 2. Para proporcionar acceso a los recursos necesarios, adjunte las políticas de IAM `AmazonAthenaFullAccess` y `S3FullAccess` a la función de Lambda.	AWS general

Tarea	Descripción	Habilidades requeridas
Cree la función s3toelasticsearch.	1. **Important** Añada una dependencia de Python a su entorno Lambda. : Para usar la función de `s3toelasticsearch`, debe añadir la dependencia de Python, ya que la función de Lambda usa las dependencias de cliente de Python Elasticsearch (`Elasticsearch==7.9.0` y `requests_aws4auth`). 2. Cree una función Lambda llamada `s3toelasticsearch` y cargue el código fuente (`s3toelasticsearch.py`) desde el GitHubrepositorio. 3. Importe la dependencia de Python como una capa de Lambda. 4. Adjunte las políticas de IAM `S3ReadOnly` y `AmazonOpenSearchSe`	AWS general

Tarea	Descripción	Habilidades requeridas
	`rviceReadOnlyAcces s` a la función de Lambda.	

Tarea	Descripción	Habilidades requeridas
Cree el clúster OpenSearch de servicios.	Cree el clúster 1. Cree un clúster OpenSearch de servicios. Al crear el clúster, haga lo siguiente: • **Note** Cree un usuario maestro y una contraseña para el clúster que pueda usar para iniciar sesión en OpenSearch Dashboards. : Este paso no es obligatorio si utiliza la autenticación a través de Amazon Cognito. • Seleccione control de acceso preciso. Esto le proporciona formas adicionales de controlar el acceso a sus datos en OpenSearch Service. 2. Copie la URL del dominio y pásela como variable de entorno 'HOST' a la función de Lambda `s3toelasticsearch` . Conceder acceso al rol de IAM	AWS general

Tarea	Descripción	Habilidades requeridas
	Para proporcionar un acceso detallado al rol de IAM de la función de Lambda (`arn:aws:iam::**:role/service-role/s3toelasticsearch-role-**`), haga lo siguiente: 1. Inicie sesión en OpenSearch Dashboards como usuario maestro. 2. Seleccione la pestaña Security (Seguridad) y, a continuación, elija Roles, all_access, Map user (Asignar usuari)o y Backend roles (Roles de backend). 3. Añada el nombre de recurso de Amazon (ARN) del rol de IAM de la función de Lambda y, a continuación, seleccione Save (Guardar). Para obtener más información, consulte Asignar funciones a los usuarios en la documentación del OpenSearch servicio.	

Tarea	Descripción	Habilidades requeridas
Cree Step Functions para la orquestación.	1. Cree un equipo de estado de Step Functions con el flujo estándar. La definició n se incluye en el GitHub repositorio. 2. En el script JSON, sustituya la función Lambda por la función Lambda ARNs de su entorno. ARNs	AWS general

Implemente y ejecute

Tarea	Descripción	Habilidades requeridas
Cargue los archivos de entrada y los copybooks en un bucket de S3;.	Descargue los archivos de ejemplo de la carpeta de ejemplos del GitHub repositor io y cárguelos en el bucket de S3 que creó anteriormente. 1. Cargue `Mockedcop y.cpy` y `acctix.cpy` en la carpeta `<S3_Bucke t>/copybook` . 2. Suba los archivos de entrada de muestra `Modedupdate.txt` y `acctindex.cpy` a la carpeta `<S3_Bucket>/ input`.	AWS general
Invoque los Step Functions.	1. Inicie sesión en la consola de administración de AWS	AWS general

Tarea	Descripción	Habilidades requeridas

	y abra la consola de Step Functions.
	2. En el panel de navegación izquierdo, elija State machines (Equipos de estado).
	3. Elija su equipo de estado y, a continuación, elija Start execution (Iniciar ejecución).
	4. En el cuadro de entrada, introduzca la siguiente copybook/file ruta como variable JSON al bucket de S3 y, a continuación, seleccione Iniciar ejecución.
	
	`{ "s3_copybook_bucket_name": "<BUCKET NAME>", "s3_copybook_bucket_key": "<COPYBOOK PATH>", "s3_source_bucket_name": "<BUCKET NAME", "s3_source_bucket_key": "INPUT FILE PATH" }`
	
	Por ejemplo:
	
	`{ "s3_copybook_bucket_name": "fileaidtest",`	

Tarea	Descripción	Habilidades requeridas

	<pre>"s3_copybook_bucke
	t_key": "copybook/
	acctix.cpy",
	"s3_source_bucket_
	name": "fileaidtest",
	"s3_source_bucket_
	key": "input/ac
	ctindex"
	}</pre>	

Valide la ejecución del flujo de trabajo en Step Functions.	En la consola de Step Functions, revise la ejecución del flujo de trabajo en el inspector de gráficos. Los estados de ejecución están codificados por colores para representar el estado de ejecución. Por ejemplo, el azul indica In progress (En curso), el verde indica Succeeded (Correcto) y el rojo indica Failed (Con error). También puede revisar la tabla de la sección Historial de eventos de ejecución para obtener información más detallada sobre los eventos de ejecución. Para ver un ejemplo de la ejecución de un flujo de trabajo gráfico, consulte el gráfico de Step Functions en la sección Información adicional de este patrón.	AWS general

Tarea	Descripción	Habilidades requeridas
Valida los registros de entrega en Amazon CloudWatch.	1. Inicie sesión en la consola de administración de AWS y abra la consola de CloudWatch . 2. En el panel de navegación, elija Logs (Registros) y, luego, Log groups (Grupos de registros). 3. En el cuadro de búsqueda, busque el grupo de registros de la función `s3toelasticsearch` . Para ver un ejemplo de registros de entregas correctos, consulta los registros de CloudWatch entrega en la sección de información adicional de este patrón.	AWS general

Tarea	Descripción	Habilidades requeridas
Valide el archivo formateado en los OpenSearch paneles de control y realice las operaciones con los archivos.	1. Inicie sesión en la Consola de administración de AWS. En Analytics, seleccion a Amazon OpenSearch Service. 2. En el panel de navegación, elija Dominios. 3. En el cuadro de búsqueda, introduce la URL de tu dominio en los OpenSearch paneles. 4. Elija su panel de control y, a continuación, inicie sesión como usuario maestro. 5. Examine los datos indexados en formato de tabla. 6. Compare el archivo de entrada con el archivo de salida formateado (documento indexado) en los paneles. OpenSearch La vista del panel muestra los encabezados de columna añadidos a los archivos formateados. Confirme que los datos de origen de los archivos de entrada sin formato coincidan con los datos de destino de la vista de panel. 7. Realice acciones como la búsqueda (por ejemplo,	AWS general

Tarea	Descripción	Habilidades requeridas
	mediante nombres de campo, valores o expresiones), el filtrado y las operaciones de DQL (Dashboard Query Language, lenguaje de consulta de paneles) en el archivo indexado.	

Recursos relacionados

Referencias

- Ejemplo de copybook de COBOL (documentación de IBM)
- Ayuda de archivo BMC Compuware (documentación de BMC)

Tutoriales

- Tutorial: uso de un desencadenador de Amazon S3 para invocar una función de Lambda (documentación de AWS Lambda)
- ¿Cómo creo un flujo de trabajo sin servidor con AWS Step Functions y AWS Lambda? (documentación de AWS)
- Uso de OpenSearch paneles con Amazon OpenSearch Service (documentación de AWS)

Información adicional

Gráfico de Step Functions

En el siguiente ejemplo se muestra un gráfico de Step Functions. El gráfico muestra el estado de ejecución de las funciones de Lambda utilizadas en este patrón.

CloudWatch registros de entrega

El siguiente ejemplo muestra los registros de entrega correctos para la ejecución de la ejecución `s3toelasticsearch`.

2022-08-10T15:53:33.033-05:00	Número de documentos en trámite: 100	
	2022-08-10T15:53:33.171-05:00	[INFO] 2022-08-10T 20:53:33 .171 Z a1b2c3d4-5678-90ab-cdef- post:443/ _bulk [estado: 200 solicitud : 0.100 s] EXAMPLE11111 https://search-essearch-3h4uqclifeqaj2vg4mphe7ffle.us-east-2.es.amazonaws.com
	2022-08-10T15:53:33.172-05:00	Escritura masiva correcta: 100 documentos

Almacenamiento en contenedores de las cargas de trabajo de mainframe que Blu Age ha modernizado

Richard Milner-Watts, Amazon Web Services

Resumen

Este patrón proporciona un ejemplo de entorno de contenedores para ejecutar cargas de trabajo de mainframe que se han modernizado con la herramienta Blu Age. Blu Age convierte las cargas de trabajo de mainframe heredadas en código Java moderno. Este patrón proporciona un envoltorio alrededor de la aplicación de Java para que pueda ejecutarla mediante servicios de orquestación de contenedores como Amazon Elastic Container Service (Amazon ECS) o Amazon Elastic Kubernetes Service (Amazon EKS).

Para obtener más información sobre la modernización de sus cargas de trabajo mediante el uso de Blu Age y los servicios de AWS, consulte estas publicaciones en las recomendaciones de AWS:

- Ejecución de cargas de trabajo de mainframe modernizadas de Blu Age en una infraestructura de AWS sin servidor
- Implementar un entorno para aplicaciones de Blu Age en contenedores mediante Terraform

Si necesita ayuda para utilizar Blu Age para modernizar las cargas de trabajo de sus mainframes, póngase en contacto con el equipo de Blu Age seleccionando la opción Contactar con nuestros expertos en el sitio web de Blu Age. Si necesita ayuda para migrar sus cargas de trabajo modernizadas a AWS, integrarlas con los servicios de AWS y pasarlas a producción, póngase en contacto con su administrador de cuentas de AWS o rellene el formulario de AWS Professional Services.

Requisitos previos y limitaciones

Requisitos previos

- Una aplicación Java modernizada creada por Blu Age. Para fines de prueba, este patrón proporciona un ejemplo de aplicación Java que puede utilizar como prueba de concepto.
- Un entorno de Docker que puede utilizar para crear el contenedor.

Limitaciones

Según la plataforma de orquestación de contenedores que utilice, es posible que los recursos que se puedan poner a disposición del contenedor (como la CPU, la RAM y el almacenamiento) estén limitados. Por ejemplo, si utiliza Amazon ECS con AWS Fargate, consulte la documentación de Amazon ECS para conocer los límites y las consideraciones.

Arquitectura

Pila de tecnología de origen

- Blu Age
- Java

Pila de tecnología de destino

- Docker

Arquitectura de destino

En el siguiente diagrama, se muestra la arquitectura de la aplicación Blu Age dentro de un contenedor de Docker.

1. El punto de entrada al contenedor es el script contenedor. Este script bash es responsable de preparar el entorno de tiempo de ejecución para la aplicación Blu Age y de procesar los resultados.
2. Las variables de entorno del contenedor se utilizan a fin de configurar variables en el script del contenedor, como los nombres de bucket de Amazon Simple Storage Service (Amazon S3) y las credenciales de la base de datos. Las variables de entorno las proporcionan AWS Secrets Manager o Parameter Store, una funcionalidad de AWS Systems Manager. Si utiliza Amazon ECS como servicio de orquestación de contenedores, también puede codificar las variables de entorno en la definición de tareas de Amazon ECS.
3. El script contenedor se encarga de introducir todos los archivos de entrada del bucket de S3 en el contenedor antes de ejecutar la aplicación Blu Age. La interfaz de la línea de comandos de AWS (AWS CLI) se instala en el contenedor. Esto proporciona un mecanismo de acceso a los objetos que se almacenan en Amazon S3 a través del punto de conexión de la nube privada virtual (VPC) de la puerta de enlace.

4. Es posible que el archivo Java Archive (JAR) de la aplicación Blu Age necesite comunicarse con otras orígenes de datos, como Amazon Aurora.
5. Una vez finalizado, el script contenedor entrega los archivos de salida resultantes a un bucket de S3 para su posterior procesamiento (por ejemplo, por parte de Amazon CloudWatch Logging Services). El patrón también permite enviar archivos de registro comprimidos a Amazon S3, si utiliza una alternativa al CloudWatch registro estándar.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores escalable y rápido que ayuda a ejecutar, detener y administrar contenedores en un clúster.

Herramientas

- Docker es una plataforma de software para crear, probar e implementar aplicaciones. Docker agrupa el software en unidades estandarizadas denominadas contenedores, que contienen todo lo que el software necesita para ejecutarse, incluidas las bibliotecas, las herramientas del sistema, el código y el tiempo de ejecución. Puede usar Docker a fin de implementar y escalar aplicaciones en cualquier entorno.
- Bash es una interfaz de lenguaje de comandos (shell) para el sistema operativo GNU.
- Java es el lenguaje de programación y el entorno de desarrollo utilizados en este patrón.
- Blu Age es una herramienta de AWS Mainframe Modernization que convierte las cargas de trabajo de mainframe heredadas, incluidos el código de las aplicaciones, las dependencias y la infraestructura, en cargas de trabajo modernas para la nube.

Repositorio de código

El código de este patrón está disponible en el repositorio de contenedores de muestras de GitHub Blu Age.

Prácticas recomendadas

- Externalice las variables para alterar el comportamiento de su aplicación mediante variables de entorno. Estas variables permiten que la solución de orquestación de contenedores modifique el entorno de tiempo de ejecución sin tener que volver a construir el contenedor. Este patrón incluye ejemplos de variables de entorno que pueden ser útiles para las aplicaciones de Blu Age.
- Valide cualquier dependencia de la aplicación antes de ejecutar la aplicación Blu Age. Por ejemplo, compruebe que la base de datos esté disponible y que las credenciales sean válidas. Escriba las pruebas en el script contenedor para comprobar las dependencias y, si no se cumplen, no las consiga antes de tiempo.
- Utilice el registro detallado dentro del script contenedor. Interactuar directamente con un contenedor en ejecución puede resultar difícil, dependiendo de la plataforma de orquestación y del tiempo que lleve el trabajo. Asegúrese de que los resultados útiles estén escritos para ayudar a `STDOUT` a diagnosticar cualquier problema. Por ejemplo, el resultado puede incluir el contenido del directorio de trabajo de la aplicación antes y después de ejecutarla.

Epics

Obtenga un archivo JAR de la aplicación Blu Age

Tarea	Descripción	Habilidades requeridas
Opción 1: trabajar con Blu Age a fin de obtener el archivo JAR de su aplicación.	El contenedor de este patrón requiere una aplicación Blu Age. Como alternativa, puede usar la aplicación Java de ejemplo que viene con este patrón para un prototipo. Trabaje con el equipo de Blu Age para obtener un archivo JAR para su aplicación que pueda incluir en el contenedor. Si el archivo JAR no está disponible, consulte la siguiente tarea para usar la	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	aplicación de ejemplo en su lugar.	
Opción 2: Cree o utilice el archivo JAR de la aplicación de muestra suministrado.	Este patrón proporciona un archivo JAR de muestra prediseñado. Este archivo genera las variables de entorno de la aplicación a `STDOUT` antes de dormir durante 30 segundos y salir. Este archivo recibe un nombre `bluAgeSample.jar` y se encuentra en la carpeta docker del GitHub repositorio. Si desea modificar el código y crear su propia versión del archivo JAR, utilice el código fuente que se encuentra en. / java_ sample/src/sample _java_app.java en el repositor io. GitHub Puede usar el script de compilación en ./java_sa mple/build.sh para compilar el código fuente de Java y crear un nuevo archivo JAR.	Desarrollador de aplicaciones

Construya el contenedor de Blue Age

Tarea	Descripción	Habilidades requeridas
Clona el repositorio. GitHub	Clone el repositorio de código de muestra mediante el comando:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`git clone https://github.com/aws-samples/aws-blu-age-sample-container`	
Utilice Docker para crear el contenedor.	Utilice Docker para crear el contenedor antes de enviarlo a un registro de Docker, como Amazon ECR: 1. Desde la terminal que elija, navegue hasta la `docker` carpeta del GitHub repositorio local. 2. Use este comando para construir el contenedor: `docker build -t <tag> .` donde `<tag>` es el nombre del contenedor que quiere usar.	AWS DevOps
Pruebe el contenedor Blu Age.	(Opcional) Si es necesario, pruebe el contenedor en las instalaciones mediante el comando: `docker run -it <tag> /bin/bash`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Autenticar en su repositorio de Docker.	Si planea usar Amazon ECR, siga las instrucciones de la documentación de Amazon ECR para instalar y configurar la AWS CLI y autenticar la CLI de Docker en su registro predeterminado. Le recomendamos que utilice el get-login-password comando para la autenticación. **Note** La consola de Amazon ECR proporciona una versión rellenada previamente de este comando si utiliza el botón Ver comandos de extracción. Para obtener más información, consulte la documentación de Amazon ECR. `aws ecr get-login -password --region <region> | docker login --username AWS --password-stdin <account>.dkr.ecr.`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`<region>.amazonaws.com` Si no piensa utilizar Amazon ECR, siga las instrucciones que se proporcionan para su sistema de registro de contenedores.	
Cree un repositorio de contenedores.	Cree un repositorio en Amazon ECR. Para obtener instrucciones, consulte el patrón Implementar un entorno para aplicaciones de Blu Age en contenedores mediante Terraform. Si utiliza otro sistema de registro de contenedores, siga las instrucciones que se proporcionan para ese sistema.	AWS DevOps

Tarea	Descripción	Habilidades requeridas

Etiquete su contenedor y colóquelo en el repositorio de destino.	Si utiliza Amazon ECR:
	1. Etiquete la imagen de Docker en las instalaciones con el registro y el repositorio de Amazon ECR para poder enviarla a su repositorio remoto:
	`docker tag <tag>:latest <account>.dkr.ecr.<region>.amazonaws.com/<repository>:<versionNumber>`
	2. Inserte la imagen en el repositorio remoto:
	`docker push <account>.dkr.ecr.<region>.amazonaws.com/<repository>:<versionNumber>`
	Para obtener más información, consulte Insertar una imagen de Docker en la Guía del usuario de Amazon ECR.
		AWS DevOps

Recursos relacionados

Recursos de AWS

- Repositorio de contenedores de muestras de AWS Blu Age

- Ejecución de cargas de trabajo de mainframe modernizadas de Blu Age en una infraestructura de AWS sin servidor
- Implementar un entorno para aplicaciones de Blu Age en contenedores mediante Terraform
- Uso de Amazon ECR con la AWS CLI (Guía del usuario de Amazon ECR)
- Autenticación de registro privado (Guía del usuario de Amazon ECR)
- Documentación de Amazon ECS
- Documentación de Amazon EKS

Recursos adicionales

- Sitio web de Blu Age
- Sitio web de Docker

Convierta y desempaquete datos EBCDIC a ASCII en AWS mediante Python

Luis Gustavo Dantas, Amazon Web Services

Resumen

Dado que los mainframe suelen alojar datos empresariales críticos, la modernización de estos datos es una de las tareas más importantes a la hora de migrar datos a la nube de Amazon Web Services (AWS) o a otro entorno de American Standard Code for Information Interchange (ASCII). En los mainframe, los datos suelen codificarse en un formato ampliado de código de intercambio decimal codificado en binario (EBCDIC). La exportación de bases de datos, los métodos de acceso al almacenamiento virtual (VSAM) o los archivos planos suelen producir archivos EBCDIC binarios empaquetados, que son más complejos de migrar. La solución de migración de bases de datos más usada es la captura de datos de cambios (CDC), que, en la mayoría de los casos, convierte automáticamente la codificación de los datos. Sin embargo, es posible que los mecanismos de CDC no estén disponibles para estas bases de datos, VSAM o archivos planos. En el caso de estos archivos, es necesario adoptar un enfoque alternativo para modernizar los datos.

Este patrón describe cómo modernizar los datos EBCDIC convirtiéndolos a formato ASCII. Tras la conversión, puede cargar los datos en bases de datos distribuidas o hacer que las aplicaciones en la nube procesen los datos directamente. El patrón utiliza el script de conversión y los archivos de muestra del mainframe-data-utilities GitHub repositorio.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un archivo de entrada EBCDIC y su correspondiente cuaderno en lenguaje común orientado a negocios (COBOL). En el repositorio se incluyen un archivo EBCDIC de muestra y un cuaderno de notas COBOL. mainframe-data-utilities GitHub Para obtener más información sobre los cuadernos de COBOL, consulte la Guía de programación de Enterprise COBOL for z/OS 6.4 en el sitio web de IBM.

Limitaciones

- No es compatible con diseños de archivo definidos en COBOL. Deben estar disponibles por separado.

Versiones de producto

- Python, versión 3.8 o posterior

Arquitectura

Pila de tecnología de origen

- Datos EBCDIC en un mainframe
- Cuaderno COBOL

Pila de tecnología de destino

- Instancia de Amazon Elastic Compute Cloud (Amazon EC2) en una nube privada virtual (VPC)
- Amazon Elastic Block Store (Amazon EBS)
- Python y sus paquetes necesarios, JavaScript Object Notation (JSON), sys y datetime
- Archivo plano ASCII listo para ser leído por una aplicación moderna o cargado en una tabla de base de datos relacional

Arquitectura de destino

El diagrama de arquitectura muestra el proceso de conversión de un archivo EBCDIC en un archivo ASCII en una instancia: EC2

1. Con el script parse_copybook_to_json.py, el cuaderno COBOL se convierte en un archivo JSON.
2. Con el archivo JSON y el script extract_ebcdic_to_ascii.py, los datos EBCDIC se convierten en un archivo ASCII.

Automatizar y escalar

Una vez que disponga de los recursos necesarios para las primeras conversiones manuales de archivos, puede automatizar la conversión de archivos. Este patrón no incluye instrucciones para la

automatización. La conversión se puede automatizar de varias formas. A continuación, se muestra un posible enfoque:

1. Encapsular la interfaz de la línea de comandos de AWS (AWS CLI) y los comandos de script de Python en un script de intérprete de comandos.
2. Cree una función de AWS Lambda que envíe de forma asíncrona el trabajo del script de shell a una instancia. EC2 Para obtener más información, consulte Programar trabajos de SSH con AWS Lambda.
3. Crear un desencadenante de Amazon Simple Storage Service (Amazon S3) que invoque la función de Lambda cada vez que se cargue un archivo heredado. Para obtener más información, consulte Utilizar un desencadenador de Amazon S3 para invocar una función de Lambda.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento a nivel de bloques para utilizarlos con instancias de Amazon Elastic Compute Cloud (Amazon). EC2
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.

Otras herramientas

- GitHubes un servicio de alojamiento de código que proporciona herramientas de colaboración y control de versiones.
- Python es un lenguaje de programación de alto nivel.

Repositorio de código

El código de este patrón está disponible en el mainframe-data-utilities GitHub repositorio.

Epics

Prepara la EC2 instancia

Tarea	Descripción	Habilidades requeridas
Lanza una EC2 instancia.	La EC2 instancia debe tener acceso saliente a Internet. Esto permite que la instancia acceda al código fuente de Python disponible en GitHub. Para crear una instancia: 1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2. 2. Lance una instancia de EC2 Linux. Use una dirección IP pública y permita el acceso entrante a través del puerto 22. Asegúrese de que el tamaño de almacenamiento de la instancia sea, al menos, el doble del tamaño del archivo de datos EBCDIC. Para obtener instrucciones, consulta la EC2 documentación de Amazon.	AWS general
Instala Git	1. Con un cliente de shell seguro (SSH), conéctese a la EC2 instancia que acaba de lanzar. Para obtener más información, consulte	AWS general, Linux

Tarea	Descripción	Habilidades requeridas

	Conexión con la instancia de Linux.
	2. En la EC2 consola de Amazon, ejecuta el siguiente comando. Esto instala Git en la EC2 instancia.
	`sudo yum install git`
	3. Ejecute el comando siguiente y confirme que Git ha sido instalado correctam ente.
	`git --version`	

Tarea	Descripción	Habilidades requeridas

Instalación de Python.	1. En la EC2 consola de Amazon, ejecuta el siguiente comando. Esto instala Python en la EC2 instancia.
	`sudo yum install python3`
	2. En la EC2 consola de Amazon, ejecuta el siguiente comando. Esto instala Pip3 en la instancia. EC2
	`sudo yum install python3-pip`
	3. En la EC2 consola de Amazon, ejecuta el siguiente comando. De este modo, se instala AWS SDK for Python (Boto3) en la instancia. EC2
	`sudo pip3 install boto3`
	4. En la EC2 consola de Amazon, ejecuta el siguiente comando, donde `<us-east-1>` está el código de tu región de AWS. Para obtener una lista completa de los códigos de región, consulta
		AWS general, Linux

Tarea	Descripción	Habilidades requeridas
	las regiones disponibles en la EC2 documentación de Amazon. `export AWS_DEFAULT_REGION=<us-east-1>`	
Clona el GitHub repositorio.	1. En la EC2 consola de Amazon, ejecuta el siguiente comando. De este modo, se clona el mainframe-data-utilitiesrepositorio GitHub y se abre la ubicación de copia predeterminada, la home carpeta. `git clone https://github.com/aws-samples/mainframe-data-utilities.git` 2. En la carpeta home, confirme que existe la carpeta `mainframe-data-utilities` .	AWS general, GitHub

Cree el archivo ASCII a partir de los datos del EBCDIC

Tarea	Descripción	Habilidades requeridas
Convierta el cuaderno COBOL en el archivo de diseño JSON.	En la carpeta `mainframe-data-utilities` , ejecute el script parse_copybook_to_json.py. Este	AWS general, Linux

Tarea	Descripción	Habilidades requeridas

	módulo de automatización lee el diseño del archivo de un cuaderno COBOL y crea un archivo JSON. Este archivo JSON contiene la informaci ón necesaria para interpret ar y extraer los datos del archivo fuente. Se crearán los metadatos de JSON a partir del cuaderno COBOL.
	
	El siguiente comando convierte el cuaderno COBOL en un archivo JSON.
	
	`python3 parse_cop ybook_to_json.py \ -copybook LegacyRef erence/COBPACK2.cpy \ -output sample-data/ cobpack2-list.json \ -dict sample-data/ cobpack2-dict.json \ -ebcdic sample-data/ COBPACK.OUTFILE.txt \ -ascii sample-data/ COBPACK.ASCII.txt \ -print 10000`
	
	El script imprime los argumentos recibidos.
	
	`---------- ---------- ---------- ----------`	

Tarea	Descripción	Habilidades requeridas

	``
	Copybook file.....
	.....| LegacyRef
	erence/COBPACK2.cpy
	Parsed copybook (JSON
	 List).| sample-data/
	cobpack2-list.json
	JSON Dict (document
	ation)...| sample-da
	ta/cobpack2-dict.json
	ASCII file.....
	.....| sample-
	data/COBPACK.ASCII.t
	xt
	EBCDIC file.....
	.....| sample-
	data/COBPACK.OUTFILE
	.txt
	Print each.....
	.....| 10000
	---------- 	
	---------- 	
	---------- 	
	---------- 	
	`` Para obtener más informaci ón sobre los argumentos, consulte el archivo README del GitHub repositorio.	

Tarea	Descripción	Habilidades requeridas
Inspeccione el archivo de diseño JSON.	1. Acceda a la ruta de salida definida en el script parse_copybook_to_json.py. 2. Compruebe la hora de creación del archivo sample-data/cobpack2-list.json para confirmar que ha seleccionado el archivo de diseño JSON adecuado. 3. Examine el archivo JSON y confirme que el contenido es similar a este. `"input": "extract-ebcdic-to-ascii/COBPACK.OUTFILE.txt", "output": "extract-ebcdic-to-ascii/COBPACK.ASCII.txt", "max": 0, "skip": 0, "print": 10000, "lrecl": 150, "rem-low-values": true, "separator": "|", "transf": [ { "type": "ch", "bytes": 19, "name": "OUTFILE-TEXT" }`	AWS general, JSON

Tarea	Descripción	Habilidades requeridas
	Los atributos más importantes del archivo de diseño JSON son: • `input` – Contiene la ruta del archivo EBCDIC que se va a convertir • `output` – Define la ruta en la que se generará el archivo ASCII • `lrecl` – Especifica el tamaño en bytes de la longitud del registro lógico • `transf` – Muestra todos los campos y su tamaño en bytes Para obtener más informaci ón sobre el archivo de diseño JSON, consulta el archivo README del GitHub repositor io.	

Tarea	Descripción	Habilidades requeridas

Cree el archivo ASCII.	Ejecute el script extract_ebcdic_to_ascii.py, que se incluye en el repositorio clonado GitHub . Este script lee el archivo EBCDIC y escribe un archivo ASCII convertido y legible.
	`python3 extract_ebcdic_to_ascii.py -local-json sample-data/cobpack2-list.json`
	A medida que el script procesa los datos del EBCDIC, imprime un mensaje por cada lote de 10 000 registros. Consulte el siguiente ejemplo.
	`---------- 2023-05-15 21:21:46.322253 | Local Json file | -local-json | sample-data/cobpack2-list.json 2023-05-15 21:21:47.034556 | Records processed | 10000 2023-05-15 21:21:47.736434 | Records processed | 20000 2023-05-15 21:21:48.441696 | Records processed | 30000`
		AWS general

Tarea	Descripción	Habilidades requeridas
	2023-05-15 21:21:49. 173781 | Records processed | 40000 2023-05-15 21:21:49. 874779 | Records processed | 50000 2023-05-15 21:21:50. 705873 | Records processed | 60000 2023-05-15 21:21:51. 609335 | Records processed | 70000 2023-05-15 21:21:52. 292989 | Records processed | 80000 2023-05-15 21:21:52. 938366 | Records processed | 89280 2023-05-15 21:21:52. 938448 Seconds 6.616232 Para obtener informaci ón sobre cómo cambiar la frecuencia de impresión, consulte el archivo README del GitHub repositorio.	

Tarea	Descripción	Habilidades requeridas
Examinar el archivo ASCII.	1. Compruebe la hora de creación del archivo extract-ebcdic-to-ascii/cobpack.ascii.txt para comprobar que se ha creado recientemente. 2. En la EC2 consola de Amazon, introduce el siguiente comando. Se abrirá el primer registro del archivo ASCII. `head sample-data/COBPACK.ASCII.txt -n 1| xxd` 3. Examine el contenido del primer registro. Ya que los archivos EBCDIC suelen ser binarios, no tienen caracteres especiales de retorno y alimentación de línea (CRLF). El script extract_ebcdic_to_ascii.py añade un carácter de barra vertical como separador de columnas, que se define en los parámetros del script. Si ha usado el archivo EBCDIC proporcionado como ejemplo, el primer registro del archivo ASCII será este.	AWS general, Linux

Tarea	Descripción	Habilidades requeridas
	00000000: 2d30 3030 3030 3030 3030 3130 3030 3030 -000000000100000 00000010: 3030 307c 3030 3030 3030 3030 3031 3030 000|00000 0000100 00000020: 3030 3030 3030 7c2d 3030 3030 3030 3030 000000|-0 0000000 00000030: 3031 3030 3030 3030 3030 7c30 7c30 7c31 0100000000| 0|0|1 00000040: 3030 3030 3030 3030 7c2d 3130 3030 3030 00000000| -100000 00000050: 3030 307c 3130 3030 3030 3030 307c 2d31 000|10000 0000|-1 00000060: 3030 3030 3030 3030 7c30 3030 3030 7c30 00000000| 00000|0 00000070: 3030 3030 7c31 3030 3030 3030 3030 7c2d 0000|1000 00000|- 00000080: 3130 3030 3030 3030 307c 3030 3030 3030 100000000| 000000 00000090: 3030 3030 3130 3030 3030 3030 307c 2d30 000010000 0000|-0 000000a0: 3030 3030 3030 3030 3031 3030	

Tarea	Descripción	Habilidades requeridas
	3030 3030 000000000 1000000 000000b0: 3030 7c41 7c41 7c0a 00|A|A|.	

Tarea	Descripción	Habilidades requeridas

Evalúe el archivo EBCDIC.	En la EC2 consola de Amazon, introduce el siguiente comando. Esto abre el primer registro del archivo EBCDIC.
	
	`head sample-data/COBPACK.OUTFILE.txt -c 150 | xxd`
	
	Si ha usado el archivo EBCDIC de ejemplo, el resultado es el siguiente.
	
	`00000000: 60f0 f0f0 f0f0 f0f0 f0f0 f0f0 f1f0 f0f0 f0f0 f0f0 `........ .... 00000010: f0f0 f0f0 f0f0 f0f0 f0f0 f0f0 f1f0 f0f0 ..... 00000020: f0f0 f0f0 f0f0 f0f0 f0f0 f0f0 f1f0 ..... 00000030: f0f0 f0f0 f0f0 d000 0000 0005 f5e1 00fa ..... 00000040: 0a1f 0000 0000 0005 f5e1 00ff ffff fffa ..... 00000050: 0a1f 0000 000f 0000 0c10 0000 000f 1000 ..... 00000060: 0000 0d00 0000 0000 1000 0000`
		AWS general, Linux, EBCDIC

Tarea	Descripción	Habilidades requeridas
	0f00 0000 .... 00000070: 0000 1000 0000 0dc1 c100 0000 0000 0000 .... 00000080: 0000 0000 0000 0000 0000 0000 0000 0000 .... 00000090: 0000 0000 0000 ...... Para evaluar la equivalencia entre los archivos de origen y de destino, es necesario un conocimiento exhaustivo de EBCDIC. Por ejemplo, el primer carácter del archivo EBCDIC de muestra es un guion (-). En la notación hexadecimal del archivo EBCDIC, este carácter se representa mediante 60, y en la notación hexadecimal del archivo ASCII, este carácter se representa mediante 2D. Para obtener una tabla EBCDIC-to-ASCII de conversión, consulte EBCDIC a ASCII en el sitio web de IBM.	

Recursos relacionados

Referencias

- El conjunto de caracteres EBCDIC (documentación de IBM)
- EBCDIC a ASCII (documentación de IBM)
- COBOL (documentación de IBM)
- Conceptos básicos de JCL (documentación de IBM)
- Conéctate a tu instancia de Linux (EC2 documentación de Amazon)

Tutoriales

- Programar trabajos de SSH con AWS Lambda (publicación del blog de AWS)
- Uso de un desencadenador de Amazon S3 para invocar una función de Lambda (documentación de AWS Lambda)

Convierta archivos de mainframe del formato EBCDIC al formato ASCII delimitado por caracteres en Amazon S3 mediante AWS Lambda

Luis Gustavo Dantas, Amazon Web Services

Resumen

Este patrón le muestra cómo lanzar una AWS Lambda función que convierte automáticamente los archivos EBCDIC (Extended Binary Coded Decimal Interchange Code) de mainframe en archivos del Código Estándar Estadounidense para el Intercambio de Información (ASCII) delimitados por caracteres. La función de Lambda se ejecuta después de cargar los archivos ASCII en un bucket de Amazon Simple Storage Service (Amazon S3). Tras la conversión de archivos, puede leer los archivos ASCII en cargas de trabajo basadas en x86 o cargarlos en bases de datos modernas.

El enfoque de conversión de archivos que se muestra en este patrón puede ayudarle a superar los desafíos que supone trabajar con archivos EBCDIC en entornos modernos. Los archivos codificados en EBCDIC suelen contener datos representados en formato binario o decimal empaquetado, y los campos tienen una longitud fija. Estas características crean obstáculos porque las cargas de trabajo modernas basadas en x86 o los entornos distribuidos suelen trabajar con datos codificados en ASCII y no pueden procesar archivos EBCDIC.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Un bucket de Amazon S3
- Un usuario AWS Identity and Access Management (IAM) con permisos administrativos
- AWS CloudShell
- Python 3.8.0 o posterior
- Archivo plano codificado en EBCDIC y su estructura de datos correspondiente en un cuaderno de texto común en un lenguaje empresarial común (COBOL)

> **Note**
>
> Este patrón utiliza un archivo EBCDIC de muestra (CLIENT.EBCDIC.txt) y su cuaderno de texto COBOL correspondiente (COBKS05.cpy). Ambos archivos están disponibles en el GitHub mainframe-data-utilitiesrepositorio.

Limitaciones

- Los cuadernos de COBOL suelen contener múltiples definiciones de diseño. El mainframe-data-utilitiesproyecto puede analizar este tipo de cuaderno, pero no puede deducir qué diseño considerar en la conversión de datos. Esto se debe a que los cuadernos no tienen esta lógica (que permanece en los programas COBOL). Por lo tanto, debe configurar manualmente las reglas para seleccionar los diseños después de analizar el cuaderno.
- Este patrón está sujeto a las cuotas de Lambda.

Arquitectura

Pila de tecnología de origen

- IBM z/OS, IBM i y otros sistemas EBCDIC
- Archivos secuenciales con datos codificados en EBCDIC (como descargas de IBM Db2)
- Cuaderno COBOL

Pila de tecnología de destino

- Amazon S3
- Notificaciones de eventos de Amazon S3
- IAM
- Función de Lambda
- Python 3.8 o posterior
- Utilidades de datos de unidad central
- Metadatos JSON
- Archivos ASCII delimitados por caracteres

Arquitectura de destino

El siguiente diagrama muestra una arquitectura para convertir archivos EBCDIC de mainframe en archivos ASCII.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El usuario ejecuta el script del analizador del cuaderno para convertir el cuaderno COBOL en un archivo JSON.
2. El usuario carga los metadatos JSON en un bucket de Amazon S3. Esto hace que los metadatos sean legibles por la función de Lambda de conversión de datos.
3. El usuario o un proceso automatizado carga el archivo EBCDIC en el bucket de Amazon S3.
4. El evento de notificación de Amazon S3 activa la función de Lambda de conversión de datos.
5. AWS verifica los permisos de lectura/escritura del bucket de Amazon S3 para la función Lambda.
6. Lambda lee el archivo del bucket de Amazon S3 y lo convierte localmente de EBCDIC a ASCII.
7. Lambda registra el estado del proceso en Amazon. CloudWatch
8. Lambda vuelve a escribir el archivo ASCII en Amazon S3.

> **Note**
>
> El script del analizador del cuaderno se ejecuta una sola vez para realizar la conversión de metadatos al formato JSON, que posteriormente se almacena en un bucket de Amazon S3. Tras la conversión inicial, todos los archivos EBCDIC que hagan referencia al mismo archivo JSON del bucket de Amazon S3 utilizarán la configuración de metadatos existente.

Tools (Herramientas)

Servicios de AWS

- Amazon le CloudWatch ayuda a supervisar las métricas de sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

- AWS CloudShelles un shell basado en un navegador que puede utilizar para gestionar Servicios de AWS mediante AWS Command Line Interface (AWS CLI) y una gama de herramientas de desarrollo preinstaladas.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Lambda ejecuta el código solo cuando es necesario y escala la capacidad de manera automática, por lo que solo pagará por el tiempo informático que utilice.

Otras herramientas

- GitHubes un servicio de alojamiento de código que proporciona herramientas de colaboración y control de versiones.
- Python es un lenguaje de programación de alto nivel.

Código

El código de este patrón está disponible en el GitHub mainframe-data-utilitiesrepositorio.

Prácticas recomendadas

Tenga en cuenta las siguientes prácticas recomendadas:

- Establezca los permisos requeridos en el nivel de nombre de recurso de Amazon (ARN).
- Otorgue siempre permisos con privilegios mínimos para las políticas de IAM. Para obtener más información, consulte Prácticas recomendadas de seguridad en IAM en la documentación de IAM.

Epics

Cree variables de entorno y una carpeta de trabajo

Tarea	Descripción	Habilidades requeridas
Crear variables de entorno.	Copie las siguientes variables de entorno en un editor de texto y, a continuac	AWS general

Tarea	Descripción	Habilidades requeridas

	ión, sustituya los valores `<placeholder>` del siguiente ejemplo por los valores de sus recursos:
	
	`bucket=<your_bucket_name>`
	`account=<your_account_number>`
	`region=<your_region_code>`
	
	Note
	Creará referencias a su bucket de Amazon S3 y Región de AWS más adelante. Cuenta de AWS
	
	Para definir las variables de entorno, abra la CloudShell consola y, a continuación, copie y pegue las variables de entorno actualizadas en la línea de comandos.
	
	Note
	Debe repetir este paso cada vez que se reinicie la CloudShell sesión.	

Tarea	Descripción	Habilidades requeridas
Cree una carpeta de trabajo.	Para simplificar el proceso de limpieza de recursos más adelante, cree una carpeta de trabajo CloudShell ejecutando el siguiente comando: `mkdir workdir; cd workdir` **Note** Debe cambiar el directorio al directorio de trabajo (`workdir`) cada vez que pierda la conexión con la CloudShell sesión.	AWS general

Definir una política y un rol de IAM

Tarea	Descripción	Habilidades requeridas
Cree una política de confianza para la función de Lambda.	El convertidor EBCDIC se ejecuta en una función de Lambda. La función debe tener un rol de IAM. Antes de crear el rol de IAM, debe definir un documento de política de confianza que permita a los recursos asumir esa política. Desde la carpeta de CloudShell trabajo, cree	AWS general

Tarea	Descripción	Habilidades requeridas

	un documento de política ejecutando el siguiente comando:
	
	`E2ATrustPol=$(cat <<EOF`
	`{`
	`  "Version": "2012-10-17",`
	`  "Statement": [`
	`  {`
	`  "Effect": "Allow",`
	`  "Principal": {`
	`  "Service": "lambda.amazonaws.com"`
	`  },`
	`  "Action": "sts:AssumeRole"`
	`  }`
	`  ]`
	`}`
	`EOF`
	`)`
	`printf "$E2ATrustPol" > E2ATrustPol.json`	

Crear el rol de IAM para la conversión de Lambda.	Para crear un rol de IAM, ejecute el siguiente AWS CLI comando desde la carpeta de CloudShell trabajo: `aws iam create-role --role-name E2AConvLambdaRole --assume-role-policy-document file://E2ATrustPol.json`	AWS general

Tarea	Descripción	Habilidades requeridas

Cree el documento de política de IAM para la función de Lambda.	La función Lambda debe tener acceso de lectura y escritura al bucket de Amazon S3 y permisos de escritura para Amazon Logs. CloudWatch
	
	Para crear una política de IAM, ejecute el siguiente comando desde la carpeta de trabajo: CloudShell
	
	`E2APolicy=$(cat <<EOF`
	`{`
	`"Version": "2012-10-17",`
	`"Statement": [`
	`{`
	`"Sid": "Logs",`
	`"Effect": "Allow",`
	`"Action": [`
	`"logs:PutLogEvents",`
	`"logs:CreateLogStream",`
	`"logs:CreateLogGroup"`
	`],`
	`"Resource": [`
	`"arn:aws:logs:*:*:log-group:*",`
	`"arn:aws:logs:*:*:log-group:*:log-stream:*"`
	`]
		AWS general

Tarea	Descripción	Habilidades requeridas

	<pre> },
	        {
	            "Sid": "S3",
	            "Effect":
	"Allow",
	            "Action": [
	
	"s3:GetObject",
	
	"s3:PutObject",
	
	"s3:GetObjectVersion"
	            ],
	            "Resource":
	[
	
	"arn:aws:s3:::%s/*",
	
	"arn:aws:s3:::%s"
	            ]
	        }
	    ]
	}
	EOF
	)
	printf "$E2APolicy"
	"$bucket" "$bucket"
	> E2AConvLambdaPolic
	y.json</pre>	

Tarea	Descripción	Habilidades requeridas
Adjuntar los documentos sobre la política de IAM al rol de IAM.	Para adjuntar la política de IAM a la función de IAM, introduzca el siguiente comando desde su CloudShell carpeta de trabajo: `aws iam put-role-policy --role-name E2AConvLambdaRole --policy-name E2AConvLambdaPolicy --policy-document file://E2AConvLambdaPolicy.json`	AWS general

Crear la función de Lambda para la conversión de EBCDIC

Tarea	Descripción	Habilidades requeridas
Descargar el código fuente de conversión a EBCDIC.	Desde la carpeta de CloudShell trabajo, ejecute el siguiente comando para descargar el código mainframe-data-utilities fuente desde la que se encuentra: GitHub `git clone https://github.com/aws-samples/mainframe-data-utilities.git mdu`	AWS general
Crear el paquete ZIP.	Desde la carpeta de CloudShell trabajo, introduzca el siguiente comando para crear el paquete ZIP que crea	AWS general

Tarea	Descripción	Habilidades requeridas
	la función Lambda para la conversión a EBCDIC: `cd mdu; zip ../mdu.zip *.py; cd ..`	

Tarea	Descripción	Habilidades requeridas
Crear la función de Lambda.	Desde la carpeta de CloudShell trabajo, introduzc a el siguiente comando para crear la función Lambda para la conversión a EBCDIC: `aws lambda create-fu nction \ --function-name E2A \ --runtime python3.9 \ --zip-file fileb://m du.zip \ --handler extract_e bcdic_to_ascii.lam bda_handler \ --role arn:aws:i am::$account:role/ E2AConvLambdaRole \ --timeout 10 \ --environment "Variable s={layout=$bucket/ layout/}"` **Note** El diseño de las variables de entorno indica a la función de Lambda dónde residen los metadatos de JSON.	AWS general

Tarea	Descripción	Habilidades requeridas
Crear la política basada en recursos para la función de Lambda.	En la carpeta de CloudShell trabajo, introduzca el siguiente comando para permitir que la notificación de eventos de Amazon S3 active la función Lambda para la conversión a EBCDIC: `aws lambda add-permi ssion \ --function-name E2A \ --action lambda:In vokeFunction \ --principal s3.amazon aws.com \ --source-arn arn:aws:s 3:::$bucket \ --source-account $account \ --statement-id 1`	AWS general

Notificaciones de eventos de Amazon S3

Tarea	Descripción	Habilidades requeridas
Cree el documento de configuración para la notificac ión de eventos de Amazon S3.	La notificación de eventos de Amazon S3 inicia la función de Lambda de conversión EBCDIC cuando los archivos se colocan en la carpeta de entrada. Desde la carpeta de CloudShell trabajo, ejecute el siguiente comando para crear el documento JSON para la	AWS general

Tarea	Descripción	Habilidades requeridas

	notificación de eventos de Amazon S3:
	
	`S3E2AEvent=$(cat <<EOF`
	`{`
	`"LambdaFunctionConf`
	`igurations": [`
	`{`
	`"Id": "E2A",`
	`"LambdaFu`
	`nctionArn": "arn:aws:`
	`lambda:%s:%s:funct`
	`ion:E2A",`
	`"Events":`
	`[ "s3:ObjectCreated:`
	`Put" ],`
	`"Filter": {`
	`"Key": {`
	`"FilterRu`
	`les": [`
	`{`
	`"Name":`
	`"prefix",`
	`"Value":`
	`"input/"`
	`}`
	`]`
	`}`
	`}`
	`}`
	`]`
	`}`
	`EOF`
	`)`
	`printf "$S3E2AEvent"`
	`"$region" "$account" >`
	`S3E2AEvent.json`	

Tarea	Descripción	Habilidades requeridas
Crear notificaciones de eventos de Amazon S3.	Desde la carpeta de CloudShell trabajo, introduzca el siguiente comando para crear la notificación de eventos de Amazon S3: `aws s3api put-bucket-notification-configuration --bucket $bucket --notification-configuration file://S3E2AEvent.json`	AWS general

Crear y cargar los metadatos JSON

Tarea	Descripción	Habilidades requeridas

Analizar el cuaderno de COBOL.	Desde la carpeta de CloudShell trabajo, introduzca el siguiente comando para convertir un cuaderno de COBOL de muestra en un archivo JSON (que define cómo leer y dividir correctamente el archivo de datos):
	`python3 mdu/parse_copybook_to_json.py \`
	`-copybook mdu/LegacyReference/COBKS05.cpy \`
	`-output CLIENT.json \`
		AWS general

Tarea	Descripción	Habilidades requeridas

	`-output-s3key CLIENT.ASCII.txt \`
	`-output-s3bkt $bucket \`
	`-output-type  s3 \`
	`-print  25`	

Tarea	Descripción	Habilidades requeridas

Añada la regla de transform ación.	El archivo de datos de ejemplo y su cuaderno de notas COBOL correspondiente son archivos de varios diseños. Esto significa que la conversió n debe dividir los datos en función de determinadas reglas. En este caso, los bytes de las posiciones 3 y 4 de cada fila definen el diseño.
	
	Desde la carpeta de CloudShell trabajo, edite el `CLIENT.json` archivo y cambie el contenido de la siguiente `"transf-rule": [],` manera:
	
	`"transf-rule": [`
	`{`
	`"offset": 4,`
	`"size": 2,`
	`"hex": "0002",`
	`"transf": "transf1"`
	`},`
	`{`
	`"offset": 4,`
	`"size": 2,`
	`"hex": "0000",`
	`"transf": "transf2"`
	`}`
	`],`
		Información general sobre AWS, lade IBM y Cobol

Tarea	Descripción	Habilidades requeridas
Cargue los metadatos JSON en el bucket de Amazon S3.	Desde la carpeta de CloudShell trabajo, introduzca el siguiente AWS CLI comando para cargar los metadatos de JSON en su bucket de Amazon S3: `aws s3 cp CLIENT.json s3://$bucket/layout/CLIENT.json`	AWS general

Convertir el archivo EBCDIC

Tarea	Descripción	Habilidades requeridas
Envíe el archivo EBCDIC al bucket de Amazon S3.	Desde la carpeta de CloudShell trabajo, introduzca el siguiente comando para enviar el archivo EBCDIC al bucket de Amazon S3: `aws s3 cp mdu/sample-data/CLIENT.EBCDIC.txt s3://$bucket/input/` **Note** Se recomienda configurar carpetas diferentes para los archivos de entrada (EBCDIC) y de salida (ASCII) para evitar volver a llamar a la	AWS general

Tarea	Descripción	Habilidades requeridas
	función de conversió n de Lambda cuando el archivo ASCII se cargue en el bucket de Amazon S3.	

Tarea	Descripción	Habilidades requeridas

Comprobar la salida.	Desde la carpeta de CloudShell trabajo, introduce el siguiente comando para comprobar si el archivo ASCII se genera en tu bucket de Amazon S3:
	`aws s3 ls s3://$bucket/`
	Note
	La conversión de datos puede tardar varios segundos en realizarse. Le recomendamos que compruebe el archivo ASCII varias veces.
	Cuando el archivo ASCII esté disponible, introduzca el siguiente comando para mostrar el contenido del archivo convertido en el bucket de Amazon S3. Si lo necesita, podrá descargarlo o utilizarlo directamente del bucket de Amazon S3:
	`aws s3 cp s3://$bucket/ CLIENT.ASCII.txt - | head`
		AWS general

Tarea	Descripción	Habilidades requeridas

	Comprobar el contenido del archivo ASCII:
	
	`0|0|220|`
	`1|1|HERBERT MOHAMED|1`
	`958-08-31|BACHELOR|`
	`0010000.00|`
	`1|2|36|THE ROE AVENUE|`
	`2|1|JAYLEN GEORGE|19`
	`69-05-29|ELEMENTARY|`
	`0020000.00|`
	`2|2|365|HEATHFIELD`
	` ESPLANADE|`
	`3|1|MIKAEEL WEBER|198`
	`2-02-17|MASTER|003`
	`0000.00|`
	`3|2|4555|MORRISON`
	` STRAND|`
	`4|1|APRIL BARRERA|1`
	`967-01-12|DOCTOR|0`
	`030000.00|`
	`4|2|1311|MARMION PARK|`
	`5|1|ALEEZA PLANT|198`
	`5-03-01|BACHELOR|0`
	`008000.00|`	

Limpiar el entorno

Tarea	Descripción	Habilidades requeridas
(Opcional) Prepare las variables y la carpeta.	Si pierdes la conexión con CloudShell, vuelve a conectarte e introduce el siguiente comando para cambiar el directorio a la carpeta de trabajo:	AWS general

Tarea	Descripción	Habilidades requeridas

	`cd workdir`
	
	Asegúrese de que las variables de entorno estén definidas:
	
	`bucket=<your_bucket_name>`
	`account=<your_account_number>`
	`region=<your_region_code>`	

Eliminar la configuración de notificación para el bucket.	Desde la carpeta de CloudShell trabajo, ejecute el siguiente comando para eliminar la configuración de notificaciones de eventos de Amazon S3:
	
	`aws s3api put-bucket-notification-configuration \`
	`--bucket=$bucket \`
	`--notification-configuration="{}"`
		AWS general

Elimine la función de Lambda.	Desde la carpeta de CloudShell trabajo, introduzca el siguiente comando para eliminar la función Lambda del convertidor EBCDIC:
	
	`aws lambda delete-function \`
	`--function-name E2A`
		AWS general

Tarea	Descripción	Habilidades requeridas

Eliminar el rol y la política de IAM.	En la carpeta de CloudShell trabajo, introduzca el siguiente comando para eliminar la función y la política del conversor EBCDIC:
	`aws iam delete-role-policy \`
	`--role-name E2AConvLambdaRole \`
	`--policy-name E2AConvLambdaPolicy`
	
	`aws iam delete-role \`
	`--role-name E2AConvLambdaRole`
		AWS general

Elimine los archivos generados en el bucket de Amazon S3.	Desde la carpeta de CloudShell trabajo, introduzca el siguiente comando para eliminar los archivos generados en el bucket de Amazon S3:
	`aws s3 rm s3://$bucket/layout --recursive`
	`aws s3 rm s3://$bucket/input --recursive`
	`aws s3 rm s3://$bucket/CLIENT.ASCII.txt`
		AWS general

Tarea	Descripción	Habilidades requeridas
Elimine la carpeta de trabajo.	Desde la carpeta de CloudShell trabajo, introduzc a el siguiente comando para eliminarlos `workdir` y su contenido: `cd ..; rm -Rf workdir`	AWS general

Recursos relacionados

- Mainframe Data Utilities README () GitHub
- El conjunto de caracteres EBCDIC (documentación de IBM)
- EBCDIC a ASCII (documentación de IBM)
- COBOL (documentación de IBM)
- Uso de un activador de Amazon S3 para invocar una función AWS Lambda Lambda (documentación)

Convertir archivos de datos de mainframe con diseños de registros complejos mediante Micro Focus

Peter West, Amazon Web Services

Resumen

Nota: AWS Mainframe Modernization El servicio (experiencia de entorno de ejecución gestionado) ya no está abierto a nuevos clientes. Para obtener funciones similares a las AWS Mainframe Modernization de Service (experiencia en entornos de ejecución gestionados), explore AWS Mainframe Modernization Service (experiencia autogestionada). Los clientes existentes pueden seguir utilizando el servicio con normalidad. Para obtener más información, consulte Cambio en la disponibilidad de AWS Mainframe Modernization.

Este patrón le muestra cómo convertir archivos de datos de mainframe con datos no textuales y diseños de registros complejos, pasando de la codificación de caracteres EBCDIC (código de intercambio decimal con código binario extendido) a la codificación de caracteres ASCII (Código estándar estadounidense para el intercambio de información) mediante un archivo de estructura de Micro Focus. Para completar la conversión de archivos, siga estos pasos:

1. Prepare un único archivo fuente que describa todos los elementos de datos y los diseños de registros de su entorno de mainframe.
2. Cree un archivo de estructura que contenga el diseño de registro de los datos mediante el editor de archivos de datos de Micro Focus como parte de las herramientas clásicas de archivos de datos o herramientas de archivos de datos de Micro Focus. El archivo de estructura identifica los datos no textuales para que pueda convertir correctamente los archivos del mainframe de EBCDIC a ASCII.
3. Pruebe el archivo de estructura mediante las herramientas clásicas de archivos de datos o las herramientas de archivos de datos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Micro Focus Enterprise Developer para Windows, disponible a través de AWS Mainframe Modernization

Versiones de producto

- Micro Focus Enterprise Server 7.0 y versiones posteriores

Tools (Herramientas)

- Micro Focus Enterprise Developer proporciona el entorno de ejecución para las aplicaciones creadas con cualquier variante del entorno de desarrollo integrado (IDE) de Enterprise Developer.
- Las herramientas de archivos de datos clásicas de Micro Focus le ayudan a convertir, navegar, editar y crear archivos de datos. Las herramientas clásicas para archivos de datos incluyen el convertidor de archivos de datos, el editor de diseño de registros y el editor de archivos de datos.
- Las herramientas de archivos de datos de Micro Focus le ayudan a crear, editar y mover archivos de datos. Las herramientas de archivos de datos incluyen el editor de archivos de datos, las utilidades de conversión de archivos y la utilidad de línea de comandos de estructura de archivos de datos.

Epics

Preparación del archivo de origen

Tarea	Descripción	Habilidades requeridas
Identificar los componentes de origen.	Identificar todos los diseños de registro posibles para el archivo, incluidas las redefinic iones que contengan datos no textuales. Si tiene diseños que contienen redefiniciones, debe reducir estos diseños a diseños únicos que describan cada posible permutación de la estructura de datos. Por lo general, los diseños de registros de un archivo de datos se pueden describir	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	mediante los siguientes arquetipos: • Diseño de registro con sólo datos de texto • Diseño de registro con datos no textuales • Diseño de registros con datos no textuales subordinados a una cláusula REDEFINES Para obtener más informaci ón sobre cómo crear diseños de registros aplanados para archivos que contienen diseños de registros complejos, consulte Realojar aplicaciones EBCDIC en entornos ASCII para migracion es de mainframe.	

Tarea	Descripción	Habilidades requeridas

Identificar las condiciones de diseño de los registros.	En el caso de los archivos con varios diseños de registro o los archivos que contienen diseños complejos con una cláusula REDEFINES, identifiq ue los datos y las condicion es de un registro que puede usar para definir qué diseño usar durante la conversión. Le recomendamos que analice esta tarea con un experto en la materia (SME) que conozca los programas que procesan estos archivos.
	
	Por ejemplo, un archivo puede contener dos tipos de registros que contienen datos no textuales. Puede inspeccionar el código fuente y encontrar código similar al siguiente:
	
	`MOVE "M" TO PART-TYPE`
	`MOVE "MAIN ASSEMBLY" TO`
	`PART-NAME`
	`MOVE "S" TO PART-TYPE`
	`MOVE "SUB ASSEMBLY 1"`
	`TO PART-NAME`
	
	El código ayuda a identificar lo siguiente:
	
	• El campo «TIPO DE PIEZA» se utiliza para determinar el tipo de registro
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	• El valor «M» se utiliza para el «M-PART-RECORD» • El valor «S» se utiliza para el «S-PART-RECORD» Puede documentar los valores que utiliza este campo para asociar los diseños de registros con los registros de datos correctos del archivo.	

Tarea	Descripción	Habilidades requeridas
Cree el archivo de origen.	Si el archivo se describe en varios archivos fuente o si el diseño de registros contiene datos no textuales que están subordinados a una cláusula REDEFINES, cree un nuevo archivo fuente que contenga los diseños de registros. No es necesario que el nuevo programa describa el archivo mediante las instrucciones SELECT y FD. El programa simplemente puede contener las descripciones de los registros en 10 niveles dentro de Working-Storage. **Note** Puede crear un archivo de origen para cada archivo de datos o crear un archivo de origen maestro que describa todos los archivos de datos.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Compilar el código fuente.	Compile el archivo fuente para crear el diccionario de datos. Se recomienda compilar el archivo fuente mediante el juego de caracteres EBCDIC. Si utiliza la directiva IBMCOMP o las directivas ODOSLIDE, también debe utilizar estas directivas en el archivo fuente. **Note** IBMCOMP afecta al almacenamiento de bytes de los campos COMP y ODOSLIDE afecta al relleno cuando se producen estructuras variables. Si estas directivas están configuradas incorrectamente, la herramienta de conversión no leerá el registro de datos correctamente. Esto da como resultado datos incorrectos en el archivo convertido.	Desarrollador de aplicaciones

(Opción A) Cree el archivo de estructura con las herramientas clásicas de archivos de datos

Tarea	Descripción	Habilidades requeridas
Inicie la herramienta y cargue el diccionario.	1. Seleccione el icono del menú Inicio de Windows, busque y seleccione Micro Focus Enterprise Developer y, a continuación, seleccione Herramientas clásicas de archivos de datos. 2. Seleccione Archivo y, a continuación, Diseño de registro. 3. En el cuadro de diálogo Seleccione un archivo a partir del cual crear los diseños, en Nombre de archivo, seleccione el archivo IDY (`.idy`) que se creó al compilar el archivo fuente anteriormente. A continuación, seleccione Abrir. 4. Para confirmar que Herramientas clásicas de archivos de datos utiliza EBCDIC, en el cuadro de diálogo Herramientas de archivos de datos, elija SÍ si el archivo IDY está establecido en EBCDIC y Herramientas de datos en ANSI.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Cree el diseño de registro predeterminado.	Utilice el diseño de registro predeterminado para todos los registros que no coincidan con ningún diseño condicional. 1. En la ventana de diseño, expanda la estructura de datos y, a continuación, busque el nivel 01 utilizado para el diseño predeterm inado. 2. Haga clic con el botón derecho en el elemento 01 y seleccione Diseño nuevo. 3. En el cuadro de diálogo del asistente de diseño de nuevos registros, seleccion e Diseño predeterminado y, a continuación, Siguiente. 4. Seleccione Finalizar. El diseño predeterminado aparece en el panel Diseños y se puede identificar mediante el icono rojo de la carpeta.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Cree un diseño de registro condicional.	Utilice el diseño de registro condicional cuando haya más de un diseño de registro en un archivo. 1. En el panel Diseños, expanda la estructura de datos y, a continuación, localice el nivel 01 utilizado para el diseño condicional. 2. Haga clic con el botón derecho en el elemento 01 y seleccione Diseño nuevo. 3. En el cuadro de diálogo del asistente de diseño de nuevos registros, seleccion e Diseño condicional y, a continuación, Siguiente. 4. Seleccione Finalizar. El diseño condicional aparece en el panel Diseños y se puede identificar mediante el icono de carpeta amarillo. 5. Amplíe el diseño condicion al, haga clic con el botón derecho en el campo en el que debe colocar una condición y, a continuación, seleccione Propiedades. 6. En el cuadro de diálogo Propiedades del campo, introduzca la condición. Confirme que el juego de caracteres esté establecido	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	en EBCDIC y, a continuación, pulse OK. Aparece una marca de verificación junto al campo que tiene una condición establecida. 7. Repita los pasos 5 y 6 para cualquier otro campo que requiera condiciones para este diseño. 8. Repita los pasos 1 a 6 para cualquier otro diseño condicional que deba añadirse. 9. Seleccione Archivo, luego, Guardar como y, a continuación, guarde el archivo de estructura en el disco.	

(Opción B) Cree el archivo de estructura mediante las herramientas de archivos de datos

Tarea	Descripción	Habilidades requeridas
Inicie la herramienta y cargue el diccionario.	1. Seleccione el icono del menú Inicio de Windows, busque y seleccione Micro Focus Enterprise Developer y, a continuación, seleccione Herramientas de archivos de datos. 2. Seleccione Archivo, Nuevo o Archivo de estructura.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	3. En el cuadro de diálogo Abrir, en Nombre de archivo, seleccione el archivo IDY (`.idy`) que se creó al compilar el archivo fuente anteriormente. A continuación, seleccione Abrir. 4. Para confirmar que las herramientas de archivos de datos utilizan EBCDIC, confirme que el menú desplegable de la sección Depurar archivos esté configurado en EBCDIC.	

Tarea	Descripción	Habilidades requeridas
Cree el diseño de registro predeterminado.	Utilice el diseño de registro predeterminado para todos los registros que no coincidan con ningún diseño condicional. 1. En la sección Diseños disponibles del panel izquierdo, expanda la estructura de datos y, a continuación, localice el nivel 01 utilizado para el diseño predeterminado. 2. Haga clic con el botón derecho en el elemento 01 y seleccione Crear diseño predeterminado. El diseño predeterminado aparece en el panel Diseños y se puede identificar mediante el icono azul en forma de “D”.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Cree un diseño de registro condicional.	Utilice el diseño de registro condicional cuando haya más de un diseño de registro en un archivo. 1. En la sección Diseños seleccionados del panel derecho, expanda la estructura de datos y, a continuación, localice el nivel 01 utilizado para el diseño condicional. 2. Haga clic con el botón derecho en el elemento 01 y elija Crear diseño condicional. El diseño condicional aparece en el panel de diseños, en el lado derecho, y se puede identificar mediante el icono verde en forma de «C». 3. Amplíe el diseño condicional, haga clic con el botón derecho en el campo en el que debe colocar una condición y, a continuación, seleccione Propiedades. 4. En el cuadro de diálogo Propiedades del campo, introduzca la condición. Confirme que el juego de caracteres esté establecido en EBCDIC y, a continuación, pulse OK. Aparece	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	un icono rojo “SI” junto al campo que tiene una condición establecida. 5. Repita los pasos 3 y 4 para cualquier otro campo que requiera condiciones para este diseño. 6. Repita los pasos 1 a 4 para cualquier otro diseño condicional que deba añadirse. 7. Seleccione Archivo, luego, Guardar como y, a continuación, guarde el archivo de estructura en el disco.	

(Opción A) Pruebe el archivo de estructura con las herramientas clásicas de archivos de datos

Tarea	Descripción	Habilidades requeridas
Probar un archivo de datos EBCDIC.	Confirme que puede usar el archivo de estructura para ver correctamente un archivo de datos de prueba del EBCDIC. 1. Seleccione el icono del menú Inicio de Windows, busque Micro Focus Enterprise Developer y, a continuación, Herramientas clásicas de datos. 2. Seleccione Archivo y, a continuación, Abrir.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	3. En el cuadro de diálogo Abrir, en Nombre de archivo, seleccione el conjunto de datos EBCDIC y, a continuación, Abrir. 4. Seleccione Archivo, Editor de archivos de datos y Cargue diseños de registros . 5. En el cuadro de diálogo Abrir, en Nombre de archivo, seleccione el archivo de estructura y, a continuación, Abrir. 6. Para confirmar que el modo de juego de caractere s está establecido en EBCDIC, confirme que el menú desplegable está configurado en EBCDIC. Puede ver los datos de registro sin procesar en el panel izquierdo y los datos formateados en el panel derecho. 7. Elija varios registros para asegurarse de que todos los formatos se renderizan con el diseño correcto.	

(Opción B) Pruebe el archivo de estructura con las herramientas de archivos de datos

Tarea	Descripción	Habilidades requeridas
Probar un archivo de datos EBCDIC.	Confirme que puede usar el archivo de estructura para ver correctamente un archivo de datos de prueba del EBCDIC. 1. Seleccione el icono del menú Inicio de Windows, busque Desarrollador de empresa Micro Focus y, a continuación, Herramientas de archivos de datos. 2. Seleccione Archivo, Abrir o Archivo de datos. 3. En el cuadro de diálogo Abrir archivo de datos, en la pestaña Local, en Nombre de archivo, seleccione Examinar para buscar la ubicación del archivo de prueba del EBCDIC. 4. En Archivo de estructur a (opcional), seleccione Examinar para buscar la ubicación del archivo de estructura. 5. En la sección Detalles del archivo, introduzca los detalles del archivo y confirme que la codificac ión esté establecida en EBCDIC.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	6. Elija el modo Abierto Compartido o Abierto Exclusivo en función de sus requisitos. 7. Confirme que el menú desplegable de la sección Apariencia de la barra de herramientas esté configurado como EBCDIC. Verá los datos de registro sin procesar en el panel izquierdo y los datos formateados en el panel derecho. 8. Elija varios registros para asegurarse de que todos los formatos se renderizan con el diseño correcto.	

Pruebe la conversión de archivos de datos

Tarea	Descripción	Habilidades requeridas
Probar la conversión de un archivo EBCDIC.	1. Elija el icono del menú Inicio de Windows, busque y seleccione Desarrollador de empresa Micro Focus y, a continuación, Herramien tas clásicas de datos. 2. Seleccione Herramientas y, a continuación, Consola. 3. En el cuadro de diálogo Convertir archivos de	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	datos, en la sección Archivo de entrada, en Nombre de archivo, seleccione Examinar para buscar y seleccionar el archivo de entrada EBCDIC. Confirme que el conjunto de caracteres esté establecido en EBCDIC. 4. En la sección Conversió n de juegos de caractere s, active las casillas de verificación Convertir juegos de caracteres y Registros que contengan elementos de datos que no sean texto. Elija Seleccionar diseño para la conversión y, a continuac ión, Examinar para buscar y seleccionar el archivo de estructura. 5. En la sección Nuevo archivo, en Nombre de archivo, introduzca la ruta y el nombre del archivo de salida ASCII que desee crear. De forma predeterm inada, la herramienta de conversión tiene el mismo formato que el archivo de entrada. Para realizar pruebas, deje las opciones	

Tarea	Descripción	Habilidades requeridas
	con sus valores predeterminados. 6. Seleccione Convertir. 7. Siga los pasos de la sección (opción A) Pruebe el archivo de estructura con las herramientas clásicas de archivos de datos u (opción B) Pruebe el archivo de estructura con las herramientas de archivos de dato, pero cargue el archivo de salida ASCII en lugar del archivo EBCDIC. 8. Cargue los archivos EBCDIC y ASCII en el editor de archivos de datos y, a continuación, compare los archivos uno al lado del otro para comprobar la precisión de la conversión.	

Recursos relacionados

- Micro Focus (documentación de Micro Focus)
- Unidades centrales y código heredado (Blog de AWS)
- AWS Prescriptive Guidance (documentación de AWS)
- Documentación de AWS (documentación de AWS)
- Referencia general de AWS (documentación de AWS)
- Glosario de AWS (documentación de AWS)

Implementar un entorno para aplicaciones de Blu Age en contenedores mediante Terraform

Richard Milner-Watts, Amazon Web Services

Resumen

La migración de las cargas de trabajo de mainframe heredadas a arquitecturas de nube modernas puede eliminar los costos de mantenimiento de un mainframe, costos que solo aumentan a medida que el entorno envejece. Sin embargo, la migración de los trabajos desde un mainframe puede plantear desafíos únicos. Es posible que los recursos internos no estén familiarizados con la lógica del trabajo, y el alto rendimiento de los mainframes en estas tareas especializadas puede resultar difícil de replicar en comparación con el rendimiento generalizado de los mainframes en estas tareas especializadas. CPUs Reescribir estas tareas puede ser una tarea ardua y requerir un esfuerzo considerable.

Blu Age convierte las cargas de trabajo heredadas de los mainframes en código Java moderno, que luego puede ejecutar como un contenedor.

Este patrón proporciona una muestra de arquitectura sin servidor para ejecutar una aplicación en contenedores que se ha modernizado con la herramienta Blu Age. Los archivos HashiCorp Terraform incluidos crearán una arquitectura segura para la organización de los contenedores de Blu Age, que admitirá tanto las tareas por lotes como los servicios en tiempo real.

Para obtener más información sobre la modernización de sus cargas de trabajo mediante el uso de Blu Age y los servicios de AWS, consulte estas publicaciones en las recomendaciones de AWS:

- Ejecución de cargas de trabajo de mainframe que se han modernizado con Blu Age en una infraestructura sin servidor de AWS
- Almacenamiento en contenedores de las cargas de trabajo de mainframe que Blu Age ha modernizado

Si necesita ayuda para utilizar Blu Age para modernizar las cargas de trabajo de sus mainframes, póngase en contacto con el equipo de Blu Age seleccionando la opción Contactar con nuestros expertos en el sitio web de Blu Age. Si necesita ayuda para migrar sus cargas de trabajo modernizadas a AWS, integrarlas con los servicios de AWS y pasarlas a producción, póngase en contacto con su administrador de cuentas de AWS o rellene el formulario de AWS Professional Services.

Requisitos previos y limitaciones

Requisitos previos

- La aplicación en contenedores de muestra de Blu Age que proporciona el patrón Almacenamiento en contenedores de las cargas de trabajo de mainframe que Blu Age ha modernizado. La aplicación de muestra proporciona la lógica necesaria para gestionar el procesamiento de las entradas y salidas de la aplicación modernizada y se puede integrar con esta arquitectura.
- Se requiere Terraform para implementar estos recursos.

Limitaciones

- Amazon Elastic Container Service (Amazon ECS) limita los recursos de tareas que se pueden poner a disposición del contenedor. Estos recursos incluyen la CPU, la RAM y el almacenamiento. Por ejemplo, cuando se utiliza Amazon ECS con AWS Fargate, se aplican los límites de recursos de la tarea.

Versiones de producto

Esta solución se probó con las siguientes versiones:

- Terraform 1.3.6
- Proveedor 4.46.0 de AWS para Terraform

Arquitectura

Pila de tecnología de origen

- Blu Age
- Terraform

Pila de tecnología de destino

- Amazon Aurora compatible con PostgreSQL
- AWS Backup
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon ECS

- Servicio AWS Identity and Access Management (IAM)
- AWS Key Management Server (AWS KMS)
- AWS Secrets Manager
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- AWS Step Functions
- AWS Systems Manager

Arquitectura de destino

En el siguiente diagrama se muestra la arquitectura de la solución.

1. La solución implementa los siguientes roles de IAM:
   - Rol de tarea por lotes
   - Rol de ejecución de tareas por lotes
   - Rol de tarea de servicio
   - Rol de ejecución de tareas del servicio
   - Rol de Step Functions
   - Rol de AWS Backup
   - Rol de monitorización mejorada RDS.

   Los roles se ajustan a los principios de acceso de privilegios mínimos.
2. Amazon ECR se utiliza para almacenar la imagen del contenedor que está orquestada por este patrón.
3. El Almacén de parámetros de AWS Systems Manager proporciona datos de configuración sobre cada entorno a la definición de tareas de Amazon ECS durante el tiempo de ejecución.
4. AWS Secrets Manager proporciona datos de configuración sobre cada entorno a la definición de tareas de Amazon ECS durante el tiempo de ejecución. AWS KMS cifró los datos.
5. Los módulos Terraform crean definiciones de tareas de Amazon ECS para todas las tareas en tiempo real y por lotes.
6. Amazon ECS ejecuta una tarea por lotes utilizando AWS Fargate como motor de computación. Se trata de una tarea de corta duración, iniciada según lo exigido por AWS Step Functions.

7. Amazon Aurora, compatible con PostgreSQL, proporciona una base de datos para admitir la aplicación modernizada. Esto reemplaza a las bases de datos de mainframe, como IBM Db2 o IBM IMS DB.
8. Amazon ECS ejecuta un servicio de larga duración para ofrecer una carga de trabajo modernizada en tiempo real. Estas aplicaciones sin estado se ejecutan de forma permanente con contenedores repartidos entre las zonas de disponibilidad.
9. Se utiliza un equilibrador de carga de red para conceder acceso a la carga de trabajo en tiempo real. El equilibrador de carga de red es compatible con protocolos anteriores, como IBM CICS. Como alternativa, puede utilizar el equilibrador de carga de aplicación con cargas de trabajo basadas en HTTP.
10. Amazon S3 proporciona almacenamiento de objetos para las entradas y salidas de los trabajos. El contenedor debe gestionar las operaciones de extracción y envío a Amazon S3 a fin de preparar el directorio de trabajo para la aplicación Blu Age.
11. El servicio AWS Step Functions se utiliza para orquestar la ejecución de las tareas de Amazon ECS para procesar las cargas de trabajo por lotes.
12. Los temas de SNS para cada carga de trabajo por lotes se utilizan para integrar la aplicación modernizada con otros sistemas, como el correo electrónico, o para iniciar acciones adicionales, como entregar los objetos de salida de Amazon S3 a FTP.

> **Note**
>
> De forma predeterminada, la solución no tiene acceso a Internet. Este patrón supone que la nube privada virtual (VPC) se conectará a otras redes mediante un servicio como AWS Transit Gateway. Por lo tanto, se implementan varios puntos de conexión de VPC de interfaz para permitir el acceso a los servicios de AWS que utiliza la solución. Para activar el acceso directo a Internet, puede utilizar el conmutador del módulo Terraform para reemplazar los puntos de conexión de VPC por una puerta de enlace de Internet y los recursos asociados.

Automatizar y escalar

El uso de recursos sin servidor en todo este patrón ayuda a garantizar que, al escalar horizontalmente, haya pocos límites en la escala de este diseño. Esto reduce los problemas de vecino ruidoso, como la competencia por los recursos de computación que podría surgir en el mainframe original. Las tareas por lotes se pueden programar para que se ejecuten simultáneamente según sea necesario.

Los contenedores individuales están limitados por los tamaños máximos admitidos por Fargate. Para obtener más información, consulte la sección CPU de tareas y memoria en la documentación de Amazon ECS.

Para escalar las cargas de trabajo en tiempo real de forma horizontal, puede añadir contenedores.

Tools (Herramientas)

Servicios de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.
- AWS Backup es un servicio totalmente gestionado que le ayuda a centralizar y automatizar la protección de datos Servicios de AWS tanto en la nube como en las instalaciones.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores escalable y rápido que ayuda a ejecutar, detener y administrar contenedores en un clúster.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.
- AWS Secrets Manager le permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Step Functions es un servicio de organización sin servidor que le ayuda a combinar AWS Lambda funciones y otras Servicios de AWS para crear aplicaciones críticas para la empresa.
- El Almacén de parámetros de AWS Systems Manager proporciona un almacenamiento seguro y jerárquico para administrar los datos de configuración y los secretos.

Otros servicios

- HashiCorp Terraform es una herramienta de infraestructura como código (IaC) que facilita usar el código para aprovisionar y administrar los recursos y la infraestructura en la nube. Este patrón usa Terraform para crear la arquitectura de muestra.

Repositorio de código

El código fuente de este patrón está disponible en el repositorio GitHub Blu Age Sample ECS Infrastructure (Terraform).

Prácticas recomendadas

- Para los entornos de prueba, use características como la opción `forceDate` para configurar la aplicación modernizada para generar resultados de prueba consistentes ejecutándola siempre durante un período de tiempo conocido.
- Ajuste cada tarea de forma individual para consumir la cantidad óptima de recursos. Puede utilizar Amazon CloudWatch Container Insights para obtener orientación sobre posibles cuellos de botella.

Epics

Preparación del entorno para la implementación

Tarea	Descripción	Habilidades requeridas
Clone el código fuente de la solución.	Clone el código de la solución del proyecto. GitHub	DevOps ingeniero
Impulse el entorno mediante la implementación de recursos para almacenar el estado de Terraform.	1. Abra una ventana de terminal y confirme que Terraform esté instalado y que AWS las credenciales estén disponibles. 2. Vaya a la carpeta `bootstrap-terraform` .	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	3. Edite el archivo `main.tf` si desea cambiar los nombres del bucket de S3 (`<accountId>-terraform-backend`) y de la tabla de Amazon DynamoDB (`terraform-lock`). 4. Ejecute el comando `terraform apply` para implementar los recursos. Anote los nombres del bucket de S3 y de las tablas de DynamoDB.	

Implementar la infraestructura de soluciones

Tarea	Descripción	Habilidades requeridas
Revise y actualice la configuración de Terraform.	En el directorio raíz, abra el archivo `main.tf,`, revise el contenido y considere la posibilidad de realizar las siguientes actualizaciones: 1. Actualícelo buscando y sustituyendo la cadena Región de AWS `eu-west-1` por la región deseada que desee utilizar. 2. Actualice el nombre del bucket en el bloque `Terraform Backend` si el valor predeterminado	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	se modificó en la épica anterior. 3. Actualice el valor `dynamodb_table` si el valor predeterminado se modificó en la épica anterior. 4. Actualice el valor de la variable `stack_prefix` a la cadena que desee. Esta cadena se antepondrá a los nombres de todos los recursos creados por este patrón. 5. Actualice el valor de `vpc_cidr` . Debe ser al menos un rango de `/24` direcciones. 6. Revise la sección `Locals`. Esto se usa para definir las tareas de Blu Age que van a implementarse. La solución recorrerá el objeto de la lista `bluage_batch_modules` , creando los recursos asociados (máquina de estado de Step Functions, definición de tareas y tema de SNS) para cada elemento de la lista. En algunos casos, es posible que desee ajustar las variables para diferentes entornos. Por ejemplo,	

Tarea	Descripción	Habilidades requeridas
	para forzar el tiempo de ejecución en los entornos de prueba, puede cambiar el valor de la variable `force_execution_time` . 7. Para activar el acceso a Internet, cambie el valor de `direct_internet_access_required` de `false` a `true`. Esto implementará una puerta de enlace de Internet, junto con las puertas de enlace NAT y las tablas de enrutamiento que activan el acceso público a Internet en la infraestructura. De forma predeterminada, la solución implementará los puntos de conexión de VPC de interfaz en una VPC sin acceso directo a Internet. 8. Para conceder acceso a cualquier carga de trabajo cliente-servidor que se sirva a través de Elastic Load Balancing, actualice los valores de `additional_nlb_igress_cidrs` con las redes CIDR que deberían permitirse.	

Tarea	Descripción	Habilidades requeridas
Implemente el archivo Terraform.	Desde su terminal, ejecute el comando `terraform apply` para implementar todos los recursos. Revise los cambios generados por Terraform e introduzca sí para iniciar la compilación. Tenga en cuenta que la implementación de esta infraestructura puede tardar más de 15 minutos.	DevOps ingeniero

(Opcional) Implementar una aplicación de Blu Age en contenedores válida

Tarea	Descripción	Habilidades requeridas
Envíe la imagen del contenedor Blu Age a Amazon ECR.	Introduzca el contenedor en el repositorio de Amazon ECR que creó en la épica anterior. Para obtener instrucciones, consulte la documentación de Amazon ECR. Anote el URI de la imagen del contenedor.	DevOps ingeniero
Actualice Terraform para que haga referencia a la imagen del contenedor de Blu Age.	Actualice el archivo `main.tf` para que haga referencia a la imagen del contenedor que usted subió.	DevOps ingeniero
Volver a implementar el archivo Terraform.	Desde su terminal, ejecute `terraform apply` para implementar todos los	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	recursos. Revise las actualizaciones sugeridas por Terraform y, a continuación, introduzca sí para continuar con la implementación.	

Recursos relacionados

- Blu Age
- Ejecución de cargas de trabajo de mainframe que se han modernizado con Blu Age en una infraestructura sin servidor de AWS
- Almacenamiento en contenedores de las cargas de trabajo de mainframe que Blu Age ha modernizado

Genere información sobre z/OS datos de Db2 mediante AWS Mainframe Modernization Amazon Q en Quick Sight

Shubham Roy, Roshna Razack y Santosh Kumar Singh, Amazon Web Services

Resumen

Nota: AWS Mainframe Modernization El servicio (experiencia de entorno de ejecución gestionado) ya no está abierto a nuevos clientes. Para obtener funciones similares a las AWS Mainframe Modernization de Service (experiencia en entornos de ejecución gestionados), explore AWS Mainframe Modernization Service (experiencia autogestionada). Los clientes existentes pueden seguir utilizando el servicio con normalidad. Para obtener más información, consulte Cambio en la disponibilidad de AWS Mainframe Modernization.

Si su organización aloja datos críticos para la empresa en un entorno de mainframe IBM Db2, obtener información a partir de esos datos es fundamental para impulsar el crecimiento y la innovación. Al desbloquear los datos del mainframe, puede crear inteligencia empresarial más rápida, segura y escalable para acelerar la toma de decisiones, el crecimiento y la innovación basados en los datos en la nube de Amazon Web Services (AWS).

Este patrón presenta una solución para generar información empresarial y crear narrativas compartibles a partir de datos de mainframe en IBM Db2 for tables. z/OS Los cambios en los datos del mainframe se transmiten al tema de Amazon Managed Streaming para Apache Kafka (Amazon MSK) mediante la replicación de datos de AWS Mainframe Modernization con Precisely. Mediante la ingesta de transmisión de Amazon Redshift, los datos de los temas de Amazon MSK se almacenan en tablas de almacenes de datos de Amazon Redshift sin servidor para su análisis en Amazon QuickSight.

Una vez que los datos estén disponibles en QuickSight, puede utilizar las peticiones en lenguaje natural con Amazon Q en QuickSight para crear resúmenes de los datos, formular preguntas y generar historias basadas en datos. No tiene que escribir consultas SQL ni aprender una herramienta de inteligencia empresarial (BI).

Contexto empresarial

Este patrón presenta una solución para casos de uso de análisis de datos e información de datos de mainframe. Con el patrón, puede crear un panel visual para los datos de su empresa. Para demostrar la solución, este patrón utiliza una empresa de atención médica que ofrece planes médicos, dentales

y oftalmológicos a sus miembros en los EE. UU. En este ejemplo, la información demográfica y del plan de los miembros se almacena en las tablas de datos de IBM Db2 for. z/OS El panel visual muestra lo siguiente:

- Distribución de miembros por región
- Distribución de miembros por género
- Distribución de miembros por edad
- Distribución de miembros por tipo de plan
- Miembros que no han completado la inmunización preventiva

Para ver ejemplos de la distribución de los miembros por región y de los miembros que no han completado la inmunización preventiva, consulte la sección de información adicional.

Después de crear el panel, se genera una historia basada en datos que explica la información del análisis anterior. Las historias basadas en datos proporcionan recomendaciones para aumentar el número de miembros que han completado la inmunización preventiva.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS. Esta solución se creó y probó en Amazon Linux 2 en Amazon Elastic Compute Cloud (Amazon EC2).
- Una nube privada virtual (VPC) con una subred a la que puede acceder el sistema de su mainframe.
- Una base de datos de mainframe con datos empresariales. Para ver los datos de ejemplo que se utilizan para crear y probar esta solución, consulte la sección de archivos adjuntos.
- La captura de datos de cambios (CDC) está habilitada en las z/OS tablas de Db2. Para habilitar la CDC en Db2 z/OS, consulte la documentación de IBM.
- Precisamente Connect CDC z/OS se instala en el z/OS sistema que aloja las bases de datos de origen. La z/OS imagen CDC for de Precision Connect se proporciona como un archivo zip dentro de la imagen Amazon Machine Image AWS Mainframe Modernization (AMI) de Data Replication for IBM z/OS. Para instalar Precily Connect CDC for z/OS en el mainframe, consulte la documentación de instalación de Precision.

Limitaciones

- Los datos de Db2 de su mainframe deben estar en un tipo de datos compatible con Precisely Connect CDC. Para obtener una lista de los tipos de datos compatibles, consulte la documentación de Precisely Connect CDC.
- Los datos de Amazon MSK deben estar en un tipo de datos compatible con Amazon Redshift. Para obtener una lista de los tipos de datos compatibles, consulte la documentación de Amazon Redshift.
- Amazon Redshift tiene diferentes comportamientos y límites de tamaño para los distintos tipos de datos. Para obtener más información, consulte la documentación de Amazon Redshift.
- Los datos casi en tiempo real de QuickSight dependen del intervalo de actualización establecido para la base de datos de Amazon Redshift.
- Algunas Servicios de AWS no están disponibles en todas Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region. Amazon Q en QuickSight no está disponible actualmente en todas las regiones que admiten QuickSight. Para ver los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- AWS Mainframe Modernization Replicación de datos con la versión 4.1.44 de Precision
- Python, versión 3.6 o posterior
- Apache Kafka versión 3.5.1

Arquitectura

Arquitectura de destino

El siguiente diagrama muestra una arquitectura para generar información empresarial a partir de datos del mainframe mediante la replicación de datos de AWS Mainframe Modernization con Precisely y Amazon Q en QuickSight.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El agente de lectura de registro de Precisely lee los datos de los registros de Db2 y los escribe en un almacenamiento transitorio de un sistema de archivos OMVS del mainframe.
2. El agente publicador lee los registros de Db2 sin procesar del almacenamiento transitorio.

3. El daemon del controlador en las instalaciones autentica, autoriza, supervisa y administra las operaciones.
4. El Apply Agent se implementa en Amazon EC2 mediante la AMI preconfigurada. Se conecta con el agente publicador a través del daemon del controlador mediante TCP/IP. El agente de aplicación envía los datos a Amazon MSK mediante varios trabajadores para lograr un alto rendimiento.
5. Los trabajadores escriben los datos en el tema de Amazon MSK en formato JSON. Como objetivo intermedio para los mensajes replicados, Amazon MSK ofrece capacidades de conmutación por error automatizadas y de alta disponibilidad.
6. La ingesta de transmisión de Amazon Redshift proporciona una ingesta de datos de alta velocidad y baja latencia de Amazon MSK a una base de datos de Amazon Redshift sin servidor. Un procedimiento almacenado en Amazon Redshift realiza la reconciliación de los datos de cambios (insert/update/deletes) del mainframe en tablas de Amazon Redshift. Estas tablas de Amazon Redshift sirven como origen de análisis de datos para QuickSight.
7. Los usuarios acceden a los datos en QuickSight para obtener análisis e información. Puede usar Amazon Q en QuickSight para interactuar con los datos mediante peticiones en lenguaje natural.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática escalable en el Nube de AWS. Puede iniciar tantos servidores virtuales como necesite y escalarlos o reducirlos horizontalmente con rapidez.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.
- Amazon Managed Streaming para Apache Kafka (Amazon MSK) es un servicio completamente administrado que le permite crear y ejecutar aplicaciones que utilizan Apache Kafka para procesar datos de streaming.
- Amazon QuickSight es un servicio de inteligencia empresarial (BI) a escala de la nube que lo ayuda a visualizar, analizar y generar informes de sus datos en un único panel. Este patrón utiliza las capacidades de BI generativa de Amazon Q en QuickSight.
- Amazon Redshift sin servidor es una opción sin servidor de Amazon Redshift que hace que sea más eficiente ejecutar y escalar los análisis en cuestión de segundos sin necesidad de configurar y administrar la infraestructura del almacén de datos.

- AWS Secrets Manager lo ayuda a reemplazar las credenciales codificadas en su código, incluidas contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.

Otras herramientas

- Precisely Connect CDC recopila e integra datos de sistemas heredados en plataformas de datos y en la nube.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub Mainframe_ DataInsights _change_data_reconciliation. El código es un procedimiento almacenado en Amazon Redshift. Este procedimiento almacenado concilia los cambios en los datos del mainframe (inserciones, actualizaciones y eliminaciones) de Amazon MSK en las tablas de Amazon Redshift. Estas tablas de Amazon Redshift sirven como origen de análisis de datos para QuickSight.

Prácticas recomendadas

- Siga las prácticas recomendadas al configurar su clúster de Amazon MSK.
- Siga las prácticas recomendadas de análisis de datos de Amazon Redshift para mejorar el rendimiento
- Al crear los roles AWS Identity and Access Management (IAM) para la configuración de Precially, siga el principio de privilegios mínimos y conceda los permisos mínimos necesarios para realizar una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Configure la replicación AWS Mainframe Modernization de datos con Precision on Amazon EC2

Tarea	Descripción	Habilidades requeridas
Configure un grupo de seguridad.	Para conectarse al daemon del controlador y al clúster de Amazon MSK, cree un grupo de seguridad para la	DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas

	EC2 instancia. Agregue las siguientes reglas de entrada y salida:
	• Regla de entrada 1:
	  • En Tipo, elija TCP personalizada.
	  • En Protocol, seleccione TCP.
	  • En Rango de puertos, elija 2626 (puerto predeterminado para el daemon del controlador de Precisely) o el número de puerto del daemon del controlador que se ejecuta en el mainframe.
	  • En Origen, elija el bloque de CIDR.
	• Regla de entrada 2:
	  • En Type (Tipo), elija Custom TCP (TCP personalizada).
	  • En Protocolo, elija SMH.
	  • En Rango de puertos, elija 22.
	  • En Origen, elija la dirección IP o la lista de prefijos.
	• Regla de entrada 3:
	  • En Type (Tipo), elija Custom TCP (TCP personalizada).	

Tarea	Descripción	Habilidades requeridas
	• En Protocol, seleccione TCP. • En Rango de puertos, elija 9092-9098. • En Origen, elija Bloque de CIDR. • Regla de salida 1: • En Type (Tipo), elija Custom TCP (TCP personalizada). • En Protocol, seleccione TCP. • En Rango de puertos, elija 9092-9098. • En Origen, elija Bloque de CIDR. • Regla de salida 2: • En Type (Tipo), elija Custom TCP (TCP personalizada). • En Protocol, seleccione TCP. • En Rango de puertos, elija 2626 (puerto predeterminado para el daemon del controlador de Precisely) o el número de puerto del daemon del controlador que se ejecuta en el mainframe. • En Origen, elija Bloque de CIDR.	

Tarea	Descripción	Habilidades requeridas
	Anote el nombre del grupo de seguridad. Deberá hacer referencia al nombre cuando lance la EC2 instancia y configure el clúster de Amazon MSK.	
Cree una política de IAM y un rol de IAM.	1. Para crear una política de IAM y un rol de IAM, siga las instrucciones de la documentación de AWS. Cree una política de IAM que conceda acceso para crear temas en el clúster de Amazon MSK y enviar datos a esos temas. 2. Después de crear el rol de IAM, asocie la política a él. Anote el nombre del rol de IAM. Esta función se utilizará como perfil de la instancia de IAM al lanzar la EC2 instancia.	DevOps ingeniero, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
Aprovisione una EC2 instancia .	Para aprovisionar una EC2 instancia para ejecutar Precily CDC y conectarse a Amazon MSK, haga lo siguiente: 1. Inicie sesión y suscríbase a AWS Mainframe Modernization – Data Replication for IBM z/OS. AWS Marketplace 2. Seleccione la AMI de las suscripciones administradas y elija Iniciar nueva instancia. 3. Proporcione otros detalles de configuración, como el nombre de la instancia, el tipo de instancia, el par de claves, la VPC y las subredes. Para obtener más información, consulta la EC2 documentación de Amazon. 4. En la lista desplegable, elija el grupo de seguridad que creó anteriormente. 5. En Detalles avanzados, Perfil de instancia de IAM, debe seleccionar el rol que creó anteriormente. 6. Seleccione Iniciar instancia.	Administrador DevOps e ingeniero de AWS

Configuración de Amazon MSK

Tarea	Descripción	Habilidades requeridas
Cree el clúster de Amazon MSK.	Para crear un clúster de Amazon MSK, haga lo siguiente: 1. Inicia sesión en Amazon MSK y navega hasta Amazon MSK. Consola de administración de AWS 2. Elija Create cluster. 3. Para el método de creación del clúster, elija Creación personalizada y, para el tipo de clúster, elija Aprovisio nado. 4. Especifique un nombre para el clúster. 5. Actualice la configura ción del clúster según sea necesario y mantenga los valores predeterminados para el resto de la configura ción. 6. Anote la <versión de Kafka>. La necesitará durante la configuración del cliente de Kafka. 7. Elija Siguiente. 8. Elija la misma VPC y las mismas subredes que utilizó para la EC2 instancia de Precily y elija el grupo	AWS DevOps, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	de seguridad que creó anteriormente. 9. En la sección Configuración de seguridad, habilite la autenticación basada en roles de IAM y SASL/SCRAM. Precisamente Connect CDC utiliza SASL/SCRAM (capa de autenticación y seguridad simple o mecanismo de respuesta a desafíos salados) y se necesita IAM para conectarse a Amazon Redshift. 10. Elija Siguiente. 11. Para revisarlos, elija Supervisión y Método de entrega de registros del agente. 12. Seleccione Siguiente y, después, Crear el clúster. Un clúster aprovisionado típico tarda hasta 15 minutos en crearse. Una vez creado el clúster, su estado cambia de Creando a Activo.	

Tarea	Descripción	Habilidades requeridas
Configure la SASL/SCRAM autenticación.	Para configurar la SASL/SCRAM autenticación de un clúster de Amazon MSK, haga lo siguiente: 1. Para configurar un secreto en Secrets Manager, siga las instrucciones de la documentación de AWS. 2. Abra la consola de Amazon MSK y seleccione el clúster de Amazon MSK que creó anteriormente. 3. Elija la pestaña Propiedad es. 4. Elija Asociar secretos, elija los secretos, seleccione la clave de secretos que creó y, a continuación, elija Asociar secretos. Verá un mensaje similar al siguiente que indica que la operación se ha realizado correctamente: `Successfully associated 1 secret for cluster <chosen cluster name>` 5. Elija el nombre del clúster. 6. En el resumen del clúster, elija Ver información del cliente.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	7. Anote la cadena de conexión del punto de conexión privado para el tipo de autenticación SASL/SCRAM.	

Tarea	Descripción	Habilidades requeridas

Cree el tema de Amazon MSK.	Para crear el tema de Amazon MSK, haga lo siguiente:
	1. Conéctese a la EC2 instancia que creó anteriormente e instale las actualizaciones más recientes ejecutando el siguiente comando:
	`sudo yum update -y`
	2. Para instalar la biblioteca de Kafka y Java, ejecute el siguiente comando:
	`sudo yum install -y java-11 librdkafka librdkafka-devel`
	3. Para crear una carpeta con el nombre `kafka` en `/home/ec2-user` , navegue hasta esa carpeta y ejecute el comando siguiente:
	`mkdir kafka;cd kafka`
	4. Descargue la biblioteca del cliente de `kafka` en la carpeta `kafka` y sustituya `<YOUR MSK VERSION>` por la versión de Kafka que indicó durante la creación del clúster de Amazon MSK:
		Administrador de la nube

Tarea	Descripción	Habilidades requeridas

	`wget https://archive.apache.org/dist/kafka//kafka_2.13-<YOUR MSK VERSION>.tgz`
	5. Para extraer el archivo descargado, ejecute el comando siguiente y sustituya `YOUR MSK VERSION>`:
	`tar -xzf kafka_2.13-<YOUR MSK VERSION>.tgz`
	6. Para ir al directorio `kafka libs` y descargar el archivo Java Archive (JAR) de autenticación de IAM de Java, ejecute los siguientes comandos y sustituya `<YOUR MSK VERSION>`:
	`cd kafka_2.13-<YOUR MSK VERSION>/libs`
	`wget https://github.com/aws/aws-msk-iam-auth/releases/download/v1.1.1/aws-msk-iam-auth-1.1.1-all.jarkafka`
	7. Para ir al directorio `bin` de Kafka y crear el archivo `client.properties` ,	

Tarea	Descripción	Habilidades requeridas

	ejecute los siguientes comandos:
	`cd /home/ec2-user/kafka/kafka_2.13-<YOUR MSK VERSION>/bin`
	`cat >client.properties`
	8. Actualice el archivo `client.properties` con el siguiente contenido:
	`security.protocol=SASL_SSL`
	`sasl.mechanism=AWS_MSK_IAM`
	`sasl.jaas.config=software.amazon.msk.auth.iam.IAMLoginModule required;`
	`sasl.client.callback.handler.class=software.amazon.msk.auth.iam.IAMClientCallbackHandler`
	9. Para crear un tema de Kafka, vaya a la papelera de Kafka y ejecute el siguiente comando y, a continuación, sustituya `<kafka broker>` por el punto de conexión privado del servidor de arranque de IAM que indicó durante la creación del clúster de Amazon MSK:	

Tarea	Descripción	Habilidades requeridas
	`./kafka-topics.sh --bootstrap-server <kafka broker> --command-config client.properties --create --replication-factor 3 –partitions 6 --topic <topic name>` 10. Cuando aparezca el mensaje `Created topic <topic name>`, anote el nombre del tema.	

Configura el motor de aplicación precisa en Amazon EC2

Tarea	Descripción	Habilidades requeridas
Configure los scripts de Precisely para replicar los cambios en los datos.	Para configurar los scripts de Precisely Connect CDC para replicar los datos modificados del mainframe al tema de Amazon MSK, haga lo siguiente: 1. Para crear una carpeta llamada precisely, navegue hasta esa carpeta y ejecute el comando siguiente: `mkdir /home/ec2-user/precisely;cd /home/ec2-user/precisely`	Desarrollador de aplicaciones, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas

	2. Para crear dos carpetas dentro de precisely llamadas `scripts` y `ddls`, y a continuación, cambiarlas a la carpeta `scripts`, ejecute el siguiente comando:
	`mkdir scripts;mkdir ddls;cd scripts`
	3. Para crear un archivo `sqdata_kafka_producer.conf` en la carpeta `scripts`, ejecute el siguiente comando:
	`cat >sqdata_kafka_producer.conf`
	4. Actualice el archivo `sqdata_kafka_producer.conf` con el siguiente contenido:
	`builtin.features=SASL_SCRAM`
	`security.protocol=SASL_SSL`
	`sasl.mechanism=SCRAM-SHA-512`
	`sasl.username=<User Name>`
	`sasl.password=<Password>`
	`metadata.broker.list=<SASL/SCRAM Bootstrap servers>`	

Tarea	Descripción	Habilidades requeridas
	Note Actualice `<SASL/SCRAM Bootstrap servers>` con la lista de SASL/SCRAM corredores de Amazon MSK que configuró previamente. Actualice `<User Name>` y `<Password>` con el nombre de usuario y la contraseña que configuró anteriormente en Secrets Manager. 5. Cree un archivo `script.sqd` en la carpeta `scripts`. `cat >script.sqd` El motor de aplicación usa `script.sqd` para procesar los datos de origen y replicarlos en el destino. Para un ejemplo de script del motor de aplicació	

Tarea	Descripción	Habilidades requeridas

	n, consulte la sección Información adicional.
	6. Para cambiar a la carpeta `ddls` y crear un archivo .ddl para cada tabla de Db2, ejecute los siguientes comandos:
	`cd /home/ec2-user/precisely/ddls`
	`cat >mem_details.ddl`
	`cat >mem_plans.ddl`
	Para archivos .ddl de ejemplo, consulte la sección Información adicional.	

Tarea	Descripción	Habilidades requeridas

Genere la clave ACL de red.	Para generar la clave de lista de control de acceso de la red (ACL de la red), haga lo siguiente:
	
	1. Para exportar la ruta de instalación de `sqdata`, ejecute el siguiente comando:
	
	`export PATH=$PATH:/usr/sbin:/opt/precisely/di/sqdata/bin`
	
	2. Para cambiar al directorio `/home/ec2-user` y generar la clave de ACL de la red, ejecute los siguientes comandos:
	
	`cd /home/ec2-user`
	`sqdutil keygen --force`
	
	Una vez generadas las claves pública y privada, aparece el siguiente mensaje:
	
	`SQDUT04I Generating a private key in file /home/ec2-user/.nacl/id_nacl`
	`SQDC017I sqdutil(pid=27344) terminated successfully`
		Arquitecto de nube, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	3. Anote la clave pública generada que se guarda en la carpeta `.nacl`.	

Preparación del entorno de origen del mainframe

Tarea	Descripción	Habilidades requeridas
Configure los valores predeterminados en la pantalla del ISPF.	Para configurar los ajustes predeterminados en el Interactive System Productivity Facility (ISPF), siga las instrucciones de la documentación de Precisely.	Administrador del sistema de mainframe
Configure el daemon del controlador.	Para configurar el daemon del controlador, haga lo siguiente: 1. En la pantalla del menú principal de SQData z/OS, elija la opción 2. 2. En la pantalla Añadir un daemon a la lista, en el campo Nombre del daemon, introduzca un nombre para el daemon y, a continuación, pulse Intro.	Administrador del sistema de mainframe
Configure el publicador.	Para configurar el publicador, haga lo siguiente: 1. En la pantalla del menú principal de SQData z/OS, elija la opción 3. Esto le llevará a la pantalla de	Administrador del sistema de mainframe

Tarea	Descripción	Habilidades requeridas
	resumen de la captura o del publicador. 2. Seleccione la opción para añadir un archivo CAB. Esto le llevará a la pantalla Añadir un archivo CAB a la lista. 3. En el campo Nombre, escriba el nombre del archivo CAB. Para Db2, introduzca el tipo como `D`. 4. Pulse Intro. Esto le llevará a la pantalla Crear un nuevo archivo CAB de captura de Db2. 5. En el campo zFS Dir, especifique el punto de montaje del almacenam iento. 6. Pulse intro para guardar y continuar.	

Tarea	Descripción	Habilidades requeridas
Actualice el archivo de configuración del daemon.	Para actualizar los detalles del publicador en el archivo de configuración del daemon del controlador, haga lo siguiente: 1. En la pantalla del menú principal de SQData z/OS, elija la opción 2. 2. Introduzca S cerca del daemon que ha creado para ver los detalles del daemon. 3. Introduzca 1 y, a continuación, pulse Intro para editar el archivo de los agentes. 4. Añada los detalles de su archivo CAB. El siguiente ejemplo muestra los detalles de un archivo CAB denominado `DB2ZTOMSK`. Utilice su ID de usuario de mainframe en lugar de `<userid>`. `ÝDB2ZTOMSK¨ type=capture cab=/u/<userid>/sqdata/DB2ZTOMSK.cab` 5. Pulse F3. 6. Introduzca 2 para editar el archivo ACL. Agregue `userid` al archivo de configuración `acl` como	Administrador del sistema de mainframe

Tarea	Descripción	Habilidades requeridas
	se muestra en el siguiente ejemplo: `Ýacls¨ prod=admin,<userid>` 7. Pulse F3 para guardar y salir.	
Cree el trabajo para iniciar el daemon del controlador.	Para crear el trabajo, haga lo siguiente: 1. En Opciones, introduzca `G`. 2. Introduzca la tarjeta de trabajo, las bibliotecas de trabajos y procesos y los detalles de la biblioteca de `Db2 load`. 3. Introduzca los detalles del archivo ACL de la red e introduzca la opción 2 para generar el archivo de lenguaje de control de tareas (JCL) en la biblioteca de trabajos especificada.	Administrador del sistema de mainframe

Tarea	Descripción	Habilidades requeridas
Genere el archivo JCL del publicador de capturas.	Para generar el archivo JCL del publicador de capturas, haga lo siguiente: 1. En la pantalla del menú principal de SQData z/OS, elija la opción 3. Esto le llevará a la pantalla de resumen de la captura o del publicador. 2. Introduzca `S` junto al archivo CAB para seleccionarlo. Esto le llevará a la pantalla de detalles de Db2 Capture/Publisher . 3. En Opciones, introduzca `G` en las opciones para generar el trabajo `capture/publisher` . 4. Introduzca la tarjeta de trabajo, las bibliotecas de procedimiento y los detalles de la biblioteca de carga de Db2. 5. Para crear el trabajo, elija la opción 4. El trabajo se crea en la biblioteca de trabajos especificada en la biblioteca de trabajos.	Administrador del sistema de mainframe

Tarea	Descripción	Habilidades requeridas

Compruebe y actualice las CDC.	1. Para comprobar el indicador DATACAPTURE de la tabla de Db2, ejecute la siguiente consulta y cambie <table name> por el nombre de la tabla de Db2:
	`SELECT DATACAPTU RE FROM SYSIBM.SY STABLES WHERE NAME='<table name>';`
	Confirme que el resultado muestre DATACAPTURE como Y.
	2. Si DATACAPTURE no es Y, ejecute la siguiente consulta para habilitar la CDC en la tabla de Db2, cambiando <table name> por el nombre de la tabla de Db2:
	`ALTER TABLE <table name> DATA CAPTURE CHANGES;`
		Administrador del sistema de mainframe

Tarea	Descripción	Habilidades requeridas
Envíe los archivos JCL.	Envíe los siguientes archivos JCL que ha configurado en los pasos anteriores: • Archivo JCL para iniciar el daemon del controlador • Archivo JCL para iniciar la captura y publicación Tras enviar los archivos JCL, puede iniciar el motor de aplicación en Precily en la EC2 instancia.	Administrador del sistema de mainframe

Ejecución y validación de las CDC

Tarea	Descripción	Habilidades requeridas
Inicie el motor de aplicación y valide la CDC.	Para iniciar el motor de aplicación en la EC2 instancia y validar el CDC, haga lo siguiente: 1. Para conectarse a la EC2 instancia, siga las instrucciones de la AWS documentación. 2. Cambie al directorio que contiene el archivo `script.sqd` : `cd /home/ec2-user/precisely/scripts`	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	3. Para iniciar el motor de aplicación, ejecute el siguiente comando `sqdeng` de inicio: `sqdeng -s script.sqd --identity=/home/ec2-user/.nacl/id_nacl` El motor de aplicación empezará a esperar las actualizaciones del origen del mainframe. 4. Para probar la CDC, inserte o actualice algunos registros en la tabla de Db2. 5. Compruebe que el registro del motor de aplicación muestre el número de registros capturados y escritos en el destino.	

Tarea	Descripción	Habilidades requeridas

Valide los registros del tema de Amazon MSK.	Para leer el mensaje del tema de Kafka, haga lo siguiente:
	1. Para cambiar al `bin` directorio de la ruta de instalación del cliente Kafka de la EC2 instancia, ejecuta el siguiente comando y `<Kafka version>` sustitúyelo por tu versión:
	`cd /home/ec2-user/kafka/kafka_2.13-<Kafka version>/bin`
	2. Para validar las CDC de Db2 escritas como mensajes en el tema de Kafka, ejecute el siguiente comando y sustituya `<kafka broker>` y `<Topic Name>` por el tema que creó anteriormente:
	`./kafka-console-consumer.sh --bootstrap-server <kafka broker>:9098 --topic <Topic Name> --from-beginning --consumer.config client.properties`
	3. Valide que los mensajes coincidan con el número de
		Desarrollador de aplicaciones, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	registros actualizados en la tabla de Db2.	

Almacene los datos de cambios del mainframe en un almacén de datos de Amazon Redshift sin servidor

Tarea	Descripción	Habilidades requeridas
Configure Amazon Redshift sin servidor.	Para crear un almacén de datos de Amazon Redshift sin servidor, siga las instrucciones de la documentación de AWS En el panel de Amazon Redshift sin servidor, compruebe que el espacio de nombres y el grupo de trabajo se crearon y están disponibles. Para este patrón de ejemplo, el proceso puede tardar entre 2 y 5 minutos.	Ingeniero de datos
Configure el rol de IAM y la política de confianza necesarios para la ingesta de transmisión.	Para configurar la ingesta de transmisión de Amazon Redshift sin servidor desde Amazon MSK, haga lo siguiente: 1. Cree una política de IAM para que Amazon Redshift pueda acceder a Amazon MSK. Si lo `[region]` sustituye Región de AWS por el de Amazon MSK, `[account-`	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	id] por su Cuenta de AWS ID y [msk-cluster-name] por el nombre del clúster de Amazon MSK, ejecute el siguiente código: `{"Version": "2012-10-17", "Statement": [{"Sid": "MSKIAMpolicy","Effect": "Allow","Action": ["kafka-cluster:ReadData","kafka-cluster:DescribeTopic","kafka-cluster:Connect"],"Resource": ["arn:aws:kafka:[region]:[account-id]:cluster/[msk-cluster-name]/*","arn:aws:kafka:[region]:[account-id]:topic/[msk-cluster-name]/*"]},{"Effect": "Allow","Action": ["kafka-cluster:AlterGroup","kafka-cluster:DescribeGroup"],"Resource": ["arn:aws:kafka:[region]:[account-id`	

Tarea	Descripción	Habilidades requeridas
	`]:group/[msk-cluster-name]/*"]}]}` Puede buscar el nombre del clúster y el nombre de recurso de Amazon (ARN) en la consola de Amazon MSK. En la consola, elija Resumen del clúster y, a continuación, ARN. 2. Para crear un rol de IAM y adjuntar la política, siga las instrucciones de la documentación de AWS. 3. Para adjuntar el rol de IAM al espacio de nombres de Amazon Redshift sin servidor, haga lo siguiente: a. Inicie sesión en la consola y abra la consola de Amazon Redshift en. https://console.aws.amazon.com/redshiftv2/ b. Elija Serverless dashboard (Panel Sin servidor). c. Elija Espacio de nombres. d. Elija la pestaña Seguridad y cifrado. e. Elija Permiso y adjunte el rol de IAM que creó.	

Tarea	Descripción	Habilidades requeridas
	4. En su grupo de seguridad Amazon Redshift sin servidor, cree una regla de entrada con los siguientes detalles: • En Type (Tipo), elija Custom TCP (TCP personalizada). • En Protocol, seleccione TCP. • En Rango de puertos, elija 9098, 9198. • En Origen, elija el grupo de seguridad de Amazon MSK. 5. En su grupo de seguridad de Amazon MSK, cree una regla de entrada con los siguientes detalles: • En Type (Tipo), elija Custom TCP (TCP personalizada). • En Protocol, seleccione TCP. • En Rango de puertos, elija 9098, 9198. • En Origen, elija el grupo de seguridad de Amazon Redshift. Este patrón usa el puerto de autenticación de IAM para la configuración de	

Tarea	Descripción	Habilidades requeridas
	Amazon Redshift y Amazon MSK. Para obtener más información, consulte la documentación de AWS (paso 2). 6. Active el enrutamiento de VPC mejorado para el grupo de trabajo de Amazon Redshift sin servidor Para obtener más información, consulte la Documentación de AWS.	
Conecte Amazon Redshift sin servidor a Amazon MSK.	Para conectarse al tema de Amazon MSK, cree un esquema externo en Amazon Redshift sin servidor. En el editor de consultas V2 de Amazon Redshift, ejecute el siguiente comando SQL y, a continuación, sustituya `'iam_role_arn'` por el rol que creó anteriormente y `'MSK_cluster_arn` por el ARN de su clúster. `CREATE EXTERNAL SCHEMA member_schema FROM MSK IAM_ROLE 'iam_role _arn' AUTHENTICATION iam URI 'MSK_cluster_arn';`	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Cree una vista materializada.	Para consumir los datos del tema de Amazon MSK en Amazon Redshift sin servidor, cree una vista materializada. En el editor de consultas V2 de Amazon Redshift, ejecute los siguientes comandos de SQL y sustituya `<MSK_Topic_name>` por el nombre del tema de Amazon MSK. `CREATE MATERIALIZED VIEW member_view AUTO REFRESH YES AS SELECT kafka_partition, kafka_offset, refresh_time, json_parse(kafka_value) AS Data FROM member_schema.<MSK_Topic_name> WHERE CAN_JSON_PARSE(kafka_value);`	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas

Cree tablas de destino en Amazon Redshift.	Las tablas de Amazon Redshift proporcionan la entrada para QuickSight. Este patrón utiliza las tablas `member_dtls` y `member_plans`, que coinciden con las tablas de Db2 de origen del mainframe.
	
	Para crear las dos tablas en Amazon Redshift, ejecute los siguientes comandos de SQL en el editor de consultas V2 de Amazon Redshift:
	
	`-- Table 1: members_dtls`
	`CREATE TABLE members_dtls (`
	`memberid INT ENCODE AZ64,`
	`member_name VARCHAR(100) ENCODE ZSTD,`
	`member_type VARCHAR(50) ENCODE ZSTD,`
	`age INT ENCODE AZ64,`
	`gender CHAR(1) ENCODE BYTEDICT,`
	`email VARCHAR(100) ENCODE ZSTD,`
	`region VARCHAR(50) ENCODE ZSTD`
	`) DISTSTYLE AUTO;`
	
	`-- Table 2: member_plans`
	`CREATE TABLE member_plans (`
		Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas

	<pre>memberid INT ENCODE
	AZ64,
	medical_plan CHAR(1)
	ENCODE BYTEDICT,
	dental_plan CHAR(1)
	ENCODE BYTEDICT,
	vision_plan CHAR(1)
	ENCODE BYTEDICT,
	preventive_immuniz
	ation VARCHAR(50)
	ENCODE ZSTD
	) DISTSTYLE AUTO;</pre>	

Cree un procedimiento almacenado en Amazon Redshift.	Este patrón utiliza un procedimiento almacenado para sincronizar los datos de cambios (`INSERT`, `UPDATE`, `DELETE`) del mainframe de origen con la tabla de almacén de datos de Amazon Redshift de destino para su análisis en QuickSight. Para crear el procedimiento almacenado en Amazon Redshift, utilice el editor de consultas v2 para ejecutar el código del procedimiento almacenado que se encuentra en el GitHub repositorio.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Lea la vista materializada de la transmisión y cárguela en las tablas de destino.	El procedimiento almacenado lee los cambios de datos de la vista materializada de transmisión y carga los cambios de datos en las tablas de destino. Para ejecutar el procedimiento almacenado, use el siguiente comando: `call SP_Members_Load();` Puede utilizar Amazon EventBridge para programar los trabajos en su almacén de datos de Amazon Redshift para llamar a este procedimiento almacenado en función de sus requisitos de latencia de datos. EventBridge ejecuta los trabajos a intervalos fijos. Para comprobar si la llamada anterior al procedimiento se ha completado, puede que necesite utilizar un mecanismo como una máquina de estado de AWS Step Functions. Para obtener más información, consulte los siguientes recursos: • Crear una EventBridge regla de Amazon que se ejecute según un cronograma	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	• Acelere la organización de un proceso de ELT mediante la AWS Step Functions API de datos de Amazon Redshift. Otra opción es utilizar el editor de consultas V2 de Amazon Redshift para programar la actualización. Para obtener más información, consulte Consultas programadas con el editor de consultas v2.	

Conexión de QuickSight a los datos en Amazon Redshift

Tarea	Descripción	Habilidades requeridas
Configure QuickSight.	Para configurar QuickSight, siga las instrucciones de la documentación de AWS.	Ingeniero de migraciones
Configure una conexión segura entre QuickSight y Amazon Redshift.	Para configurar una conexión segura entre QuickSight y Amazon Redshift, haga lo siguiente: 1. Para autorizar las conexiones de QuickSigh t a Amazon Redshift, abra la consola de Amazon Redshift y añada una regla de entrada al grupo de seguridad de Amazon Redshift. La	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	regla debe permitir el tráfico al puerto 5439 (el puerto predeterminado de Redshift) desde el rango de CIDR en el que configuró QuickSight. Para ver una lista de las direcciones IP Regiones de AWS y sus direcciones IP, consulte Compatible con Quick Regiones de AWS Sight. En la consola de Amazon Redshift, elija Grupo de trabajo, Acceso a datos, Red y seguridad y habilite el Acceso público.	

Tarea	Descripción	Habilidades requeridas
Cree un conjunto de datos para QuickSight.	Para crear un conjunto de datos para QuickSight desde Amazon Redshift, haga lo siguiente: 1. En la consola de QuickSigh t, en el panel de navegació n, elija Conjuntos de datos. 2. En la página Conjuntos de datos, seleccione Nuevo conjunto de datos. 3. Elija Conexión manual de Redshift. 4. En la ventana Nuevo origen de datos de Redshift, introduzca la información de conexión: • En Nombre de origen de datos, escriba un nombre para el origen de datos de Amazon Redshift. • En Servidor de base de datos, introduzca el punto de conexión del clúster de Amazon Redshift. Puede obtener el valor del punto de conexión en el campo Punto de conexión de la sección Informaci ón general del grupo de trabajo del clúster en el panel de Amazon Redshift sin servidor. La	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	dirección del servidor es la primera parte del punto de conexión antes de los dos puntos, tal y como se muestra en el ejemplo siguiente: `mfdata-insights.NNNNNNNN.us-east-1.redshift-serverless.amazonaws.com:5439/dev` • Para el puerto, introduzca `5439` (el puerto predeterminado para Amazon Redshift). • Introduzca el nombre de la base de datos (después de la barra del punto de conexión). En este caso, el nombre de la base de datos es `dev`. • En Nombre de usuario y Contraseña, introduzca el nombre de usuario y la contraseña de la base de datos de Amazon Redshift. 5. Elija Validar conexión. Si se ejecuta correctamente, debería ver una marca de verificación verde que indica la validación. Si la validación falla, consulta	

Tarea	Descripción	Habilidades requeridas
	la sección Solución de problemas. 6. Elija Crear origen de datos.	
Una el conjunto de datos.	Para crear análisis en QuickSight, combine las dos tablas; para ello, siga las instrucciones de la documentación de AWS. En el panel Configuración de unión, elija Izquierda en Tipo de unión. En Cláusulas de unión, utilice `memberid from member_plans = memberid from members_details` .	Ingeniero de migraciones

Obtenga información empresarial a partir de los datos del mainframe mediante Amazon Q en QuickSight

Tarea	Descripción	Habilidades requeridas
Configure Amazon Q en QuickSight.	Para configurar la capacidad de BI generativa de Amazon Q in QuickSight, siga las instrucciones de la documentación de AWS.	Ingeniero de migraciones
Analice los datos del mainframe y cree un panel visual.	Para analizar y visualizar sus datos en QuickSight, haga lo siguiente: 1. Para crear el análisis de datos del mainframe, siga	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	las instrucciones de la documentación de AWS. En el conjunto de datos, elija el conjunto de datos que ha creado. 2. En la página de análisis, elija Crear elemento visual. 3. En la ventana Crear tema para el análisis, elija Actualizar tema existente. 4. En la lista desplegable Seleccione un tema, elija el tema que creó anteriorm ente. 5. Seleccione Vinculación de temas. 6. Después de vincular el tema, elija Crear elemento visual para abrir la ventana Crear un elemento visual de Amazon Q. 7. En la barra de peticiones, escriba sus preguntas de análisis. Los ejemplos de preguntas que se utilizan para este patrón son los siguientes: • Mostrar la distribución de miembros por región • Mostrar la distribución de miembros por edad • Mostrar la distribución de miembros por género	

Tarea	Descripción	Habilidades requeridas
	• Mostrar la distribución de miembros por tipo de plan • Mostrar los miembros que no han completado la inmunización preventiva Después de introducir las preguntas, elija Crear. Amazon Q en QuickSigh t crea los elementos visuales. 8. Para añadir los elementos visuales a su panel visual, elija AÑADIR AL ANÁLISIS. Cuando termine, puede publicar el panel de control para compartirlo con otras personas de su organización. Para ver ejemplos, consulte el panel visual del mainframe en la sección de información adicional.	

Cree una historia basada en datos con Amazon Q en QuickSight a partir de datos del mainframe.

Tarea	Descripción	Habilidades requeridas
Cree una historia basada en datos.	Cree una historia basada en datos para explicar la información del análisis anterior y genere una recomendación para aumentar	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	la inmunización preventiva de los miembros: 1. Para crear la historia basada en datos, siga las instrucciones de la documentación de AWS. 2. Para la petición de la historia basada en datos, utilice lo siguiente: `Build a data story about Region with most numbers of members. Also show the member distribution by medical plan, vision plan, dental plan. Recommend how to motivate members to complete immunizat ion. Include 4 points of supportin g data for this pattern.` También puede crear su propia petición para generar historias basadas en datos que le sirvan para obtener información empresarial adicional. 3. Elija Añadir elementos visuales y añada los	

Tarea	Descripción	Habilidades requeridas
	elementos visuales que sean relevantes para la historia basada en datos. Para este patrón, utilice los elementos visuales que creó anteriormente. 4. Elija Compilar. 5. Para ver un ejemplo de salida de una historia basada en datos, consulte Salida de una historia basada en datos en la sección de información adicional.	
Vea la historia basada en datos generada.	Para ver la historia basada en datos generada, selección ela en la página de Historias basadas en datos.	Ingeniero de migraciones
Edite una historia basada en datos generada.	Para cambiar el formato, el diseño o los elementos visuales de una historia basada en datos, siga las instrucciones de la documentación de AWS.	Ingeniero de migraciones
Comparta una historia basada en datos.	Para compartir una historia basada en datos, siga las instrucciones de la documentación de AWS.	Ingeniero de migraciones

Resolución de problemas

Problema	Solución
Se ha producido el error `Validate Connection` al crear un conjunto de datos de QuickSight a Amazon Redshift.	1. Confirme que el grupo de seguridad adjunto a la instancia de Amazon Redshift sin servidor permite el tráfico entrante desde el rango de direcciones IP asociado a la región en la que configuró QuickSight. 2. Confirme que la VPC en la que se ha implementado Amazon Redshift sin servidor esté disponible públicamente. 3. Confirme que utiliza el nombre de usuario y la contraseña correctos para Amazon Redshift. Puede restablecer el nombre de usuario y la contraseña en la consola de Amazon Redshift.
Al intentar iniciar el motor de aplicación en la EC2 instancia, aparece el siguiente error: `-bash: sqdeng: command not found`	Para exportar la ruta de instalación de `sqdata`, ejecute el siguiente comando: `export PATH=$PATH:/usr/sbin:/opt/precisely/di/sqdata/bin`
Al intentar iniciar el motor de aplicación, se produce uno de los siguientes errores de conexión: • `SQDD018E Cannot connect to transfer socket(rc==0x18468). Agent:<Agent Name > Socket:/u /./sqdata/.DB2ZTOMSK.cab.data` • `SQDUR06E Error opening url cdc:// <VPC end point name>:2626/ DB2ZTOMSK/DB2ZTOMSK : errno:112 8 (Unknown error 1128)`	Compruebe el spool del mainframe para asegurarse de que los trabajos del daemon del controlador se estén ejecutando.

Recursos relacionados

- Genere información mediante AWS Mainframe Modernization Amazon Q en Quick Sight (patrón)
- Genere información de datos con AWS Mainframe Modernization Amazon Q en Quick Sight (demostración)
- AWS Mainframe Modernization - Replicación de datos para IBM z/OS
- Ingesta de transmisión de Amazon Redshift a una vista materializada

Información adicional

Ejemplo: archivos .ddl

members_details.ddl

```
CREATE TABLE MEMBER_DTLS (
memberid INTEGER NOT NULL,
member_name VARCHAR(50),
member_type VARCHAR(20),
age INTEGER,
gender CHAR(1),
email VARCHAR(100),
region VARCHAR(20)
);
```

member_plans.ddl

```
CREATE TABLE MEMBER_PLANS (
memberid INTEGER NOT NULL,
medical_plan CHAR(1),
dental_plan CHAR(1),
vision_plan CHAR(1),
preventive_immunization VARCHAR(20)
);
```

Ejemplo de archivo .sqd

Sustituya <kafka topic name> por el nombre de su tema de Amazon MSK.

script.sqd

```
-- Name: DB2ZTOMSK: DB2z To MSK JOBNAME DB2ZTOMSK;REPORT EVERY 1;OPTIONS
 CDCOP('I','U','D');-- Source Descriptions
JOBNAME DB2ZTOMSK;
REPORT EVERY 1;
OPTIONS CDCOP('I','U','D');

-- Source Descriptions
BEGIN GROUP DB2_SOURCE;
DESCRIPTION DB2SQL /var/precisely/di/sqdata/apply/DB2ZTOMSK/ddl/mem_details.ddl AS
 MEMBER_DTLS;
DESCRIPTION DB2SQL /var/precisely/di/sqdata/apply/DB2ZTOMSK/ddl/mem_plans.ddl AS
 MEMBER_PLANS;
END GROUP;
-- Source Datastore
DATASTORE cdc://<zos_host_name>/DB2ZTOMSK/DB2ZTOMSK
OF UTSCDC
AS CDCIN
DESCRIBED BY GROUP DB2_SOURCE ;
-- Target Datastore(s)
DATASTORE 'kafka:///<kafka topic name>/key'
OF JSON
AS TARGET
DESCRIBED BY GROUP DB2_SOURCE;
PROCESS INTO TARGET
SELECT
{
REPLICATE(TARGET)
}
FROM CDCIN;
```

Panel visual de mainframe

Amazon Q creó el siguiente elemento visual de datos en QuickSight para la pregunta de análisis `show member distribution by region`.

Amazon Q creó el siguiente elemento visual de datos en QuickSight para la pregunta `show member distribution by Region who have not completed preventive immunization, in pie chart`.

Salida de una historia basada en datos

Las siguientes capturas de pantalla muestran secciones de la historia basada en datos creada por Amazon Q en QuickSight para la petición `Build a data story about Region with most numbers of members. Also show the member distribution by age, member distribution by gender. Recommend how to motivate members to complete immunization. Include 4 points of supporting data for this pattern`.

En la introducción, la historia basada en datos recomienda elegir la región con más miembros para obtener el mayor impacto de las iniciativas de inmunización.

La historia basada en datos proporciona un análisis del número de miembros de las cuatro regiones. Las regiones noreste, sudoeste y sureste son las que tienen más miembros.

La historia basada en datos presenta un análisis de los miembros por edad.

La historia basada en datos se centra en las iniciativas de inmunización en el medio oeste.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Genere información de datos mediante AWS Mainframe Modernization Amazon Q en Quick Sight

Shubham Roy, Roshna Razack y Santosh Kumar Singh, Amazon Web Services

Resumen

Nota: AWS Mainframe Modernization El servicio (experiencia de entorno de ejecución gestionado) ya no está abierto a nuevos clientes. Para obtener funciones similares a las AWS Mainframe Modernization de Service (experiencia en entornos de ejecución gestionados), explore AWS Mainframe Modernization Service (experiencia autogestionada). Los clientes existentes pueden seguir utilizando el servicio con normalidad. Para obtener más información, consulte Cambio en la disponibilidad de AWS Mainframe Modernization.

Si su organización aloja datos críticos para la empresa en un entorno de mainframe, obtener información a partir de esos datos es fundamental para impulsar el crecimiento y la innovación. Al desbloquear los datos del mainframe, puede crear inteligencia empresarial más rápida, segura y escalable para acelerar la toma de decisiones, el crecimiento y la innovación basados en los datos en la nube de Amazon Web Services (AWS).

Este patrón presenta una solución para generar información empresarial y crear narrativas compartibles a partir de datos de mainframe mediante la transferencia de archivos AWS Mainframe Modernization con BMC y Amazon Q en QuickSight. Los conjuntos de datos de mainframe se transfieren a Amazon Simple Storage Service (Amazon S3) mediante AWS Mainframe Modernization la transferencia de archivos con BMC. Una AWS Lambda función formatea y prepara el archivo de datos del mainframe para cargarlo en Quick Sight.

Una vez que los datos estén disponibles en QuickSight, puede utilizar las peticiones en lenguaje natural con Amazon Q en QuickSight para crear resúmenes de los datos, formular preguntas y generar historias basadas en datos. No tiene que escribir consultas SQL ni aprender una herramienta de inteligencia empresarial (BI).

Contexto empresarial

Este patrón presenta una solución para casos de uso de análisis de datos e información de datos de mainframe. Con el patrón, puede crear un panel visual para los datos de su empresa. Para demostrar la solución, este patrón utiliza una empresa de atención médica que ofrece planes médicos, dentales y oftalmológicos a sus miembros en los EE. UU. En este ejemplo, la información demográfica y de

planes de los miembros se almacena en las tablas de datos de mainframe. El panel visual muestra lo siguiente:

- Distribución de miembros por región
- Distribución de miembros por género
- Distribución de miembros por edad
- Distribución de miembros por tipo de plan
- Miembros que no han completado la inmunización preventiva

Después de crear el panel, se genera una historia basada en datos que explica la información del análisis anterior. Las historias basadas en datos proporcionan recomendaciones para aumentar el número de miembros que han completado la inmunización preventiva.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Conjuntos de datos de mainframe con datos empresariales
- Acceso a la instalación de un agente de transferencia de archivos en el mainframe

Limitaciones

- El archivo de datos del mainframe debe estar en uno de los formatos de archivo compatibles con QuickSight. Para obtener una lista de los formatos de archivo compatibles, consulte Orígenes de datos compatibles.
- Este patrón utiliza una función de Lambda para convertir el archivo de mainframe a un formato compatible con QuickSight.

Arquitectura

El siguiente diagrama muestra una arquitectura para generar información empresarial a partir de datos de mainframe mediante la transferencia de AWS Mainframe Modernization archivos con BMC y Amazon Q en Quick Sight.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un conjunto de datos de mainframe que contiene datos empresariales se transfiere a Amazon S3 mediante la transferencia de AWS Mainframe Modernization archivos con BMC.
2. La función de Lambda convierte el archivo que está en el bucket de S3 de destino de transferencia de archivos en formato de valores separados por comas (CSV).
3. La función de Lambda envía el archivo convertido al bucket de S3 del conjunto de datos de origen.
4. QuickSight ingiere los datos del archivo.
5. Los usuarios acceden a los datos en QuickSight. Puede usar Amazon Q en QuickSight para interactuar con los datos mediante peticiones en lenguaje natural.

Tools (Herramientas)

Servicios de AWS

- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Mainframe Modernization la transferencia de archivos con BMC convierte y transfiere conjuntos de datos de mainframe a Amazon S3 para casos de uso de modernización, migración y aumento de mainframes.
- Amazon QuickSight es un servicio de BI a escala de la nube que lo ayuda a visualizar, analizar y generar informes de sus datos en un único panel. Este patrón utiliza las capacidades de BI generativa de Amazon Q en QuickSight.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Prácticas recomendadas

- Al crear las funciones AWS Identity and Access Management (IAM) para la transferencia de AWS Mainframe Modernization archivos con BMC y la función Lambda, siga el principio del privilegio mínimo.
- Asegúrese de que el conjunto de datos de origen tenga tipos de datos compatibles con QuickSight. Si el conjunto de datos de origen contiene tipos de datos no compatibles, conviértalos en tipos

de datos compatibles. Para obtener información sobre los tipos de datos de mainframe no compatibles y cómo convertirlos en tipos de datos compatibles con Amazon Q en QuickSight, consulte la sección Recursos relacionados.

Epics

Configure la transferencia de AWS Mainframe Modernization archivos con BMC

Tarea	Descripción	Habilidades requeridas
Instale el agente de transferencia de archivos.	Para instalar el agente de transferencia de AWS Mainframe Modernization archivos, siga las instrucciones de la AWS documentación.	Administrador del sistema de mainframe
Cree un bucket de S3 para la transferencia de archivos de mainframe.	Cree un depósito de S3 para almacenar el archivo de salida de la transferencia de AWS Mainframe Modernization archivos con BMC. En el diagrama de arquitectura, este es el bucket de destino de la transferencia de archivos.	Ingeniero de migraciones
Cree un punto de conexión de transferencia de datos.	1. Cree un depósito de S3 para organizar el archivo de entrada de la unidad central para la transferencia de AWS Mainframe Modernization archivos con BMC. 2. Para crear el punto de conexión de la transferencia de archivos del mainframe, siga las instrucciones de la documentación de AWS.	Especialista en AWS Mainframe Modernization

Conversión de la extensión del nombre del archivo del mainframe para integrarla con QuickSight

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Cree un bucket de S3 para que la función de Lambda copie el archivo de mainframe convertido del bucket de origen al bucket de destino final.	Ingeniero de migraciones
Creación de una función de Lambda.	Para crear una función de Lambda que cambie la extensión del archivo y copie el archivo de mainframe en el bucket de destino, haga lo siguiente: 1. Inicie sesión en y navegue hasta la AWS Lambda consola. Consola de administración de AWS 2. Elija Crear función y, a continuación, elija Crear desde cero. 3. En Nombre de la función, introduzca un nombre para la función. 4. En la lista Tiempo de ejecución, elija Python 3.X. 5. Expanda Cambiar el rol de ejecución predeterm inado y, a continuación, elija Crear un nuevo rol con permisos básicos de Lambda.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	6. Elija Crear función. 7. Seleccione la pestaña Código y, a continuación, pegue el código Python `S3CopyLambda.py` que se proporciona en la sección Información adicional. El código Python se generó mediante Amazon Q en el entorno de desarrollo integrado (IDE) de Microsoft Visual Studio. 8. Edite el `destination_bucket_name` para el nombre del bucket de S3 que creó anteriormente y `change destination_file_key` para el nombre del archivo del mainframe. 9. Implemente la función de Lambda.	

Tarea	Descripción	Habilidades requeridas
Cree un desencadenador de Amazon S3 para invocar una función de Lambda.	Para configurar un desencadenador que invoque la función de Lambda, haga lo siguiente: 1. Abra la página Funciones en la consola de Lambda. 2. Elija la función de Lambda. 3. En el panel Información general de la función, elija Añadir desencadenador. 4. En la lista desplegable Configuración del desencadenador, seleccione S3. 5. En el campo Bucket, escriba el nombre del bucket de origen. 6. En la lista desplegable Tipo de evento, seleccione Todos los eventos de creación de objetos. 7. Seleccione la casilla de verificación Acepto que no se recomienda usar el mismo bucket de S3 para la entrada y la salida y, a continuación, elija Añadir. Para obtener más información, consulte Tutorial: utilizar un desencadenador de Amazon S3 para invocar una función de Lambda.	Líder de migración

Tarea	Descripción	Habilidades requeridas
Proporcione permisos de IAM para la función de Lambda.	Se requieren permisos de IAM para que la función de Lambda acceda a los buckets de S3 del conjunto de datos de origen y destino de la transferencia de archivos. Actualice la política asociada al rol de ejecución de la función de Lambda mediante la concesión de permisos `s3:GetObject` y `s3:DeleteObject` para el bucket de S3 de destino de la transferencia de archivos y el acceso `s3:PutObject` al bucket de S3 del conjunto de datos de origen. Para obtener más información, consulte la sección Creación de una política de permisos del Tutorial: utilizar un desencadenador de Amazon S3 para invocar una función de Lambda.	Líder de migración

Definición de una tarea de transferencia de datos de mainframe

Tarea	Descripción	Habilidades requeridas
Cree una tarea de transferencia de para copiar el archivo de mainframe en el bucket de S3.	Para crear una tarea de transferencia de archivos de mainframe, siga las instrucciones de la documentación de	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	AWS Mainframe Modernization. **Note** Especifique la codificación de la página de códigos fuente como IBM1047 y la codificación de la página de códigos de destino como UTF-8.	
Compruebe la tarea de transferencia.	Para comprobar que la transferencia de datos se ha realizado correctamente, siga las instrucciones de la documentación de AWS Mainframe Modernization. Confirme que el archivo de mainframe esté en el bucket de S3 de destino de la transferencia de archivos.	Líder de migración

Tarea	Descripción	Habilidades requeridas
Compruebe la función de copia de Lambda.	Compruebe que se haya iniciado la función de Lambda y que el archivo se haya copiado con la extensión .csv en el bucket de S3 del conjunto de datos de origen. El archivo .csv creado por la función de Lambda es el archivo de datos de entrada de QuickSight. Para ver datos de ejemplo, consulte el archivo `Sample-data-member-healthcare-APG` en la sección de conexiones.	Líder de migración

Conexión de QuickSight a los datos del mainframe

Tarea	Descripción	Habilidades requeridas
Configure QuickSight.	Para configurar QuickSight, siga las instrucciones de la documentación de AWS.	Líder de migración
Cree un conjunto de datos para QuickSight.	Para crear un conjunto de datos para QuickSight, siga las instrucciones de la documentación de AWS. El archivo de datos de entrada es el archivo de mainframe convertido que se creó al definir la tarea de transferencia de datos de mainframe.	Líder de migración

Obtenga información empresarial a partir de los datos del mainframe mediante Amazon Q en QuickSight

Tarea	Descripción	Habilidades requeridas
Configure Amazon Q en QuickSight.	Esta capacidad requiere la edición Enterprise. Para configurar Amazon Q en QuickSight, haga lo siguiente: 1. Para obtener el complemento Amazon Q, siga las instrucciones del paso 1: Obtención del complemento Q de la documentación de AWS. 2. Para utilizar las capacidades de BI generativa de Amazon Q, actualice las cuentas de sus usuarios. Siga las instrucciones de la documentación de AWS. 3. Cree un tema de Amazon Q con el conjunto de datos que ha creado anteriormente. Siga las instrucciones de la documentación de AWS. 4. Para configurar los metadatos del tema de manera que sean compatibles con el lenguaje natural, siga las instrucciones de la documentación de AWS.	Líder de migración

Tarea	Descripción	Habilidades requeridas
Analice los datos del mainframe y cree un panel visual.	Para analizar y visualizar sus datos en QuickSight, haga lo siguiente: 1. Para crear el análisis de datos del mainframe, siga las instrucciones de la documentación de AWS. Para el conjunto de datos, elija el conjunto de datos creado en el paso anterior. 2. En la página de análisis, elija Crear elemento visual. 3. En la ventana Crear tema para el análisis, elija Actualizar tema existente. 4. En la lista desplegable Seleccione un tema, elija el tema que creó anteriorm ente. 5. Seleccione Vinculación de temas. 6. Después de vincular el tema, elija Crear elemento visual para abrir la ventana Crear un elemento visual de Amazon Q. 7. En la barra de peticiones, escriba sus preguntas de análisis. Los ejemplos de preguntas que se utilizan para este patrón son los siguientes:	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	• Mostrar la distribución de miembros por región • Mostrar la distribución de miembros por edad • Mostrar la distribución de miembros por género • Mostrar la distribución de miembros por tipo de plan • Mostrar los miembros que no han completado la inmunización preventiva Después de introducir las preguntas, elija Crear. Amazon Q en QuickSigh t crea los elementos visuales. 8. Para añadir los elementos visuales a su panel visual, elija AÑADIR AL ANÁLISIS. Cuando termine, puede publicar el panel de control para compartirlo con otras personas de su organización. Para ver ejemplos, consulte el panel visual del mainframe en la sección de información adicional.	

Creación de una historia basada en datos con Amazon Q en QuickSight a partir de datos del mainframe

Tarea	Descripción	Habilidades requeridas
Cree una historia basada en datos.	Cree una historia basada en datos para explicar la información del análisis anterior y genere una recomendación para aumentar la inmunización preventiva de los miembros: 1. Para crear la historia basada en datos, siga las instrucciones de la documentación de AWS. 2. Para la petición de la historia basada en datos, utilice lo siguiente: `Build a data story about Region with most numbers of members. Also show the member distribution by medical plan, vision plan, dental plan. Recommend how to motivate members to complete immunizat ion. Include 4 points of supportin g data for this pattern.`	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	También puede crear su propia petición para generar historias basadas en datos que le sirvan para obtener información empresarial adicional. 3. Elija Añadir elementos visuales y añada los elementos visuales que sean relevantes para la historia basada en datos. Para este patrón, utilice los elementos visuales que creó anteriormente. 4. Elija Compilar. 5. Para ver un ejemplo de salida de una historia basada en datos, consulte Salida de una historia basada en datos en la sección de información adicional.	
Vea la historia basada en datos generada.	Para ver la historia basada en datos que se ha generado, siga las instrucciones de la documentación de AWS.	Líder de migración
Edite una historia basada en datos generada.	Para cambiar el formato, el diseño o los elementos visuales de una historia basada en datos, siga las instrucciones de la documentación de AWS.	Líder de migración

Tarea	Descripción	Habilidades requeridas
Comparta una historia basada en datos.	Para compartir una historia basada en datos, siga las instrucciones de la documentación de AWS.	Ingeniero de migraciones

Resolución de problemas

Problema	Solución
No se han podido detectar los archivos o conjuntos de datos del mainframe introducidos en los criterios de búsqueda de conjuntos de datos para Crear una tarea de transferencia en AWS Mainframe Modernization la transferencia de archivos con BMC.	1. En primer lugar, compruebe la conexión seleccionando los puntos finales de transferencia de datos en la consola AWS Mainframe Modernization Transferir con BMC. Si el tiempo del último latido es superior a 2 minutos, significa que no se ha establecido la conexión para la transferencia de archivos. Si el tiempo del último latido es inferior a 2 minutos para el agente que se ejecuta en el mainframe, la conexión con el agente se ha realizado correctamente. Continúe con el paso 2. 2. Compruebe la AWS Secrets Manager configuración. Se debe configurar una clave secreta en Secrets Manager con una clave de `userId` (I mayúscula) con un valor del ID de usuario del mainframe y una clave de `password` con el valor de la contraseña del mainframe. Las claves secretas `userId` y `password` distinguen mayúsculas de minúsculas y se deben introducir tal cual.

Recursos relacionados

Para convertir tipos de datos de mainframe como PACKED-DECIMAL (COMP-3) o BINARY (COMP o COMP-4) a un tipo de datos compatible con QuickSight, consulte los siguientes patrones:

- Convierta y descomprima datos EBCDIC a ASCII mediante Python AWS
- Convierta archivos de mainframe del formato EBCDIC al formato ASCII delimitado por caracteres en Amazon S3 mediante AWS Lambda

Información adicional

S3 .py CopyLambda

El siguiente código de Python se generó mediante una petición con Amazon Q en un IDE:

```
#Create a lambda function triggered by S3. display the S3 bucket name and key
import boto3
s3 = boto3.client('s3')
def lambda_handler(event, context):
print(event)
bucket = event['Records'][0]['s3']['bucket']['name']
key = event['Records'][0]['s3']['object']['key']
print(bucket, key)
#If key starts with object_created, skip copy, print "copy skipped". Return lambda with
 key value.
if key.startswith('object_created'):
print("copy skipped")
return {
'statusCode': 200,
'body': key
}
# Copy the file from the source bucket to the destination bucket.
 Destination_bucket_name = 'm2-filetransfer-final-opt-bkt'. Destination_file_key =
 'healthdata.csv'
copy_source = {'Bucket': bucket, 'Key': key}
s3.copy_object(Bucket='m2-filetransfer-final-opt-bkt', Key='healthdata.csv',
 CopySource=copy_source)
print("file copied")
#Delete the file from the source bucket.
s3.delete_object(Bucket=bucket, Key=key)
return {
'statusCode': 200,
```

```
'body': 'Copy Successful'
}
```

Panel visual de mainframe

Amazon Q creó el siguiente elemento visual de datos en QuickSight para la pregunta de análisis `show member distribution by region`.

Amazon Q creó el siguiente elemento visual de datos en QuickSight para la pregunta `show member distribution by Region who have not completed preventive immunization, in pie chart`.

Salida de una historia basada en datos

Las siguientes capturas de pantalla muestran secciones de la historia basada en datos creada por Amazon Q en QuickSight para la petición `Build a data story about Region with most numbers of members. Also show the member distribution by medical plan, vision plan, dental plan. Recommend how to motivate members to complete immunization. Include 4 points of supporting data.`

En la introducción, la historia basada en datos recomienda elegir la región con más miembros para obtener el mayor impacto de las iniciativas de inmunización.

La historia con datos proporciona un análisis del número de miembros de las tres principales regiones y menciona al sudoeste como la región que más se centra en las iniciativas de inmunización.

> **Note**
>
> Cada una de las regiones del sudoeste y del noreste tiene ocho miembros. Sin embargo, el sudoeste tiene más miembros que no están completamente vacunados, por lo que tiene más posibilidades de beneficiarse de las iniciativas para aumentar las tasas de inmunización.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Implemente la autenticación basada en Microsoft Entra ID en una aplicación de mainframe modernizada de AWS Blu Age

Vishal Jaswani y Rimpy Tewani, Amazon Web Services

Resumen

> **Note**
>
> AWS Mainframe Modernization El servicio (experiencia de entorno de ejecución gestionado) ya no está abierto a nuevos clientes. Para obtener funcionalidades similares a las AWS Mainframe Modernization de Service (experiencia en entornos de ejecución gestionados), explore AWS Mainframe Modernization Service (experiencia autogestionada). Los clientes existentes pueden seguir utilizando el servicio con normalidad. Para obtener más información, consulte Cambio en la disponibilidad de AWS Mainframe Modernization.

Las aplicaciones de mainframe que se modernizan mediante patrones de refactorización, como las de AWS Mainframe Modernization Refactor con AWS Blu Age, requieren una integración cuidadosa de los mecanismos de autenticación en la nueva arquitectura de la aplicación. Esta integración suele abordarse como una actividad posterior a la modernización. La tarea puede ser compleja y, a menudo, implica la migración o la externalización de los sistemas de autenticación existentes para alinearlos con los estándares de seguridad modernos y las prácticas nativas en la nube. Los desarrolladores deben considerar cómo implementar la autenticación de manera eficaz mientras trabajan dentro de las limitaciones del tiempo de ejecución y las bibliotecas de la aplicación modernizada. Tras la modernización, AWS proporciona formas de facilitar la integración del código moderno de AWS Blu Age con sistemas de administración de identidades y accesos, como Amazon Cognito y Microsoft Entra ID (anteriormente conocido como Azure AD).

Este patrón explica cómo implementar un mecanismo de autenticación en una aplicación modernizada cuando el proveedor de autenticación es Microsoft Entra ID, sin perder tiempo en investigaciones y pruebas. El patrón proporciona lo siguiente:

- Bibliotecas de Angular pertinentes y probadas en campo de la Biblioteca de autenticación de Microsoft (MSAL) y otra documentación de Microsoft Entra ID que son esenciales para la implementación de la autenticación.
- Se requieren configuraciones en el entorno de ejecución de AWS Blu Age para habilitar Spring Security mediante la OAuth versión 2.0.

- Una biblioteca que captura las identidades de los usuarios autenticados y las pasa al AWS Blu Age Runtime.
- Medidas de seguridad que recomendamos implementar.
- Sugerencias de solución de problemas frecuentes con la configuración de Microsoft Entra ID.

> **Note**
>
> Este patrón utiliza la biblioteca de OAuth extensiones AWS Blu Age, que se proporciona a los clientes como parte de su contratación con los servicios AWS profesionales. Esta biblioteca no forma parte de AWS Blu Age Runtime.

Requisitos previos y limitaciones

Requisitos previos

- Una aplicación modernizada que fue producida por las herramientas de refactorización y modernización de mainframes de AWS Blu Age. Este patrón se utiliza CardDemocomo ejemplo de una aplicación de mainframe de código abierto.
- La biblioteca de OAuth extensiones de AWS Blu Age, proporcionada por el equipo de AWS Blu Age durante su contratación con AWS Professional Services.
- Activa Cuenta de AWS para implementar y probar la aplicación modernizada.
- Familiaridad con los archivos de configuración de AWS Blu Age y los fundamentos de Microsoft Entra ID.

Limitaciones

- Este patrón abarca la autenticación OAuth 2.0 y los flujos básicos de autorización basados en tokens. Los escenarios de autorización avanzada y los mecanismos de control de acceso detallados no están dentro del alcance.
- Algunos Servicios de AWS no están disponibles en todos. Regiones de AWS Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

Este patrón se desarrolló mediante lo siguiente:

- AWS Blu Age Runtime versión 4.1.0 (el patrón también funciona con versiones posteriores compatibles con versiones anteriores)
- Biblioteca MSAL, versión 3.0.23
- Java Development Kit (JDK), versión 17
- Angular, versión 16.1

Arquitectura

Pila de tecnología de origen

En los entornos de mainframe típicos, la autenticación se implementa a través de los perfiles de usuario. Estos perfiles identifican a los usuarios del sistema, definen quién puede iniciar sesión y especifican qué funciones pueden llevar a cabo los usuarios con los recursos del sistema. Los perfiles de usuario los administran los responsables de seguridad o los administradores de seguridad.

Pila de tecnología de destino

- ID de Microsoft Entra
- Backend modernizado basado en Java Spring Boot
- AWS Blu Age Runtime
- Spring Security con OAuth 2.0
- Aplicación de una sola página de Angular (SPA)

Arquitectura de destino

AWS El tiempo de ejecución de Blu Age admite la autenticación OAuth basada en la versión 2.0 de forma predeterminada, por lo que el patrón utiliza ese estándar para proteger el backend APIs.

En el diagrama siguiente se ilustra el flujo del proceso.

> **Note**
>
> En el diagrama se incluye Amazon Aurora como ejemplo de modernización de bases de datos, aunque Aurora no se incluye en los pasos de este patrón.

donde:

1. Un usuario intenta autenticarse con Microsoft Entra ID.
2. Microsoft Entra ID devuelve los tokens de actualización, acceso e ID que la aplicación utiliza en llamadas posteriores.
3. El interceptor MSAL incluye el token de acceso en el `Authorization` encabezado de una solicitud HTTPS para llamar al Blu Age Runtime. AWS
4. La `extension-oauth` biblioteca AWS Blu Age extrae la información del usuario del encabezado mediante un archivo de configuración de AWS Blu Age Runtime (`application-main.yml`) y coloca esta información en un `SharedContext` objeto para que la lógica empresarial pueda consumirla.

   > **Note**
   >
   > `SharedContext`es un componente de tiempo de ejecución proporcionado por AWS Blu Age que gestiona la información de contexto y estado de la aplicación en toda la aplicación modernizada. Para obtener más información sobre los componentes y las actualizaciones de AWS Blu Age Runtime, consulta las notas de la versión de AWS Blu Age en la AWS Mainframe Modernization documentación. Para obtener más información sobre el `application-main.yml` archivo, consulte Configurar la configuración de AWS Blu Age Runtime en la AWS Mainframe Modernization documentación.

5. El AWS Blu Age Runtime comprueba si el token está presente.
   a. Si el token está presente, se comunica con Microsoft Entra ID para comprobar su validez.
   b. Si el token no está presente, el AWS Blu Age Runtime devuelve un error con el código de estado HTTP 403.
6. Si el token es válido, el AWS Blue Age Runtime permite que la lógica empresarial continúe. Si el token no es válido, AWS Blu Age Runtime devuelve un error con el código de estado HTTP 403.

OAuth Flujo de trabajo 2.0

Para ver un diagrama de alto nivel del flujo de trabajo OAuth 2.0, consulte la documentación de Microsoft Entra.

Tools (Herramientas)

Servicios de AWS

AWS Mainframe Modernizationproporciona herramientas y recursos para ayudarlo a planificar e implementar la migración y la modernización de los mainframes a los entornos de tiempo de ejecución AWS gestionados. Puede utilizar las funciones de refactorización de este servicio, que proporciona AWS Blu Age, para convertir y modernizar sus aplicaciones de mainframe antiguas.

> **Note**
>
> AWS Mainframe Modernization El servicio (experiencia de entorno de ejecución gestionado) ya no está abierto a nuevos clientes. Para obtener funcionalidades similares a las AWS Mainframe Modernization de Service (experiencia en entornos de ejecución gestionados), explore AWS Mainframe Modernization Service (experiencia autogestionada). Los clientes existentes pueden seguir utilizando el servicio con normalidad. Para obtener más información, consulte Cambio en la disponibilidad de AWS Mainframe Modernization.

Repositorio de código

La CardDemo aplicación se ha actualizado para demostrar la integración con Microsoft Entra ID. Puedes acceder al código de este patrón desde el GitHub repositorio.

Configuración de backend

Este patrón requiere cambios en el archivo de `application-main.yml` configuración para habilitar Spring Security mediante el uso de la OAuth versión 2.0 en la aplicación de fondo. El archivo `.yml` tiene este aspecto:

```
gapwalk-application.security: enabled
gapwalk-application:
  security:
    identity: oauth
    issuerUri: ${issuerUrl}
```

```
    claim:
      claims:
        -
          claimName: upn
          claimMapValue: username
spring:
  autoconfigure:
    exclude:
     -
 org.springframework.boot.autoconfigure.security.oauth2.client.servlet.OAuth2ClientAutoConfigur
     -
 org.springframework.boot.autoconfigure.security.oauth2.resource.servlet.OAuth2ResourceServerAu
  security:
    oauth2:
      client:
        registration:
          azure:
            client-id: {clientId}
            client-secret: ${clientSecret}
            provider: azure
            authorization-grant-type: authorization_code
            redirect-uri: ${redirectUri}
            scope: openid

        provider:
          azure:
            authorization-uri: ${gapwalk-application.security.issuerUri}/oauth2/v2.0/
authorize
            token-uri:  ${gapwalk-application.security.issuerUri}/oauth2/v2.0/token
            jwk-set-uri: ${gapwalk-application.security.issuerUri}/discovery/v2.0/keys
      resourceserver:
        jwt:
          jwk-set-uri: ${gapwalk-application.security.issuerUri}/discovery/v2.0/keys
```

AWS Biblioteca de filtros de OAuth extensiones Blu Age

La biblioteca de OAuth extensiones de AWS Blu Age la proporciona el equipo de AWS Blu Age durante su contratación con AWS Professional Services.

Esta biblioteca lee la configuración `claim.claims` del archivo `application-main.yml` que se muestra en el bloque de código anterior. Esta configuración es una lista. Cada elemento de la lista proporciona dos valores: `claimName` y `claimMapValue`. `claimName` representa el nombre de una clave en un token web JSON (JWT) enviado por el frontend y `claimMapValue` es el nombre

de la clave en `SharedContext`. Por ejemplo, si quieres capturar el ID de usuario en el backend, establezca `claimName` en el nombre de la clave en el JWT que contiene el valor de `userId` proporcionado por Microsoft Entra ID y establezca `claimMapValue` en el nombre de la clave para obtener el ID de usuario en el código del backend.

Por ejemplo, si establece `UserId` en `claimMapValue`, puede usar el siguiente código para extraer el ID de usuario:

```
SharedContext.get().getValue("userId", [UserId]);
```

Prácticas recomendadas

Al implementar este patrón, tenga en cuenta las siguientes consideraciones de seguridad importantes.

> **Important**
>
> Este patrón proporciona una base para la integración de la autenticación. Le recomendamos que implemente medidas de seguridad además de las descritas en esta sección en función de los requisitos de su empresa antes de implementarla en producción.

- AWS seguridad de configuración.Mueva los valores de configuración confidenciales de `application-main.yml` a AWS Secrets Manager. Por ejemplo, configure las siguientes propiedades mediante Secrets Manager:

  ```
  security:
      oauth2:
        client:
          registration:
            azure:
              client-id: {clientId}
              client-secret: ${clientSecret}
  ```

  Para obtener más información sobre cómo usar Secrets Manager para configurar los parámetros de AWS Blu Age, consulta los secretos de AWS Blu Age Runtime en la AWS Mainframe Modernization documentación.
- Protección del entorno del tiempo de ejecución. Configure el entorno de aplicaciones modernizado con los controles AWS de seguridad adecuados:

```
server:
  tomcat:
    remoteip:
     protocol-header: X-Forwarded-Proto
     remote-ip-header: X-Forwarded-For
  forward-headers-strategy: NATIVE
```

- CloudWatch Registro de Amazon. Considere la posibilidad de agregar el archivo `logback-spring.xml to src/main/resources`:

```
<configuration>
 <appender name="CLOUDWATCH"
 class="com.amazonaws.services.logs.logback.CloudWatchAppender">
   <logGroup>/aws/bluage/application</logGroup>
   <logStream>${AWS_REGION}-${ENVIRONMENT}</logStream>
   <layout>
    <pattern>%d{yyyy-MM-dd HH:mm:ss} [%thread] %-5level %logger{36} - %msg%n</
pattern>
   </layout>
 </appender>

 <root level="INFO">
 <appender-ref ref="CLOUDWATCH"/>
 </root>
</configuration>
```

  Para obtener información sobre cómo habilitar el rastreo con la correlación CloudWatch, consulte Habilitar la correlación entre el rastreo y el registro en la CloudWatch documentación.

- Configuración y gestión de tokens. Configure la vida útil de los tokens en Microsoft Entra ID para adaptarla a sus requisitos de seguridad. Configure los tokens de acceso para que caduquen en 1 hora y actualícelos para que caduquen en 24 horas. En la configuración de AWS Blu Age Runtime (`application-main.yml`), asegúrese de que la validación de JWT esté configurada correctamente con el URI del emisor y los valores de audiencia exactos del registro de la aplicación Entra ID.

  Cuando un token caduca y se actualiza:

  1. El interceptor de errores de la aplicación de Angular gestiona la respuesta 401 obteniendo un nuevo token a través de MSAL.
  2. El nuevo token se envía con la solicitud posterior.

3. El OAuth filtro del AWS Blu Age Runtime valida el nuevo token y se actualiza automáticamente `SharedContext` con la información de usuario actual. Esto garantiza que la lógica empresarial siga teniendo acceso al contexto de usuario válido a través de las llamadas `SharedContext.get().getValue()`.

Para obtener más información sobre los componentes de AWS Blu Age Runtime y sus actualizaciones, consulta las notas de la versión de AWS Blu Age.

- Seguridad del tiempo de ejecución de AWS Blu Age. La `oauth2-ext` biblioteca proporcionada por AWS Blu Age debe colocarse en la ubicación correcta del directorio compartido (`{app-server-home}/shared/`) con los permisos de archivo adecuados. Compruebe que la biblioteca extrae correctamente la información del usuario JWTs comprobando la población de `SharedContext` objetos en sus registros.
- Configuración de notificaciones específicas. En `application-main.yml`, defina las notificaciones que necesita de Microsoft Entra ID de forma explícita. Por ejemplo, para capturar el correo electrónico y los roles del usuario, especifique lo siguiente:

```
gapwalk-application:
  security:
    claim:
      claims:
        - claimName: upn
          claimMapValue: username
        - claimName: roles
          claimMapValue: userRoles
        - claimName: email
          claimMapValue: userEmail
```

- Gestión de errores. Agregue el manejo de errores para abordar los errores de autenticación en su aplicación de Angular; por ejemplo:

```
@Injectable()
export class AuthErrorInterceptor implements HttpInterceptor {
  intercept(request: HttpRequest<any>, next: HttpHandler): Observable<HttpEvent<any>>
 {
    return next.handle(request).pipe(
      catchError((error: HttpErrorResponse) => {
        if (error.status === 401) {
          // Handle token expiration
          this.authService.login();
        }
```

```
        if (error.status === 403) {
          // Handle unauthorized access
          this.router.navigate(['/unauthorized']);
        }
        return throwError(() => error);
      })
    );
  }
}
```

- Configuración del tiempo de espera de la sesión. Configure los ajustes de tiempo de espera de la sesión tanto en el AWS Blu Age Runtime como en el Microsoft Entra ID. Por ejemplo, agregue el siguiente código al archivo `application-main.yml`:

```
server:
  servlet:
    session:
      timeout: 3600 # 1 hour in seconds
```

- MsalGuard. Debe implementar la MsalGuard función en todas las rutas protegidas para evitar el acceso no autorizado. Por ejemplo:

```
const routes: Routes = [
    { path: '', redirectTo: '/transaction-runner', pathMatch: 'full' },
    { path: 'transaction-runner', component: TransactionRunnerComponent,
 canActivate:guards },
    { path: 'user-info', component: UserInfoComponent, canActivate:guards },
    { path: 'term/:transid/:commarea', component: TermComponent,
 canActivate:guards },
 { path: 'code', component: TransactionRunnerComponent  }
];
```

Se podrá acceder a las rutas que MsalGuard no estén protegidas sin autenticación, lo que podría exponer funciones confidenciales. Asegúrese de que todas las rutas que requieren autenticación incluyan las protecciones en su configuración.

Epics

Configuración de Microsoft Entra ID

Tarea	Descripción	Habilidades requeridas
Configurar una cuenta de Microsoft Azure para crear una instancia de Entra ID.	Para ver las opciones e instrucciones, consulte el sitio web de Microsoft Azure.	Desarrollador de aplicaciones
Configurar una instancia de Microsoft Entra ID en la aplicación.	Para obtener informaci ón sobre cómo agregar la autenticación de Microsoft Entra ID B2C (Azure AD B2C) a su SPA de Angular, consulte la documentación de Microsoft . En concreto: 1. Registre su aplicación y los identificadores. 2. Exponga el punto final de las transacciones de AWS Blu Age añadiendo y exponiendo un ámbito personalizado. 3. Tras definir el ámbito y la URL de la API, configure estos valores en las propiedades `apiUri` y `apiScope` del archivo `environment.ts` en el repositorio de código.	Desarrollador de aplicaciones

Clona el repositorio e implementa tu código de AWS Blu Age

Tarea	Descripción	Habilidades requeridas
Clona el GitHub repositorio para obtener el código angular necesario para la autentica ción.	Ejecuta el siguiente comando para clonar el GitHub repositor io que viene con este patrón en tu directorio de trabajo actual local: `git clone https://g ithub.com/aws-samp les/sample-microsoft- entra-id-based-auth- in-aws-bluage-moderniz ed-mainframe-app.git`	Desarrollador de aplicaciones
Implemente el código modernizado de AWS Blu Age en un servidor Tomcat para implementar la autenticación.	Para configurar el entorno local que incluye Tomcat y el servidor de desarrollo Angular, siga los pasos de instalaci ón proporcionados por el equipo de AWS Blu Age como parte de la interacción de los clientes con AWS los servicios profesionales.	Desarrollador de aplicaciones

Creación de la solución de autenticación

Tarea	Descripción	Habilidades requeridas
Habilitar la seguridad del tiempo de ejecución de AWS Blu Age para proteger los puntos de conexión de la API de REST de AWS Blu Age.	Configure el `application-main.yml` archivo que utiliza el AWS Blu Age Runtime de la siguiente manera. Para ver un ejemplo de este archivo, consulte la sección	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	Repositorio de código, incluida anteriormente en este patrón. • `spring:security:oauth2:client:*` habilita la compatibilidad con el cliente Spring Security OAuth 2.0. Sustituya la configuración por valores que sean específicos de la configuración de su instancia de Microsoft Entra ID. • `spring:security:oauth2:resourceserver` habilita la compatibilidad con el servidor de recursos Spring Security OAuth 2.0. • `gapwalk-application.security.issuerUri` especifica la URL del proveedor de identidades para obtener información de configuración, como el punto de conexión de autorización, el punto de conexión de tokens, etc. • `gapwalk-application.security.identity` debe definirse en `oauth`. • `gapwalk-application.security.claim.claims` especifica la lista de notificaciones necesaria	

Tarea	Descripción	Habilidades requeridas
	s para capturar el usuario IDs y los nombres de usuario. Para ver un ejemplo, consulte la sección Repositorio de código, incluida anteriormente en este patrón. • `gapwalk-application.security` debe definirse en `enabled`. • `spring.autoconfigure.exclude` debe eliminarse para habilitar la autenticación.	
Incorporar el código de ejemplo de su entorno local a su base de código de Angular modernizada de Blu Age.	Para obtener información sobre cómo incorporar el ejemplo en su base de código angular modernizada de AWS Blu Age, consulte la sección sobre el repositorio de códigos que aparece anteriormente en este patrón.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Colocar la biblioteca `oauth2-ext` en el directorio compartido.	Coloque la biblioteca `oauth2-ext` en el directorio compartido del servidor de aplicaciones para que su aplicación modernizada de AWS Blu Age pueda usarla.Ejecute los siguientes comandos :
	`cd oauth2-ext/target`
	`cp extension-oauth-filter-<version>.jar /{app-server-home}/shared/`
		Desarrollador de aplicaciones

Implementación de la solución de autenticación

Tarea	Descripción	Habilidades requeridas

Implementar la aplicación de frontend.	Ejecute los comandos siguientes para iniciar la aplicación de frontend de forma local:
	`npm install`
	`ng serve --ssl`
	`npm start`
	Note
	Al agregar la marca `--ssl` al comando `ng serve`, se garantiza que el servidor de desarrollo utilice
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	HTTPS, que es más seguro que otros protocolos y proporciona una mejor simulación de un entorno de producció n.	
Iniciar la aplicación de backend.	Inicie el servidor de Tomcat en Eclipse.	Desarrollador de aplicaciones

Pruebe la aplicación

Tarea	Descripción	Habilidades requeridas
Probar la funcionalidad de inicio de sesión.	Acceda a la aplicación implementada localmente en `http://localhost:4200` para comprobar que se pide a los usuarios que confirmen su identidad. **Note** Aquí se usa HTTP con fines ilustrativos. En un entorno de producción u otro entorno de acceso público, debe utilizar HTTPS por motivos de seguridad. Incluso para el desarrollo local, le recomenda	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	mos que configure HTTPS siempre que sea posible. Debería aparecer el mensaje de inicio de sesión de Microsoft y los usuarios configurados en Microsoft Entra ID deberían poder acceder a la aplicación.	

Tarea	Descripción	Habilidades requeridas
Probar el encabezado de la autorización de la solicitud.	**Note** En los siguientes pasos, se usa la CardDemoaplicación como ejemplo. Los pasos de prueba para otras aplicaciones modernas variarán. 1. Inicie la transacción `CC00` en la CardDemo aplicación. 2. Inicie sesión con las credenciales del usuario. Por ejemplo, si va a usar el taller autoguiado de nivel 3 de AWS Blu Age, puede usar el nombre `USER0001` y la contraseña `PASSWORD` como credenciales. 3. Abra la ventana Herramientas para desarrolladores en la misma pestaña de su navegador. 4. Abra la pestaña Red y compruebe la solicitud enviada al backend `http://localhost:8080/gapwalk-application/transaction` . 5. Compruebe el encabezado de la solicitud y verifique que ve un encabezado	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	de autorización con el valor `Bearer <token>`, donde `<token>` es un valor generado por Microsoft Entra ID.	
Probar la funcionalidad de cierre de sesión.	Elija Salir para cerrar sesión e intente acceder de nuevo a la aplicación. Debería ver un nuevo mensaje de inicio de sesión.	Desarrollador de aplicaciones

Resolución de problemas

Problema	Solución
El token emitido por Microsoft Entra ID no es compatible con la seguridad de Spring Boot OAuth 2.0.	Para resolver el problema, consulta Microsoft Entra ID OAuth Flow en el OAuth blog.
Preguntas generales relacionadas con los tokens.	Para decodificar y ver el contenido de un token JWT, utilice el sitio web https://jwt.io/.

Recursos relacionados

- Para obtener información sobre cómo refactorizar tu aplicación mediante AWS Blu Age, consulta la AWS Mainframe Modernization documentación.
- Para entender cómo funciona la OAuth versión 2.0, consulte el sitio web de la OAuth versión 2.0.
- Para obtener información general sobre la Biblioteca de autenticación de Microsoft (MSAL), consulte la documentación de Microsoft Entra.
- Para obtener información sobre los perfiles de usuario en un sistema AS/400, consulte el tutorial de IBM i (AS400).

- Para ver el OAuth flujo de autenticación 2.0 y OpenID Connect (OIDC) en la plataforma de identidad de Microsoft, consulte la documentación de Microsoft Entra.

Integrar el controlador universal Stonebranch con AWS Mainframe Modernization

Vaidy Sankaran y Pablo Alonso Prieto, Amazon Web Services

Robert Lemieux y Huseyin Gomleksizoglu, Stonebranch

Resumen

Nota: AWS Mainframe Modernization El servicio (experiencia de entorno de ejecución gestionado) ya no está abierto a nuevos clientes. Para obtener funciones similares a las AWS Mainframe Modernization de Service (experiencia en entornos de ejecución gestionados), explore AWS Mainframe Modernization Service (experiencia autogestionada). Los clientes existentes pueden seguir utilizando el servicio con normalidad. Para obtener más información, consulte Cambio en la disponibilidad de AWS Mainframe Modernization.

Este patrón explica cómo integrar la orquestación de cargas de trabajo de Stonebranch Universal Automation Center (UAC) con el servicio de AWS Mainframe Modernization de Amazon Web Services (AWS). El servicio de AWS Mainframe Modernization migra y moderniza las aplicaciones de mainframe a la nube de AWS. Ofrece dos patrones: Redefinición de la plataforma de AWS Mainframe Modernization con Micro Focus y la refactorización automatizada de AWS Mainframe Modernization con AWS Blu Age.

Stonebranch UAC es una plataforma de automatización y organización de TI en tiempo real. El UAC está diseñado para automatizar y organizar los trabajos, las actividades y los flujos de trabajo en los sistemas de TI híbridos, desde los entornos locales hasta los de AWS. Los clientes empresariales que utilizan sistemas de mainframe están realizando la transición a infraestructuras y aplicaciones modernizadas centradas en la nube. Las herramientas y los servicios profesionales de Stonebranch facilitan la migración de los programadores y las capacidades de automatización existentes a la nube de AWS.

Al migrar o modernizar sus programas de mainframe a la nube de AWS mediante el servicio AWS Mainframe Modernization, puede utilizar esta integración para automatizar la programación por lotes, aumentar la agilidad, mejorar el mantenimiento y reducir los costos.

Este patrón proporciona instrucciones para integrar el programador Stonebranch con las aplicaciones de mainframe migradas al tiempo de ejecución de Micro Focus Enterprise del servicio de AWS Mainframe Modernization. Este patrón es para arquitectos de soluciones,

desarrolladores, consultores, especialistas en migración y otras personas que trabajan en migraciones, modernizaciones, operaciones o DevOps

Resultados específicos

Este patrón se centra en proporcionar los siguientes resultados objetivo:

- La capacidad de programar, automatizar y ejecutar trabajos por lotes de mainframe que se ejecutan en el servicio AWS Mainframe Modernization (tiempo de ejecución de Microfocus) de Stonebranch Universal Controller.
- Supervise los procesos por lotes de la aplicación desde el controlador universal Stonebranch.
- Start/Restart/Rerun/Stopprocesa por lotes de forma automática o manual desde el controlador universal Stonebranch.
- Recupere los resultados de los procesos por lotes de AWS Mainframe Modernization.
- Capture los CloudWatch registros de AWS de los trabajos por lotes en Stonebranch Universal Controller.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una aplicación de demostración de Micro Focus Bankdemo con archivos de Job Control Language (JCL) y un proceso por lotes implementado en un entorno del servicio de AWS Mainframe Modernization (tiempo de ejecución de Micro Focus)
- Conocimientos básicos sobre cómo crear e implementar una aplicación de mainframe que se ejecute en Micro Focus Enterprise Server
- Conocimientos básicos del controlador universal Stonebranch
- Licencia de prueba de Stonebranch (póngase en contacto con Stonebranch)
- Instancias de Amazon Elastic Compute Cloud (Amazon EC2) para Windows o Linux (por ejemplo, xlarge) con un mínimo de cuatro núcleos, 8 GB de memoria y 2 GB de espacio en disco
- Apache Tomcat, versión 8.5.x o 9.0.x
- Entorno de ejecución de Java (JRE) o OpenJDK versión 8 u 11
- Edición de Amazon Aurora compatible con MySQL
- Bucket de Amazon Simple Storage Service (Amazon S3) para repositorio de exportación

- Amazon Elastic File System (Amazon EFS) para las conexiones del agente Stonebranch Universal Message Service (OMS) para una alta disponibilidad (HA)
- Archivos de instalación de Universal Agent 7.2 de Stonebranch Universal Controller 7.2
- AWS Mainframe Modernization plantilla de programación de tareas (última versión publicada del archivo .zip)

Limitaciones

- El producto y la solución se han probado y se ha validado su compatibilidad solo con OpenJDK 8 y 11.
- La plantilla aws-mainframe-modernization-stonebranchde programación de tareas de integración solo funcionará con el servicio de modernización de mainframe de AWS.
- Esta plantilla de programación de tareas solo funcionará en las ediciones para Unix, Linux o Windows de los agentes de Stonebranch.
- Algunos servicios de AWS no están disponibles en todas las regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS services by Region. Para ver los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

Arquitectura de estado objetivo

En el siguiente diagrama se muestra el entorno de AWS de ejemplo que se requiere para este piloto.

1. El Universal Automation Center (UAC) de Stonebranch incluye dos componentes principales: Universal Controller y Universal Agents. Stonebranch OMS se utiliza como un bus de mensajes entre el controlador y los agentes individuales.
2. Universal Controller utiliza la base de datos UAC de Stonebranch. La base de datos puede ser compatible con MySQL, Microsoft SQL Server, Oracle o Aurora MySQL.
3. Servicio de modernización de mainframe de AWS: entorno de ejecución de Micro Focus con la BankDemo aplicación implementada. Los archivos de la BankDemo aplicación se almacenarán en un bucket de S3. Este bucket también contiene los archivos JCL de la unidad central.
4. Stonebranch UAC puede ejecutar las siguientes funciones para la ejecución por lotes:

   a. Inicie un trabajo por lotes con el nombre del archivo JCL que existe en el bucket de S3 vinculado al servicio de AWS Mainframe Modernization.
   b. Obtenga el estado de la ejecución del trabajo por lotes.
   c. Espere hasta que se complete la ejecución del trabajo por lotes.
   d. Obtenga los registros de la ejecución del trabajo por lotes.
   e. Vuelva a ejecutar los trabajos por lotes fallidos.
   f. Cancele el trabajo por lotes mientras se está ejecutando.
5. Stonebranch UAC puede ejecutar las siguientes funciones para la aplicación:
   a. Iniciar la aplicación
   b. Obtener el estado de la aplicación
   c. Espere hasta que la aplicación se inicie o se detenga
   d. Detener la aplicación
   e. Obtener los registros del funcionamiento de la aplicación

Conversión de trabajos en Stonebranch

El siguiente diagrama representa el proceso de conversión de puestos de trabajo de Stonebranch durante el proceso de modernización. Describe cómo los cronogramas de trabajo y las definiciones de tareas se convierten a un formato compatible que puede ejecutar tareas por lotes de AWS Mainframe Modernization.

1. Para el proceso de conversión, las definiciones de los trabajos se exportan desde el sistema de mainframe existente.
2. Los archivos JCL se pueden cargar en el depósito S3 de la aplicación Mainframe Modernization para que el servicio AWS Mainframe Modernization pueda implementarlos.
3. La herramienta de conversión convierte las definiciones de trabajo exportadas en tareas de UAC.
4. Una vez creadas todas las definiciones de tareas y los cronogramas de trabajos, estos objetos se importarán al controlador universal. A continuación, las tareas convertidas ejecutan los procesos en el servicio de AWS Mainframe Modernization en lugar de ejecutarlos en el mainframe.

Arquitectura UAC de Stonebranch

El siguiente diagrama de arquitectura representa un active-active-passive modelo de controlador universal de alta disponibilidad (HA). El UAC de Stonebranch se implementa en varias zonas de disponibilidad para proporcionar una alta disponibilidad y respaldar la recuperación de desastres (DR).

Controlador universal

Se aprovisionan dos servidores Linux como controladores universales. Ambos se conectan al mismo punto de conexión de la base de datos. Cada servidor alberga una aplicación Universal Controller y un OMS. La versión más reciente de Universal Controller se utiliza en el momento del aprovisionamiento.

Los controladores universales se implementan en la aplicación web de Tomcat como el documento ROOT y se distribuyen en el puerto 80. Esta implementación facilita la configuración del equilibrador de carga de frontend.

El HTTP a través de TLS o HTTPS se habilita mediante el certificado comodín de Stonebranch (por ejemplo, `https://customer.stonebranch.cloud`). Esto asegura la comunicación entre el navegador y la aplicación.

OMS

Un agente universal y un OMS (servicio de mensajes de Opswise) residen en cada servidor de Universal Controller. Todos los agentes universales desplegados por el cliente están configurados para conectarse a ambos servicios de OMS. OMS actúa como un servicio de mensajería común entre los agentes universales y el controlador universal.

Amazon EFS monta un directorio de bobinas en cada servidor. OMS utiliza este directorio compartido para mantener la información de conexión y tareas de los controladores y los agentes. OMS funciona en un modo de alta disponibilidad. Si el OMS activo deja de funcionar, el OMS pasivo tiene acceso a todos los datos y reanuda las operaciones activas automáticamente. Los agentes universales detectan este cambio y se conectan automáticamente al nuevo OMS activo.

Base de datos

Amazon Relational Database Service (Amazon RDS) aloja la base de datos de UAC y su motor es compatible con Amazon Aurora MySQL. Amazon RDS ayuda a gestionar y ofrecer copias de seguridad programadas a intervalos regulares. Ambas instancias de Universal Controller se conectan al mismo punto de conexión de la base de datos.

Equilibrador de carga

Se configura un equilibrador de carga de aplicación para cada instancia. El equilibrador de carga dirige el tráfico al controlador activo en cualquier momento dado. Los nombres de dominio de su instancia apuntan a los puntos finales del equilibrador de carga respectivos.

URLs

Cada una de sus instancias tiene una URL, como se muestra en el siguiente ejemplo.

Entorno	Instancia
Producción	`customer.stonebranch.cloud`
Desarrollo (no producción)	`customerdev.stonebranch.cloud`
Pruebas (fuera de producción)	`customertest.stonebranch.cloud`

> **Note**
>
> Los nombres de las instancias que no son de producción se pueden configurar en función de sus necesidades.

Alta disponibilidad

La alta disponibilidad (HA) es la capacidad de un sistema de funcionar de forma continua y sin fallos durante un período de tiempo designado. Estos fallos incluyen, entre otros, el almacenamiento, las demoras en la respuesta de las comunicaciones del servidor causadas por problemas de la CPU o la memoria y la conectividad de red.

Para cumplir con los requisitos de alta disponibilidad:

- Todas las instancias, bases de datos y demás configuraciones de EC2 se reflejan en dos zonas de disponibilidad independientes dentro de la misma región de AWS.
- El controlador se aprovisiona a través de una imagen de máquina de Amazon (AMI) en dos servidores Linux en las dos zonas de disponibilidad. Por ejemplo, si está aprovisionado en la región de Europa eu-west-1, tiene un controlador universal en la zona de disponibilidad eu-west-1a y en la zona de disponibilidad eu-west-1c.

- No se permite que ningún trabajo se ejecute directamente en los servidores de aplicaciones ni que se almacene ningún dato en estos servidores.
- El equilibrador de carga de aplicación realiza comprobaciones de estado en cada controlador universal para identificar el controlador activo y dirigir el tráfico hacia él. En caso de que se produzcan problemas con un servidor, el equilibrador de carga pasa automáticamente al estado activo del controlador universal pasivo. A continuación, el equilibrador de cargas identifica la nueva instancia activa de Universal Controller a partir de las comprobaciones de estado y comienza a dirigir el tráfico. La conmutación por error se produce en un plazo de cuatro minutos sin pérdida de trabajo, y la URL de frontend sigue siendo la misma.
- El servicio de base de datos Aurora compatible con MySQL almacena los datos de Universal Controller. Para los entornos de producción, un clúster de base de datos se crea con dos instancias de base de datos en dos zonas de disponibilidad diferentes dentro de una sola región de AWS. Ambos controladores universales utilizan una interfaz de conectividad de bases de datos Java (JDBC) que apunta a un único punto de conexión del clúster de base de datos. En caso de que una instancia de base de datos tenga problemas, el punto de conexión del clúster de base de datos apunta dinámicamente a la instancia en buen estado. No se requiere intervención manual alguna.

Backup y purga

El controlador universal Stonebranch está configurado para realizar copias de seguridad y purgar los datos antiguos siguiendo el programa que se muestra en la tabla.

Tipo	Schedule
Actividad	7 días
Auditoría	90 días
Historial	60 días

Los datos de backup anteriores a las fechas mostradas se exportan al formato.xml y se almacenan en el sistema de archivos. Una vez finalizado el proceso de copia de seguridad, los datos más antiguos se purgan de la base de datos y se archivan en un depósito de S3 durante un máximo de un año en el caso de las instancias de producción.

Puede ajustar este programa en la interfaz de la controladora universal. Sin embargo, el aumento de estos plazos puede provocar un tiempo de inactividad más prolongado durante el mantenimiento.

Tools (Herramientas)

Servicios de AWS

- AWS Mainframe Modernization es un servicio que le ayuda a modernizar sus aplicaciones de unidad central para convertirlas en entornos de tiempo de ejecución administrados nativos en la nube de AWS. Ofrece herramientas y recursos para ayudarle a planificar e implementar la migración y modernización.
- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento de nivel de bloque para su uso con instancias de Amazon EC2.
- Amazon Elastic File System (Amazon EFS) le ayuda a crear y configurar sistemas de archivos compartidos en la nube de AWS.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS. Este patrón utiliza la edición de Amazon Aurora compatible con MySQL.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos. Así, por ejemplo, puede distribuir el tráfico entre instancias de Amazon EC2, contenedores y direcciones IP de una o varias zonas de disponibilidad. Este patrón utiliza un Equilibrador de carga de aplicación.

Stonebranch

- Universal Automation Center (UAC) es un sistema de productos de automatización de cargas de trabajo empresariales. Este patrón utiliza los siguientes componentes del UAC:
  - Universal Controller, una aplicación web Java que se ejecuta en un contenedor web de Tomcat, es la solución empresarial de programación de trabajos y agente de automatización de cargas de trabajo de Universal Automation Center. El controlador presenta una interfaz de usuario para crear, supervisar y configurar la información del controlador; gestiona la lógica de programación; procesa todos los mensajes con Universal Agents como origen y destino; y sincroniza gran parte del funcionamiento de alta disponibilidad de Universal Automation Center.

  - Universal Agent es un agente de programación independiente del proveedor que colabora con el programador de tareas existente en las principales plataformas informáticas, tanto antiguas como distribuidas. Se admiten todos los programadores que se ejecutan en z/Series, i/Series Unix, Linux o Windows.
- Universal Agent es un agente de programación independiente del proveedor que colabora con el programador de tareas existente en las principales plataformas informáticas, tanto antiguas como distribuidas. Se admiten todos los programadores que se ejecutan en Unixz/Series, i/Series, Linux o Windows.
- Integración con Stonebranch La extensión universal de aws-mainframe-modernization-stonebranch AWS Mainframe Modernization es la plantilla de integración para ejecutar, monitorear y volver a ejecutar trabajos por lotes en la plataforma AWS Mainframe Modernization.

Código

El código de este patrón está disponible en el repositorio -integration. aws-mainframe-modernization-stonebranch GitHub

Epics

Instalación de Universal Controller y Universal Agent en Amazon EC2

Tarea	Descripción	Habilidades requeridas
Descargue los archivos de instalación.	Descargue la instalación desde los servidores de Stonebranch. Para obtener los archivos de instalación, póngase en contacto con Stonebranch.	Arquitecto de la nube
Lanzar la instancia EC2.	Necesitará unos 3 GB de espacio adicional para las instalaciones de Universal Controller y Universal Agent. Por lo tanto, proporciona al menos 30 GB de espacio en disco para la instancia.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Agrega el puerto 8080 al grupo de seguridad para que sea accesible.	

Tarea	Descripción	Habilidades requeridas

Compruebe los requisitos previos.	Antes de la instalación, haga lo siguiente:
	1. Instale Java como se describe en Descarga del entorno de ejecución de Java.
	`$ sudo yum -y update`
	`$ sudo yum install java-11-amazon-corretto`
	Asegúrese de utilizar una de las versiones de JAVA compatibles. El comando anterior debería instalar java-11. Compruebe la versión de Java y asegúrese de que está utilizando la versión 11 antes de continuar.
	2. Como se describe en Installing Apache Tomcat, ejecute los siguientes comandos.
	`$ sudo yum install tomcat tomcat-admin-webapps`
	`$ sudo systemctl enable tomcat`
	`$ sudo systemctl start tomcat`
	3. Cree una base de datos de Amazon Aurora como
		Administrador de la nube, administrador de Linux

Tarea	Descripción	Habilidades requeridas
	se describe en Creación de un clúster de base de datos de Aurora MySQL y conexión a él. Edición de Amazon Aurora compatible con MySQL. Elija un nombre de usuario maestro y una contraseña maestra. Mantenga los valores predeterminados para el resto de los ajustes.	

Tarea	Descripción	Habilidades requeridas

Instale Universal Controller.	1. Cargue el archivo de instalación `universal-controller-7.2.0.0.tar` en la instancia EC2.
	2. Desarchive los archivos de instalación en una carpeta `temp`.
	`$ tar -xvf universal-controller-7.2.0.0.tar`
	3. Conceda permiso de ejecución al script de instalación.
	`$ chmod a+x install-controller.sh`
	4. Instale el controlador. En este ejemplo, se utiliza el siguiente comando para instalar Universal Controller en `/usr/share/tomcat`. Utilice el nombre de la base de datos de Amazon Aurora que creó en los pasos anteriores.
	`$ sudo ./install-controller.sh --tomcat-dir /usr/share/tomcat/ --controller-file universal-controller-7.2.0.0-build.145.war --`
		Arquitecto de la nube, administrador de Linux

Tarea	Descripción	Habilidades requeridas
	dbuser admin --dbpass "****" --dbname uc --rdbms mysql --dburl jdbc:mysql://database-2-instance-1.cih63miincgy.us-east-1.rds.amazonaws.com:3306/ La última línea de la salida del script debe ser “Instalación completa”. 5. Navegue hasta la siguiente URL en la instancia de EC2. http://<public_ip>:8080/uc 6. En la pantalla de inicio de sesión, introduzca ops.admin en la sección Nombre de usuario y deje vacío el campo Contraseña. 7. Establezca una contraseña para el usuario de `ops.admin` .	

Tarea	Descripción	Habilidades requeridas

Instale Universal Agent.	1. Cargue el archivo de instalación `sb-7.2.0.1-linux-3.10-x86_64.tar.Z` en la instancia EC2.
	2. Inicie sesión en la instancia EC2.
	3. Desarchive el paquete de instalación de Universal Agent.
	`$ zcat sb-7.2.0.1-linux-3.10-x86_64.tar.Z | tar xvf -`
	4. Ejecute el comando siguiente.
	`$ sudo ./unvinst --oms_servers 7878@localhost --oms_autostart yes --python yes`
	5. Cree un archivo PAM.
	`$ cp /etc/pam.d/login /etc/pam.d/ucmd`
	6. Habilite el inicio automático para Universal Agent.
	`$ /sbin/restorecon -v /etc/rc.d/init.d/ubrokerd`
		Administrador de la nube, administrador de Linux

Tarea	Descripción	Habilidades requeridas
Agregue OMS a Universal Controller.	1. Inicie sesión en Universal Controller con el usuario de `ops.admin` . 2. Elija el menú de Servicios en la esquina superior izquierda de la pantalla y, a continuación, elija el menú de Servidores OMS en el Sistema 3. En el campo Dirección del servidor OMS, escriba `localhost` y, a continuación, guarde. 4. Verá el estado del servidor OMS como Conectado y el Estado de la sesión como Operativo.	Administrador de Universal Controller

Importe la extensión universal de AWS Mainframe Modernization y cree una tarea

Tarea	Descripción	Habilidades requeridas
Plantilla de integración de importación.	Para este paso, necesita la extensión universal de AWS Mainframe Modernization. Asegúrese de descargar la última versión publicada del archivo .zip. 1. Inicie sesión en el Universal Controller con el `ops.admin` usuario.	Administrador de Universal Controller

Tarea	Descripción	Habilidades requeridas
	2. Vaya a Servicios, Importar la plantilla de integración. 3. Seleccione el archivo .zip de la plantilla de integración (`aws_mainframe_modernization_stonebranch_extension.zip`) y elija Importar. Una vez importada la plantilla de integración, verá las tareas de AWS Mainframe Modernization en la sección Servicios disponibles.	

Tarea	Descripción	Habilidades requeridas
Habilite las credenciales que se pueden resolver.	1. Navegue hasta Servicios, Tareas de AWS Mainframe Modernization. 2. En el panel derecho, rellene los campos obligatorios: • Nombre: nueva tarea de modernización de la unidad central • Agente: seleccione el único agente (AGNT0001). En los detalles de la AWS Mainframe Modernization: • Acción: enumerar los entornos • Credenciales de AWS: si se le ha agregado un rol de AWS Identity and Access Management IAM a la instancia EC2, puede dejar este campo en blanco. Si va a utilizar `AWSAccessKeyID` y`AWSSecretKey` , seleccione el icono () situado junto al campo. En la ventana de Detalles de la credencial que se abre, introduzca la siguiente información y, a continuac ión, guárdela.	Administrador de Universal Controller

Tarea	Descripción	Habilidades requeridas
	• Nombre: credenciales de AWS Mainframe Modernization • Usuario en tiempo de ejecución: escriba el ID de la clave de acceso de AWS en este campo. • Contraseña de tiempo de ejecución: escriba la clave secreta de AWS en este campo. • Punto de conexión: asegúrese de que el punto de conexión tenga la región de AWS correcta. El valor predeterminado es `https://m2.us-east-1.amazonaws.com` . • Región: introduzca la región del servicio de AWS Mainframe Modernization. El valor predeterminado es `us-east-1` . 3. Mantenga los valores predeterminados en el resto de los campos y guarde la tarea.	

Tarea	Descripción	Habilidades requeridas
Iniciar la tarea.	1. En la parte superior del panel derecho, seleccione Iniciar tarea. 2. En la ventana de Confirmación, seleccione Lanzar. Después de eso, la consola universal Controller mostrará un mensaje similar al siguiente. 2022-08-24 10:11:49 AM Se lanzó correctamente la tarea universal «Nueva tarea de modernización del mainframe» con la instancia de tarea sys_id NC8 1661291493634146313 E38 OZJY. DB8 3. Navegue hasta las Instancias. Si no ve la pestaña Instancias, utilice la flecha derecha para desplazarse hacia la derecha. 4. Abra el menú contextual (haga clic con el botón derecho) de la instancia de la tarea de la lista, seleccione Recuperar salida y, a continuación, Enviar en la opción de Recuperar salida	Administrador de Universal Controller

Tarea	Descripción	Habilidades requeridas
	5. En la ventana Recuperar resultados, verá la lista de entornos de STDOUT.	

Probar el inicio de un trabajo por lotes

Tarea	Descripción	Habilidades requeridas
Crear una tarea para el trabajo por lotes.	1. Navegue hasta Servicios, Tareas de AWS Mainframe Modernization. 2. En el panel derecho, rellene los campos obligatorios: • Nombre: nueva tarea de modernización de la unidad central • AgenteAGNT0001: seleccione el único agente (). En los detalles de la AWS Mainframe Modernization: • Acción: iniciar el lote (o iniciar el lote y esperar a que se ejecute el trabajo por lotes y esperar a que la tarea se complete en AWS) • Credenciales de AWS: si ha agregado un rol de IAM a la instancia EC2, puede dejar este campo vacío. Si va a utilizar `AWSAccess`	Administrador de Universal Controller

Tarea	Descripción	Habilidades requeridas
	`KeyID` `yAWSSecret Key` , seleccione el icono () situado junto al campo. • Punto de conexión: asegúrese de que el punto de conexión tenga la región de AWS correcta. El valor predeterminado es https://m2.us-east-1.amazonaws.com. • Región: introduzca la región del servicio de AWS Mainframe Modernization. El valor predeterminado es `us-east-1` . • Solicitud: seleccione el icono situado junto al campo () y luego, Enviar en las opciones de actualización de la solicitud . Esto se conectará al servicio de AWS Mainframe Modernization y devolverá la lista de aplicaciones. Ahora puede seleccionar la aplicación de la lista desplegable. Seleccione la aplicación en la que desea ejecutar el trabajo por lotes.	

Tarea	Descripción	Habilidades requeridas
	• Nombre del archivo JCL: `RUNHELLO.jcl` • Espere a que se complete correctamente o reciba un error: si se selecciona esta opción, la tarea esperará hasta que el estado del trabajo por lotes sea exitoso o fallido. • Intervalo de sondeo: es el tiempo que transcurre entre cada sondeo. • Obtener registros de ejecución: si se seleccion a, los registros se recuperarán automátic amente cuando se complete el trabajo por lotes. • Formato de registro: este es el formato de los registros que se van a imprimir. Puede ser en formato texto o JSON. 3. Mantenga los valores predeterminados en el resto de los campos y guarde la tarea.	

Tarea	Descripción	Habilidades requeridas
Iniciar la tarea.	1. En la parte superior del panel derecho, seleccione Iniciar tarea. 2. En la ventana de Confirmación, seleccione Lanzar. Después de eso, la consola universal Controller mostrará un mensaje similar al siguiente. 2022-08-24 11:11:59 AM Se lanzó correctamente la tarea de Universal “Mainframe Modernization Start Batch” con la instancia de tarea sys_id <sys id>. 3. Navegue hasta las Instancias. Si no ve la pestaña Instancias, utilice la flecha derecha para desplazarse hacia la derecha. 4. Abra el menú contextual (haga clic con el botón derecho) de la instancia de la tarea de la lista, seleccione Recuperar salida y, a continuación, Enviar en la opción de Recuperar salida 5. En la ventana Recuperar resultados, verá la lista de entornos de STDOUT.	Administrador de Universal Controller

Cree un flujo de trabajo para múltiples tareas

Tarea	Descripción	Habilidades requeridas
Copie las tareas.	1. Abra el menú contextual (haga clic con el botón derecho) de la tarea de la que quiera crear copias y elija Copiar. 2. En la ventana Copy AWS Mainframe Modernization Task, introduzca el siguiente nombre nuevo para la nueva tarea: Mainframe Modernization Start Batch -. RUNAWS2 3. Vuelva a copiar la tarea con el siguiente nombre: Mainframe Modernization Start Batch -RUNAWS3. 4. Vuelva a copiar la tarea con el siguiente nombre: Mainframe Modernization Start Batch -RUNAWS4. 5. Copie la tarea por última vez con el siguiente nombre: Mainframe Modernization Start Batch - FOOBAR.	Administrador de Universal Controller
Tarea de actualizar.	1. Abra (haga doble clic) la RUNAWS2 tarea Start Batch: de Mainframe Modernization, cambie el campo Nombre de archivo	Administrador de Universal Controller

Tarea	Descripción	Habilidades requeridas
	JCL a y `RUNAWS2.jcl` guárdela. 2. Abra (haga doble clic) la RUNAWS3 tarea Start Batch: de Mainframe Modernization, cambie el campo Nombre de archivo JCL a y `RUNAWS3.jcl` guárdela. 3. Abra (haga doble clic) la RUNAWS4 tarea Start Batch: de Mainframe Modernization, cambie el campo Nombre de archivo JCL a y `RUNAWS4.jcl` guárdela. 4. Abra (haga doble clic) la tarea Start Batch - FOOBAR de Mainframe Modernization, cambie el campo Nombre de archivo JCL a `MISSING.jcl` , y guárdela. Esta tarea fallará porque el valor del nombre de archivo JCL es incorrecto.	

Tarea	Descripción	Habilidades requeridas
Cree un flujo de trabajo.	1. Navegue hasta Servicios, Flujos de trabajo. 2. En el panel derecho, introduzca Mainframe Modernization Workflow en el campo Nombre y guarde. 3. En el panel de la derecha, seleccione Editar flujo de trabajo. 4. En la Pestaña del editor de flujos de trabajo, el botón Añadir tarea (+). 5. En la ventana de Búsqueda de tareas, seleccione Buscar para ver todas las tareas de Universal Controller. 6. Haga clic en el icono situado junto a Mainframe Modernization Start Batch Task y arrastre el icono a un lugar vacío del Editor de flujos de trabajo. 7. Repita la misma acción para las demás tareas de modernización de la unidad central y colóquelas como se muestra en la sección de Información adicional. 8. Pulse el botón Conectar () y conecte las tareas entre sí. Para conectar una tarea con otra, haga clic en el	Administrador de Universal Controller

Tarea	Descripción	Habilidades requeridas
	centro de la tarea y arrástrel a hasta la tarea de destino. 9. Conecta las tareas como se muestra en la sección Información adicional y guarda el flujo de trabajo. 10. Haga clic con el botón derecho en un lugar vacío del editor de flujos de trabajo, seleccione Iniciar flujo de trabajo y, a continuación, Aceptar.	

Tarea	Descripción	Habilidades requeridas
Compruebe el estado del flujo de trabajo.	1. En el menú de la izquierda, seleccione la Actividad 2. En el centro de la ventana, seleccione Iniciar. Verá la lista de instancias de tareas en la lista. 3. Abra el flujo de trabajo de modernización de mainframe (haga doble clic en él) en la lista o abra el menú contextual (haga clic con el botón derecho) y seleccione Comandos de tareas del flujo de trabajo y Ver flujo de trabajo. Verá las tareas tal y como se muestra en la sección de información adicional. Se esperaba que la segunda tarea fallara porque utilizast e un archivo JCL que faltaba.	Administrador de universal Controller

Solucione los problemas de los trabajos por lotes fallidos y vuelva a ejecutarlos

Tarea	Descripción	Habilidades requeridas
Corrija la tarea fallida y vuelva a ejecutarla.	1. Abra (haga doble clic en) la tarea fallida para ver el error de la tarea. 2. Tiene dos opciones al corregir la tarea fallida.	Administrador de Universal Controller

Tarea	Descripción	Habilidades requeridas
	• Corrija el nombre del archivo JCL y configúrelo en `F00BAR.jcl` . • Añada el nombre de archivo JCL correcto al nombre de archivo JCL (Temp). Este campo sobrescribirá el campo Nombre del archivo JCL. Para este piloto, seleccione la segunda opción y guarde la instancia de la tarea. 3. En el Supervisor de flujo de trabajo, abra el menú contextual (haga clic con el botón derecho) de la tarea fallida y seleccion e Comandos y Volver a ejecutar. 4. Después de eso, todas las tareas se completarán correctamente.	

Cree las tareas de inicio y detención de la aplicación

Tarea	Descripción	Habilidades requeridas
Cree la acción Iniciar aplicació n.	1. Navegue hasta Servicios, Tareas de AWS Mainframe Modernization. 2. En el panel derecho, rellene los campos obligatorios.	Administrador de Universal Controller

Tarea	Descripción	Habilidades requeridas
	• Nombre: aplicación de inicio de modernización de mainframe • Agente: seleccione el único agente () AGNT0001 En los detalles de la AWS Mainframe Modernization: • Acción: iniciar la aplicación • Credenciales de AWS: si ha agregado un rol de IAM a la instancia EC2, puede dejar este campo vacío. Si va a utilizar `AWSAccessKeyID` y `AWSSecretKey` , seleccione la credencial que creó anteriormente. • Punto de conexión: asegúrese de que el punto de conexión tenga la región correcta. El valor predeterminado es `https://m2.us-east-1.amazonaws.com` . • Región: introduzca la región del servicio de AWS Mainframe Modernization. El valor predeterminado es `us-east-1` .	

Tarea	Descripción	Habilidades requeridas
	• Solicitud: seleccione el icono situado junto al campo () y luego, Enviar en las opciones de actualización de la solicitud. Esto se conectará al servicio de AWS Mainframe Modernization y devolverá la lista de aplicaciones. Ahora puede seleccionar la aplicación de la lista desplegable. Seleccione la aplicación en la que desea ejecutar el trabajo por lotes. • Espere a que se complete correctamente o reciba un error: si se selecciona esta opción, la tarea esperará hasta que el estado del trabajo por lotes sea exitoso o fallido. • Intervalo de sondeo: es el tiempo que transcurre entre cada sondeo. • Obtener registros de ejecución: si se selecciona, los registros se recuperarán automáticamente cuando se complete el trabajo por lotes.	

Tarea	Descripción	Habilidades requeridas
	• Formato de registro: este es el formato de los registros que se van a imprimir. Puede ser en formato texto o JSON. 3. Mantenga los valores predeterminados en el resto de los campos y guarde la tarea. 4. Ahora copie esta tarea y cree una tarea para Stop Application. Cambie el nombre a Mainframe Moderinization Stop Application y cambie la acción a Detener aplicació n.	

Crear una tarea de cancelación de ejecución por lotes

Tarea	Descripción	Habilidades requeridas
Cree la acción Cancelar Batch.	1. Navegue hasta Servicios, Tareas de AWS Mainframe Modernization. 2. En el panel derecho, rellene los campos obligatorios. • Nombre: Mainframe Modernization Cancel Batch Execution • Agente: seleccione el único agente (AGNT0001)	

Tarea	Descripción	Habilidades requeridas
	En los detalles de la AWS Mainframe Modernization: • Acción: cancelar la ejecución por lotes • Credenciales de AWS: si ha agregado un rol de IAM a la instancia EC2, puede dejar este campo vacío. Si va a utilizar `AWSAccessKeyID` y `AWSSecretKey` , seleccione la credencial que creó anteriormente. • Punto de conexión: asegúrese de que el punto de conexión tenga la región correcta. El valor predeterminado es `https://m2.us-east-1.amazonaws.com` . • Región: introduzca la región del servicio de AWS Mainframe Modernization. El valor predeterminado es `us-east-1` . • Solicitud: seleccione el icono situado junto al campo () y luego, Enviar en las opciones de actualización de la solicitud . Esto se conectará	

Tarea	Descripción	Habilidades requeridas
	al servicio de AWS Mainframe Moderniza tion y devolverá la lista de aplicaciones. Ahora puede seleccionar la aplicación de la lista desplegable. Seleccion e la aplicación en la que desea ejecutar el trabajo por lotes. • Espere a que se complete correctamente o reciba un error: si se selecciona esta opción, la tarea esperará hasta que el estado del trabajo por lotes sea exitoso o fallido. • Intervalo de sondeo: es el tiempo que transcurre entre cada sondeo. • Obtener registros de ejecución: si se seleccion a, los registros se recuperarán automátic amente cuando se complete el trabajo por lotes. • Formato de registro: este es el formato de los registros que se van a imprimir. Puede ser en formato texto o JSON. 3. Mantenga los valores predeterminados en el resto	

Tarea	Descripción	Habilidades requeridas
	de los campos y guarde la tarea.	

Recursos relacionados

- Controlador universal
- Agente universal
- Configuración de LDAP
- SAML Single Sign-On
- Herramienta de conversión Xpress

Información adicional

Iconos en el editor de flujos de trabajo

Todas las tareas están conectadas

Estado del flujo de trabajo

Migración y réplica de archivos VSAM a Amazon RDS o Amazon MSK mediante Connect de Precisely

Prachi Khanna y Boopathy Gopalsamy, Amazon Web Services

Resumen

Este patrón le muestra cómo migrar y replicar archivos del Método de Acceso a Almacenamiento Virtual (VSAM) de un mainframe a un entorno de destino en la nube de AWS mediante Connect de Precisely. Los entornos de destino indicados en este patrón incluyen Amazon Relational Database Service (Amazon RDS) y Amazon Managed Streaming para Apache Kafka (Amazon MSK). Connect emplea registro de datos de cambios (CDC) para supervisar continuamente las actualizaciones de sus archivos VSAM de origen y, a continuación, transferir estas actualizaciones a uno o más de sus entornos de destino de AWS. Puede usar este patrón para lograr sus objetivos de modernización de aplicaciones o análisis de datos. Por ejemplo, puede usar Connect para migrar los archivos de aplicaciones de VSAM a la nube de AWS con baja latencia, o migrar sus datos de VSAM a un almacenamiento de datos o lago de datos de AWS para realizar análisis que puedan tolerar latencias de sincronización superiores a las requeridas para la modernización de las aplicaciones.

Requisitos previos y limitaciones

Requisitos previos

- IBM z/OS V2R1 o posterior
- CICS Transaction Server para z/OS (CICS TS) V5.1 o posterior (captura de datos CICS/VSAM)
- IBM MQ 8.0 o posterior
- Cumplimiento de los requisitos de seguridad de z/OS (por ejemplo, la autorización de la APF para cargar bibliotecas) SQData
- Registros de recuperación de VSAM activados
- (Opcional) Versión de recuperación de CICS VSAM (CICS VR) para capturar automáticamente los registros de CDC
- Una cuenta de AWS activa
- Una nube privada virtual (VPC) de Amazon con una subred a la que pueda acceder la plataforma antigua
- Una licencia de VSAM Connect de Precisely

Limitaciones

- Connect no admite la creación automática de tablas de destino basadas en cuadernos o esquemas VSAM de origen. Debe definir la estructura de la tabla de destino por primera vez.
- En el caso de destinos que no son de transmisión, como Amazon RDS, debe especificar el mapeo entre el origen de la conversión y el destino en el script de configuración de Apply Engine.
- Las funciones de registro, monitoreo y alerta se implementan a través de componentes externos (como Amazon CloudWatch) APIs y requieren que estén completamente operativas.

Versiones de producto

- SQData 40134 para z/OS
- SQData 4.0.43 para la Amazon Machine Image (AMI) de Amazon Linux en Amazon Elastic Compute Cloud (Amazon) EC2

Arquitectura

Pila de tecnología de origen

- Lenguaje de control de tareas (JCL)
- Shell z/OS Unix e Instalación de Sistema Interactivo de Productividad (ISPF)
- Utilidades VSAM (IDCAMS)

Pila de tecnología de destino

- Amazon EC2
- Amazon MSK
- Amazon RDS
- Amazon VPC

Arquitectura de destino

Migración de archivos VSAM a Amazon RDS

El siguiente diagrama muestra cómo migrar archivos VSAM a una base de datos relacional, como Amazon RDS, en tiempo real o casi en tiempo real mediante el CDC agent/publisher en el entorno de origen (mainframe local) y el Apply Engine en el entorno de destino (nube de AWS).

El diagrama muestra el siguiente flujo de trabajo por lotes:

1. Connect registra los cambios en un archivo comparando los archivos VSAM de los archivos de copia de seguridad para identificar los cambios y, a continuación, los envía al flujo de registro.
2. El publicador consume los datos del flujo de registro del sistema.
3. El publicador comunica los cambios registrados en los datos a un motor de destino a través de TCP/IP. El controlador Daemon autentica la comunicación entre los entornos de origen y destino.
4. El Apply Engine del entorno de destino recibe los cambios del agente publicador y los aplica a una base de datos relacional o no relacional.

En el diagrama, se muestra el siguiente flujo on line:

1. Connect registra los cambios en el archivo online mediante una réplica de registro y, a continuación, transmite los cambios registrados a un flujo de registro.
2. El publicador consume los datos del flujo de registro del sistema.
3. El publicador comunica los cambios en los datos registrados al motor de destino a través de TCP/IP. El controlador Daemon autentica la comunicación entre los entornos de origen y destino.
4. El motor de implementación del entorno de destino recibe los cambios del agente publicador y los aplica a una base de datos relacional o no relacional.

Migración de archivos VSAM a Amazon MSK

El siguiente diagrama muestra cómo transmitir estructuras de datos de VSAM desde un mainframe a Amazon MSK en modo de alto rendimiento, y cómo generar automáticamente conversiones de esquemas JSON o AVRO que se integran con Amazon MSK.

El diagrama muestra el siguiente flujo de trabajo por lotes:

1. Connect registra los cambios en un archivo mediante CICS VR o comparando los archivos VSAM de los archivos de copia de seguridad para identificar los cambios. Los cambios registrados se envían al flujo de registro.

2. El publicador consume los datos del flujo de registro del sistema.
3. El publicador comunica los cambios en los datos registrados al motor de destino a través de TCP/IP. El controlador Daemon autentica la comunicación entre los entornos de origen y destino.
4. El motor replicador, que funciona en modo de procesamiento paralelo, divide los datos en una unidad de caché de trabajo.
5. Los subprocesos de trabajo registran los datos de la caché.
6. Los datos se publican en los temas de Amazon MSK desde los hilos de trabajo.
7. Los usuarios aplican los cambios de Amazon MSK a destinos como Amazon DynamoDB, Amazon Simple Storage Service (Amazon S3) OpenSearch o Amazon Service mediante conectores.

En el diagrama, se muestra el siguiente flujo on line:

1. Los cambios en el archivo online se registran mediante una réplica de registro. Los cambios registrados se envían al flujo de registro.
2. El publicador consume los datos del flujo de registro del sistema.
3. El publicador comunica los cambios en los datos registrados al motor de destino a través de TCP/IP. El controlador Daemon autentica la comunicación entre los entornos de origen y destino.
4. El motor replicador, que funciona en modo de procesamiento paralelo, divide los datos en una unidad de caché de trabajo.
5. Los subprocesos de trabajo registran los datos de la caché.
6. Los datos se publican en los temas de Amazon MSK desde los hilos de trabajo.
7. Los usuarios aplican los cambios de Amazon MSK a destinos como DynamoDB, Amazon S3 o Service mediante OpenSearch conectores.

Tools (Herramientas)

- Amazon Managed Streaming para Apache Kafka (Amazon MSK) es un servicio completamente administrado que le permite crear y ejecutar aplicaciones que utilizan Apache Kafka para procesar datos de streaming.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.

Epics

Prepare el entorno de origen (mainframe)

Tarea	Descripción	Habilidades requeridas
Instale Connect CDC 4.1.	1. Póngase en contacto con el equipo de soporte de Precisely para obtener una licencia y paquetes de instalación. 2. Utilice el ejemplo JCLs para instalar Connect CDC 4.1. Para obtener instrucciones, consulte Instalar Connect CDC (SQData) con JCL en la documentación de Precily. 3. Ejecute el comando `SETPROG APF` para autorizar las bibliotec as de carga de Connect SQDATA.V4nnn.LOADLIB.	Desarrollador/administrador de IBM Mainframe
Configure el directorio zFS.	Para configurar un directori o zFS, siga las instrucciones de Directorios de variables zFS en la documentación de Precisely. **Note** Las configuraciones de Controller Daemon y Capture/Publisher agente se almacenan en el sistema de	Desarrollador/administrador de IBM Mainframe

Tarea	Descripción	Habilidades requeridas
	archivos de z/OS UNIX Systems Services (denomina do ZfS). Los agentes de controlador Daemon, registrad or, almacenamiento y publicador requieren una estructura de directorios zFS predefinida para almacenar un número reducido de archivos.	
Configure los puertos. TCP/IP	Para configurar TCP/IP los puertos, siga las instrucciones de los puertos TCP/IP de la documentación de Precily. **Note** El controlador Daemon requiere TCP/IP puertos en los sistemas de origen. Los puertos son referenciados por los motores en los sistemas de destino (donde se procesan los datos de cambios registrados).	Desarrollador/administrador de IBM Mainframe

Tarea	Descripción	Habilidades requeridas
Cree un flujo de z/OS registro.	Para crear un flujo de registro de z/OS, siga las instrucciones de Create z/OS system LogStreams en la documentación de Precily. **Note** Connect utiliza el flujo de registro para registrar y transmitir datos entre el entorno de origen y el entorno de destino durante la migración. Para ver un ejemplo de JCL que crea un z/OS LogStream, consulte Crear flujos de registro z/OS del sistema en la documentación de Precily.	Desarrollador de Mainframe de IBM
Identifique y autorice a IDs los usuarios de ZfS y a las tareas iniciadas.	Use RACF para conceder acceso al sistema de archivos OMVS zFS. Para ver un ejemplo de JCL, consulte Identificar y autorizar el usuario de ZfS y la tarea iniciada IDs en la documentación de Precily.	Desarrollador/administrador de IBM Mainframe

Tarea	Descripción	Habilidades requeridas
Genere las claves z/OS públicas/privadas y el archivo de claves autorizado.	Ejecute JCL para generar el par de claves. Para ver un ejemplo, consulte Ejemplo de par de claves en la sección de Información adicional de este patrón. Para obtener instrucciones, consulte Generar claves z/OS públicas y privadas y un archivo de claves autorizadas en la documentación de Precily.	Desarrollador/administrador de IBM Mainframe

Active el registro replicado de CICS VSAM y adjúntelo al flujo de registro.	Ejecute el siguiente script de JCL.
	
	``
	 //STEP1 EXEC PGM=IDCAMS
	 //SYSPRINT DD SYSOUT=*
	 //SYSIN DD *
	   ALTER SQDATA.CICS.FILEA -
	   LOGSTREAMID(SQDATA.VSAMCDC.LOG1) -
	   LOGREPLICATE
	``
		Desarrollador/administrador de IBM Mainframe

Tarea	Descripción	Habilidades requeridas
Active el registro de recuperación de archivos de VSAM mediante FCT.	Modifique la tabla de control de archivos (FCT) para que refleje los siguientes cambios en los parámetros: `Configure FCT Parms CEDA ALT FILE(name) GROUP(groupname) DSNAME(data set name) RECOVERY(NONE|BACKOUTONLY|ALL) FWDRECOVLOG(NO|1-99) BACKUPTYPE(STATIC|DYNAMIC) RECOVERY PARAMETERS RECOVery : None | Backoutonly | All Fwdrecovlog : No | 1-99 BAckuptype : Static | Dynamic`	Desarrollador/administrador de IBM Mainframe
Configure el CDCz registro para el agente publicador.	1. Cree el archivo CAB de CDCz Log Publisher. 2. Cifre los datos publicados. 3. Prepare el JCL de tiempo de ejecución de CDCz Log Publisher.	Desarrollador/administrador de IBM Mainframe

Tarea	Descripción	Habilidades requeridas
Active el controlador Daemon.	1. Abra el panel de ISPF y ejecute el siguiente comando para abrir el menú de Precisely: `EXEC 'SQDATA.V4nnnnn.ISPFLIB(SQDC$STA)' 'SQDATA.V4nnnnn'` 2. Para configurar el controlador Daemon, seleccione la opción 2 del menú.	Desarrollador/administrador de IBM Mainframe
Active el publicador.	1. Abra el panel de ISPF y ejecute el siguiente comando para abrir el menú de Precisely: `EXEC 'SQDATA.V4nnnnn.ISPFLIB(SQDC$STA)' 'SQDATA.V4nnnnn'` 2. Para configurar el publicador, seleccione la opción 3 del menú e I para insertar.	Desarrollador/administrador de IBM Mainframe

Tarea	Descripción	Habilidades requeridas
Active el flujo de registro.	1. Abra el panel de ISPF y ejecute el siguiente comando para abrir el menú de Precisely: `EXEC 'SQDATA.V4nnnnn.ISPFLIB(SQDC$STA)' 'SQDATA.V4nnnnn'` 2. Para configurar el flujo de registro, elija la opción 4 del menú e I para insertar. A continuación, introduzca el nombre del flujo de registro creado en los pasos anteriores.	Desarrollador/administrador de IBM Mainframe

Prepare el entorno de destino (AWS)

Tarea	Descripción	Habilidades requeridas
Instale Precily en una EC2 instancia.	Para instalar Connect from Precisely en la AMI de Amazon Linux para Amazon EC2, siga las instrucciones de Instalar Connect CDC (SQData) en UNIX en la documentación de Precily.	AWS general
Abra los TCP/IP puertos.	Para modificar el grupo de seguridad e incluir los puertos del controlador Daemon para el acceso entrante y saliente, siga las instrucciones de TCP/IP en la documentación de Precisely.	AWS general

Tarea	Descripción	Habilidades requeridas
Cree directorios de archivos.	Para crear directorios de archivos, siga las instrucciones de Preparación del entorno de aplicación de destino en la documentación de Precisely.	AWS general

Cree el archivo de configuración de Apply Engine.	Cree el archivo de configuración de Apply Engine en el directorio de trabajo de Apply Engine. El siguiente ejemplo de archivo de configuración muestra Apache Kafka como destino:
	`builtin.features=SASL_SCRAM`
	`security.protocol=SASL_SSL`
	`sasl.mechanism=SCRAM-SHA-512`
	`sasl.username=`
	`sasl.password=`
	`metadata.broker.list=`
	Note
	Para obtener más información, consulte Security en la documentación de Apache Kafka.
		AWS general

Tarea	Descripción	Habilidades requeridas
Cree scripts para el procesamiento de Apply Engine.	Cree scripts para que Apply Engine procese los datos de origen y los replique en el destino. Para obtener más información, consulte Crear un script de Apply Engine en la documentación de Precisely.	AWS general
Ejecute los scripts.	Para iniciar el script, ejecute los comandos `SQDPARSE` y `SQDENG`. Para obtener más información, consulte Analizar un script para zOS en la documentación de Precisely.	AWS general

Validar el entorno

Tarea	Descripción	Habilidades requeridas
Valide la lista de archivos VSAM y las tablas de destino para su procesamiento en CDC.	1. Valide los archivos VSAM, incluidos los registros de replicación, los registros de recuperación, los parámetros de FCT y el flujo de registro. 2. Valide las tablas de la base de datos de destino, indicando si las tablas se han creado según la según la definición de esquema requerida, el acceso a las tablas y otros criterios.	AWS general, Mainframe

Tarea	Descripción	Habilidades requeridas
Compruebe que el SQData producto Connect CDC esté vinculado.	Ejecute un trabajo de prueba y compruebe que el código de retorno de este trabajo es 0 (correcto). **Note** Los mensajes de estado de Connect CDC SQData Apply Engine deben mostrar mensajes de conexión activa.	AWS general, Mainframe

Ejecute y valide casos de prueba (lote)

Tarea	Descripción	Habilidades requeridas
Ejecute el trabajo por lotes en el mainframe.	Ejecute el trabajo de aplicación por lotes con un JCL modificado. Incluya pasos en el JCL modificado para hacer lo siguiente: 1. Realizar una copia de seguridad de los archivos de datos. 2. Comparar el archivo de copia de seguridad con los archivos de datos modificados, generar el archivo delta y, a continuación, anotar el recuento de registros de delta de los mensajes.	AWS general, Mainframe

Tarea	Descripción	Habilidades requeridas
	3. Inserte el archivo delta en el z/OS flujo de registro. 4. Ejecutar JCL. Para ver un JCL de ejemplo, consulte Preparación del JCL de comparación y captura de archivos en la documenta ción de Precisely.	
Comprobar el flujo de registros .	Compruebe el flujo de registro para confirmar que puede ver los datos de cambios del trabajo por lotes completado en el mainframe.	AWS general, Mainframe
Valide los recuentos de la tabla de cambios delta de origen y de destino.	Para confirmar que se han contabilizado los registros, haga lo siguiente: 1. Recopile el recuento delta de origen a partir de los mensajes de lotes de JCL. 2. Supervise Apply Engine para ver los recuentos a nivel de registro del número de registros insertados, actualizados o eliminados en el archivo VSAM. 3. Consulte los recuentos de registros en la tabla de destino. 4. Compare y contabilice los distintos recuentos de registros.	AWS general, Mainframe

Ejecute y valide casos de prueba (On line)

Tarea	Descripción	Habilidades requeridas
Ejecute la transacción online en una región CICS.	1. Ejecute la transacción online para validar el caso de prueba. 2. Valide el código de ejecución de la transacción (RC=0: correcta).	Desarrollador de Mainframe de IBM
Comprobar el flujo de registros .	Confirme que el flujo de registro incluye los cambios específicos a nivel de registro.	Desarrollador de AWS Mainframe
Valide el recuento en la base de datos de destino.	Supervise Apply Engine para comprobar el recuento a nivel de registro.	Precisely, Linux
Valide los recuentos de registros y los registros de datos en la base de datos de destino.	Consulte la base de datos de destino para validar los recuentos de registros y los registros de datos.	AWS general

Recursos relacionados

- VSAM z/OS (documentación de Precisely)
- Apply engine (documentación de Precisely)
- Motor de replicador (documentación de Precisely)
- Flujo de registro (documentación de IBM)

Información adicional

Archivo de configuración de ejemplo

Este es un archivo de configuración de ejemplo para un flujo de registro en el que el entorno de origen es un mainframe y el entorno de destino es Amazon MSK:

```
 -- JOBNAME -- PASS THE SUBSCRIBER NAME
 -- REPORT  progress report will be produced after "n" (number) of Source records
processed.

 JOBNAME VSMTOKFK;
 --REPORT EVERY 100;
 -- Change Op has been ‘I’ for insert, ‘D’ for delete , and ‘R’ for Replace. For RDS
it is 'U' for update
 -- Character Encoding on z/OS is Code Page 1047, on Linux and UNIX it is Code Page
819 and on Windows, Code Page 1252
 OPTIONS
 CDCOP('I', 'U', 'D'),
 PSEUDO NULL = NO,
 USE AVRO COMPATIBLE NAMES,
 APPLICATION ENCODING SCHEME = 1208;

 --       SOURCE DESCRIPTIONS

 BEGIN GROUP VSAM_SRC;
 DESCRIPTION COBOL ../copybk/ACCOUNT AS account_file;
 END GROUP;

 --       TARGET DESCRIPTIONS

 BEGIN GROUP VSAM_TGT;
 DESCRIPTION COBOL ../copybk/ACCOUNT AS account_file;
 END GROUP;

 --       SOURCE DATASTORE (IP & Publisher name)

 DATASTORE cdc://10.81.148.4:2626/vsmcdct/VSMTOKFK
 OF VSAMCDC
 AS CDCIN
 DESCRIBED BY GROUP VSAM_SRC ACCEPT ALL;

 --       TARGET DATASTORE(s) - Kafka and topic name

 DATASTORE 'kafka:///MSKTutorialTopic/key'
 OF JSON
 AS CDCOUT
 DESCRIBED BY GROUP VSAM_TGT FOR INSERT;
```

```
  --       MAIN SECTION

  PROCESS INTO
  CDCOUT
  SELECT
  {
  SETURL(CDCOUT, 'kafka:///MSKTutorialTopic/key')
  REMAP(CDCIN, account_file, GET_RAW_RECORD(CDCIN, AFTER), GET_RAW_RECORD(CDCIN,
 BEFORE))
  REPLICATE(CDCOUT, account_file)
  }
  FROM CDCIN;
```

Ejemplo de par de claves

Este es un ejemplo de cómo ejecutar JCL para generar el par de claves:

```
//SQDUTIL EXEC PGM=SQDUTIL //SQDPUBL DD DSN=&USER..NACL.PUBLIC, //
 DCB=(RECFM=FB,LRECL=80,BLKSIZE=21200), // DISP=(,CATLG,DELETE),UNIT=SYSDA, //
 SPACE=(TRK,(1,1)) //SQDPKEY DD DSN=&USER..NACL.PRIVATE, //
 DCB=(RECFM=FB,LRECL=80,BLKSIZE=21200), // DISP=(,CATLG,DELETE),UNIT=SYSDA, //
 SPACE=(TRK,(1,1)) //SQDPARMS DD  keygen //SYSPRINT DD SYSOUT= //SYSOUT DD SYSOUT=* //
SQDLOG DD SYSOUT=* //*SQDLOG8 DD DUMMY
```

Modernice la aplicación de CardDemo mainframe mediante AWS Transform

Santosh Kumar Singh y Cheryl du Preez, Amazon Web Services

Resumen

AWS Transform se diseñó para acelerar la modernización de las aplicaciones de mainframe. Utiliza IA generativa para agilizar el proceso de modernización del mainframe. Automatiza tareas complejas, como el análisis de código heredado, la documentación del mainframe, la extracción de reglas empresariales, la descomposición de aplicaciones monolíticas en el dominio empresarial y la refactorización del código. Acelera los proyectos de modernización al automatizar tareas complejas, como el análisis de aplicaciones y la planificación de las secuencias de migración. Al descomponer las aplicaciones monolíticas, secuencia de AWS Transform forma inteligente la transformación de las aplicaciones del mainframe, lo que le ayuda a transformar las funciones empresariales en paralelo. AWS Transform puede acelerar la toma de decisiones y mejorar la agilidad operativa y la eficiencia de la migración.

Este patrón ofrece step-by-step instrucciones que le ayudarán a probar las capacidades de modernización del mainframe AWS Transform mediante CardDemoel uso de un ejemplo de una aplicación de mainframe de código abierto.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- AWS IAM Identity Center, habilitado
- Permisos que permiten a los administradores habilitar AWS Transform
- Permisos que permiten a los administradores aceptar solicitudes de conexión de Amazon Simple Storage Service (Amazon S3) para AWS Transform la aplicación web

Limitaciones

- AWS Transform está disponible solo en algunos Regiones de AWS. Para obtener la lista completa de regiones admitidas, consulte Supported Regions for AWS Transform.
- AWS Transform admite el análisis de código, la generación de documentos, la extracción de reglas empresariales, la descomposición y la refactorización del lenguaje común orientado a los

negocios (COBOL) a Java. Para obtener más información, consulte Capabilities and key features y Supported file types for transformation of mainframe applications.

- Hay una cuota de servicio para las capacidades de transformación del mainframe en AWS Transform. Para obtener más información, consulte Cuotas para AWS Transform.
- Para poder colaborar en un espacio de trabajo compartido, todos los usuarios deben estar registrados en la misma instancia AWS IAM Identity Center que esté asociada a la instancia de la aplicación web. AWS Transform
- El bucket de Amazon S3 AWS Transform debe estar en la misma región Cuenta de AWS y.

Arquitectura

En el siguiente diagrama se muestra la arquitectura que configuró en este patrón.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. AWS Transform utiliza un conector para acceder a la aplicación de CardDemo mainframe, que está almacenada en un bucket de Amazon S3.
2. AWS Transform AWS IAM Identity Center se utiliza para administrar el acceso y la autenticación de los usuarios. El sistema implementa distintos niveles de controles de seguridad para la autenticación, la autorización, el cifrado y la administración del acceso para proteger el código y los artefactos durante el procesamiento. Los usuarios interactúan con el AWS Transform agente a través de una interfaz de chat. Puede dar instrucciones al agente de IA para realizar tareas específicas en inglés. Para obtener más información, consulte Human in the loop (HITL) en la AWS Transform documentación.
3. El agente de IA interpreta las instrucciones del usuario, crea un plan de trabajo, divide el trabajo en tareas ejecutables y lo ejecuta de forma autónoma. Los usuarios pueden revisar y aprobar la transformación. Estas son algunas de las tareas de transformación:
   - Análisis de código: AWS Transform analiza el código de cada archivo para obtener detalles como el nombre y el tipo de archivo, las líneas de código y sus rutas. El agente analiza el código fuente, ejecuta clasificaciones, crea asignaciones de las dependencias e identifica cualquier artefacto que falte. También identifica los componentes duplicados.
   - Generación de documentos: AWS Transform genera documentación para la aplicación de mainframe. Al analizar el código, puede crear automáticamente documentación detallada de los programas de las aplicaciones, así como descripciones de la lógica empresarial, los flujos, las integraciones y las dependencias que hay en los sistemas heredados.

- Extracción de la lógica empresarial: AWS Transform analiza los programas de COBOL para documentar su lógica empresarial principal, a fin de ayudarlo a comprender la lógica empresarial fundamental.
- Descomposición del código: AWS Transform descompone el código en dominios que tienen en cuenta las dependencias entre los programas y los componentes. La agrupación de archivos y programas relacionados en el mismo dominio mejora la organización y ayuda a preservar la estructura lógica de la aplicación al dividirla en componentes más pequeños.
- Planificación de la oleada de migración: en función de los dominios que haya creado durante la fase de descomposición, AWS Transform genera un plan de migración con el orden de modernización recomendado.
- Refactorización de código: AWS Transform refactoriza el código de todos los archivos de dominio o de algunos de ellos en código Java. El objetivo de este paso es preservar la lógica empresarial fundamental de la aplicación y, al mismo tiempo, refactorizarla para convertirla en una aplicación de Java modernizada y optimizada para la nube.

4. AWS Transform almacena el código refactorizado, los documentos generados, los artefactos asociados y las bibliotecas de tiempo de ejecución en su bucket de Amazon S3. Se puede hacer lo siguiente:
   - Acceda a la carpeta del tiempo de ejecución del bucket de Amazon S3.
   - Cree e implemente la aplicación siguiendo las instrucciones de la documentación sobre cómo crear e implementar la aplicación modernizada después de la refactorización. AWS Transform
   - A través de la interfaz de chat, solicite y descargue una muestra o una plantilla Terraform de AWS CloudFormation AWS Cloud Development Kit (AWS CDK) Hashicorp. Estas plantillas pueden ayudarlo a implementar los AWS recursos necesarios para respaldar la aplicación refactorizada.
   - Utilice Reforge para mejorar la calidad del código refactorizado mediante el uso de modelos de lenguaje de gran tamaño (). LLMs El motor de refactorización conserva la equivalencia funcional de COBOL y, al mismo tiempo, la transforma en código Java. El uso de Reforge es un paso opcional que está disponible después de la transformación. Este paso se utiliza LLMs para reestructurar el código para que se parezca mucho al Java nativo, lo que puede mejorar la legibilidad y el mantenimiento. Reforge también agrega comentarios legibles por humanos para ayudarlo a entender el código e implementa patrones de programación modernos y prácticas recomendadas.

Tools (Herramientas)

Servicios de AWS

- AWS Transformutiliza la IA agentic para ayudarlo a acelerar la modernización de las cargas de trabajo heredadas, como .NET, los mainframes y las cargas de trabajo. VMware
- AWS IAM Identity Centerle ayuda a gestionar de forma centralizada el acceso mediante inicio de sesión único (SSO) a sus aplicaciones y a las de la nube. Cuentas de AWS
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Repositorio de código

Puede utilizar la aplicación de AWS CardDemomainframe de código abierto como ejemplo de aplicación para empezar a modernizar el mainframe.

Prácticas recomendadas

- Comience de a poco: comience con un código pequeño y menos complejo (entre 15 000 y 20 000 líneas de código) para comprender cómo se AWS Transform analizan y transforman las aplicaciones de mainframe.
- Combínelo con la experiencia humana: utilícelo AWS Transform como acelerador y, al mismo tiempo, aplique la experiencia humana para obtener resultados óptimos.
- Haga revisiones y pruebas minuciosas: revise siempre detenidamente el código transformado y ejecute pruebas exhaustivas para validar la equivalencia funcional después de la transformación.
- Envía comentarios: para enviar comentarios y sugerencias de mejora, utiliza el botón Enviar comentarios del Consola de administración de AWS o crea un caso con AWS Support. Para obtener más información, consulte Creación de un caso de soporte. Sus comentarios son valiosos para poder mejorar y seguir desarrollando el servicio.

Epics

Preparación de la aplicación del mainframe

Tarea	Descripción	Habilidades requeridas
Crear un bucket.	Cree un bucket de Amazon S3 en la misma Cuenta de AWS región en la que AWS Transform está activado. Utiliza este depósito para almacenar el código de la aplicación del mainframe y AWS Transform utiliza este depósito para almacenar los documentos generados , el código refactorizado y otros archivos asociados a la transformación. Para obtener instrucciones, consulte Crear un bucket en la documenta ción de Amazon S3.	AWS general
Prepare la aplicación del mainframe de ejemplo.	1. Introduzca el siguiente comando para clonar el CardDemorepositorio en su estación de trabajo local: `git clone https://github.com/aws-samples/aws-mainframe-modernization-carddemo.git` 2. Cree una nueva carpeta denominada `carddemo`. 3. Copie la carpeta `app`, que contiene el código fuente	Desarrollador de aplicaciones, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	del mainframe, del repositorio clonado a la carpeta `carddemo`. 4. Comprima la carpeta `cardemo` en un archivo ZIP. 5. Cargue el archivo ZIP en el bucket de Amazon S3 que creó. Para más instrucciones, consulte Cargar objetos en la documentación de Amazon S3.	

Configure el Centro de Identidad de IAM y AWS Transform

Tarea	Descripción	Habilidades requeridas
Agregue usuarios a IAM Identity Center.	Agregue los posibles usuarios a IAM Identity Center. Siga las instrucciones de la documentación sobre cómo añadir usuarios al Centro de identidades de IAM. AWS Transform	Administrador de AWS
Habilite AWS Transform y añada usuarios.	1. Habilitar AWS Transform. Siga las instrucciones que se indican en Enable AWS Transform. 2. Añadir usuarios a AWS Transform. Siga las instrucciones de Añadir usuarios a AWS Transform.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure el acceso de los usuarios a la aplicación AWS Transform web.	Cada usuario debe aceptar la invitación para acceder a la aplicación AWS Transform web. Siga las instrucciones que se indican en la AWS Transform documentación sobre cómo aceptar la invitación.	Desarrollador de aplicaciones, propietario de la aplicación
Inicie sesión en la aplicación AWS Transform web.	Siga las instrucciones que se indican en Iniciar sesión en AWS Transform.	Desarrollador de aplicaciones, propietario de la aplicación
Configure un espacio de trabajo.	Configure un espacio de trabajo en el que los usuarios puedan colaborar en la aplicación AWS Transform web. Siga las instrucciones de la AWS Transform documentación sobre cómo iniciar su proyecto.	Administrador de AWS

Transformación de la aplicación del mainframe

Tarea	Descripción	Habilidades requeridas
Cree un trabajo de transformación.	Cree un trabajo de transformación para modernizar la aplicación de CardDemo mainframe. Para obtener instrucciones, consulte Crear e iniciar un trabajo en la AWS Transform documentación. Cuando se le pida que defina los objetivos en la interfaz	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	de AWS Transform chat, elija Realizar la moderniza ción del mainframe (z/OS a IBM AWS) y, a continuac ión, elija Analizar código, Generar documentación técnica, Lógica empresari al, Descomponer código, Planificar la secuencia de migración y Transformar código a Java.	
Configure el conector.	Establezca un conector al bucket de Amazon S3 que contiene la aplicación de CardDemo mainframe. Este conector permite acceder AWS Transform a los recursos del bucket y realizar funciones de transformación consecuti vas. Para obtener instrucci ones, consulte Configurar un conector en la AWS Transform documentación.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Realice el análisis del código.	1. En la página Especificar la ubicación del activo, introduzca la ruta del bucket de Amazon S3 del archivo ZIP de `carddemo` que ha cargado. 2. Seleccione Aprobar y enviar a AWS Transform . Se empieza a analizar el código. 3. Supervise el estado en la pestaña Registro de trabajo. 4. Cuando se complete el análisis, en Analizar código en el panel de navegación izquierdo, seleccione Ver resultados del análisis de código. 5. (Opcional) Seleccione Descargar para descargar la lista completa de activos, el código fuente que falta y el archivo de dependencias. Para obtener más información, consulte Análisis de código en la AWS Transform documenta ción.	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Genere la documentación técnica.	1. En el panel de navegación izquierdo, en Generar documentación técnica, seleccione Seleccionar archivos y configurar ajustes. 2. Expanda COBOL o JCL y, a continuación, seleccione uno o varios archivos. 3. Seleccione el nivel de detalle de la documentación: • Resumen: proporciona información general de alto nivel sobre cada archivo que está dentro del ámbito. Además, ofrece un resumen de una línea de cada archivo. • Especificación funcional detallada: proporciona detalles completos de cada archivo que está incluido en el ámbito de la transformación de las aplicaciones del mainframe. Algunos detalles son la lógica y el flujo, las reglas empresariales identificadas, el flujo de datos, las dependencias, el procesamiento de entradas y salidas	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	y varios detalles de las transacciones. 4. Elija Enviar a AWS Transform. 5. Supervise el progreso en la pestaña Registro de trabajo. **Note** El tiempo de generación de los documentos varía de minutos a horas en función de la cantidad de archivos y líneas de código. 6. Cuando haya terminado , seleccione Revisar los resultados de la documentación. 7. Acceda al documento generado a través de la aplicación web o descárguelo. La documentación que se genera también se almacena en el bucket de Amazon S3. 8. Para explorar la documentación generada, haga preguntas específicas en la interfaz de chat. Por	

Tarea	Descripción	Habilidades requeridas
	ejemplo, puedes decir «Cuéntame las caracterí sticas de CBACT01 C» Para obtener más información, consulte Generar documenta ción técnica en la AWS Transform documentación.	

Tarea	Descripción	Habilidades requeridas
Extraiga la lógica empresarial.	1. En el panel de navegación izquierdo, expanda Extraer lógica empresarial y, a continuación, elija Seleccionar archivos para la extracción de lógica empresarial. 2. Expanda COBOL o JCL y, a continuación, seleccione uno o varios archivos. 3. Elija Enviar a AWS Transform. 4. Supervise el progreso en la pestaña Registro de trabajo. **Note** El tiempo de extracción de la lógica empresarial varía de minutos a horas en función de la cantidad de archivos y líneas de código. 5. Cuando se complete la extracción, seleccione Revisar los resultados de la extracción de la lógica empresarial. 6. Seleccione un archivo COBOL o JCL y, a	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	continuación, seleccione Ver. 7. Cambie el alcance de Diagrama de flujo y reglas funcionales para revisar los diferentes niveles de los diagramas de flujo, incluido el código complementario. 8. (Opcional) Revise la lógica empresarial generada, que se almacena en formato JSON en el bucket de Amazon S3. Para obtener más informaci ón, consulte Extraer la lógica empresarial en la AWS Transform documentación.	

Tarea	Descripción	Habilidades requeridas
Descomponga el código.	1. En el panel de navegación izquierdo, expanda Descomponer código y, a continuación, elija Descomponer en dominios. 2. En la lista Acciones, seleccione Crear dominio. 3. Introduzca un nombre para el nuevo dominio, como `Bill payment`. 4. (Opcional) Proporcione una descripción. 5. En la barra de búsqueda Buscar archivos, busque `CB00` y, a continuación, seleccione el archivo. 6. Seleccione Marcar como semilla. 7. Compruebe que la marca de semilla cambie de No a Sí. 8. Seleccione Crear. 9. Seleccione Save. 10. Seleccione Descomponer. 11. Revise el resultado de la descomposición; para ello, elija el nombre de dominio. 12. Cuando se complete la descomposición, elija Enviar a AWS Transform.	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	Para obtener más información sobre la descomposición y las semillas, consulte Descomposición en la documentación. AWS Transform	
Planifique las oleadas de migración.	Planifique las oleadas de migración de la CardDemo aplicación. Siga las instrucciones que aparecen en la AWS Transform documentación sobre la planificación de la oleada de migración para revisar y editar el plan de oleada.	Desarrollador de aplicaciones, propietario de la aplicación
Refactorice el código	1. Refactoriza la aplicación de CardDemo mainframe en código Java en todos los archivos de dominio o en algunos de ellos. Siga las instrucciones de refactorización del código de la documentación. AWS Transform 2. Una vez finalizado el proceso de refactorización, cree e implemente la aplicación Java moderniza da. Siga las instrucciones de la documentación sobre cómo crear e implement ar la aplicación moderniza da después de la refactori zación. AWS Transform	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
(Opcional) Utilice Reforge para mejorar el código de Java.	1. Cree un nuevo trabajo y, a continuación, introduzca un objetivo de `Reforge the code`. 2. Introduzca el de un proyecto que se haya modernizado previamen te. AWS Transform Este proyecto tiene que estar en el bucket de Amazon S3. 3. Introduzca una lista de clases de Java que especifique qué clases de servicio desea reforjar. 4. Revise la salida generada en el bucket de Amazon S3. Para obtener más información, consulte Reforge en la AWS Transform documentación.	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Optimice la implementación.	AWS Transform puede proporcionar plantillas de infraestructura como código (IaC) para Terraform o CloudFormation AWS CDK Terraform. Estas plantilla s lo ayudan a implementar los componentes principal es, como los recursos de computación, base de datos, almacenamiento y seguridad. 1. En la interfaz de AWS Transform chat, solicite las plantillas ingresand o `Share the mainframe refactor <service> templates` , donde `<service>` se encuentra uno de los servicios de iAc compatibles. 2. Implemente la plantilla mediante el servicio que prefiera. Por ejemplo, consulte los recursos siguientes: • Cree una pila desde la CloudFormation consola (CloudFormation documentación) • Implemente AWS CDK aplicaciones (AWS CDK documentación)	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	• Build infrastructure (documentación de Terraform) Para obtener más información, consulte Capacidades de implementación en la AWS Transform documentación.	

Resolución de problemas

Problema	Solución
No puede ver el código fuente ni el documento generado en la aplicación AWS Transform web.	Añada una política al permiso CORS para que el bucket de Amazon S3 la permita AWS Transform como origen. Para obtener más información, consulte los permisos CORS del bucket S3 en la AWS Transform documentación.

Recursos relacionados

AWS documentación

- Transformación de aplicaciones de mainframe (AWS Transform documentación)

Otros recursos AWS

- Acelere su proceso de modernización del mainframe utilizando agentes de IA con AWS Transform (AWS entrada del blog)
- AWS Transform FAQs
- AWS IAM Identity Center FAQs

Videos y tutoriales

- Introducción a Amazon Q Developer: Transform (AWS Skill Builder)
- AWS re:Invent 2024: Modernice las aplicaciones de mainframe más rápido con Amazon Q Developer () YouTube
- AWS re:Invent 2024: Automatizar la migración y la modernización para acelerar la transformación () YouTube
- AWS re:Invent 2024: Toyota impulsa la innovación y mejora la eficiencia operativa con la generación de IA () YouTube

> **Note**
>
> AWS Transform anteriormente se conocía como transformación de Amazon Q Developer para mainframe.

Modernice e implemente aplicaciones de mainframe con Terraform AWS Transform

Mason Cahill, Polaris Jhandi, Prachi Khanna, Sivasubramanian Ramani y Santosh Kumar Singh, Amazon Web Services

Resumen

AWS Transformpuede acelerar la modernización a gran escala de .NET, el mainframe y las cargas VMware de trabajo. Implementa agentes de IA especializados que automatizan las tareas complejas como las evaluaciones, el análisis de código, la refactorización, la descomposición, la asignación de dependencias, la validación y la planificación de la transformación. Este patrón demuestra cómo AWS Transform modernizar una aplicación de mainframe y luego implementarla en la AWS infraestructura mediante Hashicorp Terraform. Estas step-by-step instrucciones le ayudan a pasar de COBOL a una aplicación Java moderna CardDemo, que es un ejemplo de aplicación de mainframe de código abierto.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Permisos administrativos para crear AWS recursos e implementar aplicaciones
- La versión 1.5.7 o posterior de Terraform configurada
- AWS Proveedor de Terraform, configurado
- AWS IAM Identity Center, activado
- AWS Transform, habilitado
- Un usuario incorporado a un espacio de AWS Transform trabajo con un rol de colaborador que puede ejecutar tareas de transformación

Limitaciones

- AWS Transform solo está disponible en algunos. Regiones de AWS Para obtener la lista completa de regiones admitidas, consulte Supported Regions for AWS Transform.
- Hay una cuota de servicio para las capacidades de transformación del mainframe en AWS Transform. Para obtener más información, consulte Cuotas para AWS Transform.

- Para colaborar en un espacio de trabajo compartido, todos los usuarios deben ser usuarios registrados de la misma instancia AWS IAM Identity Center que esté asociada a tu instancia de la aplicación AWS Transform web.
- El bucket de Amazon Simple Storage Service (Amazon S3) debe estar en la Cuenta de AWS misma región AWS Transform y.

Arquitectura

El siguiente diagrama muestra la end-to-end modernización de la aplicación antigua y su implementación en Nube de AWS. Las credenciales de la aplicación y la base de datos se almacenan en AWS Secrets Manager, y Amazon CloudWatch proporciona capacidades de monitoreo y registro.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. A través de él AWS IAM Identity Center, el usuario se autentica y accede al AWS Transform . Cuenta de AWS
2. El usuario carga el código de mainframe COBOL en el bucket de Amazon S3 e inicia la transformación en AWS Transform.
3. AWS Transform moderniza el código COBOL para convertirlo en código Java nativo de la nube y almacena el código modernizado en el bucket de Amazon S3.
4. Terraform crea la AWS infraestructura para implementar la aplicación modernizada, que incluye un Application Load Balancer, una instancia de Amazon Elastic Compute Cloud (Amazon EC2) y una base de datos del Amazon Relational Database Service (Amazon RDS). Terraform implementa el código modernizado en la instancia de Amazon EC2.
5. Los archivos VSAM se cargan en Amazon EC2 y se migran de Amazon EC2 a la base de datos de Amazon RDS.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez. En este patrón, las instancias de clúster de conmutación por error de SQL Server se instalan en las instancias de Amazon EC2.

- AWS IAM Identity Centerle ayuda a gestionar de forma centralizada el acceso mediante el inicio de sesión único (SSO) a sus aplicaciones y a las de la nube. Cuentas de AWS
- Amazon Relational Database Service (Amazon RDS) lo ayuda a configurar, utilizar y escalar una base de datos relacional en la Nube de AWS.
- AWS Secrets Manager lo ayuda a reemplazar las credenciales codificadas en su código, incluidas contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Transformutiliza la IA agentic para ayudarlo a acelerar la modernización de las cargas de trabajo antiguas, como .NET, los mainframes y las cargas de trabajo. VMware

Otras herramientas

- Apache Maven es una herramienta de automatización de compilaciones y administración de proyectos de software de código abierto para proyectos de Java.
- Apache Tomcat es un contenedor de servlets de código abierto y un servidor web para el código Java.
- HashiCorp Terraform es una herramienta de infraestructura como código (IaC) que facilita usar el código para aprovisionar y administrar los recursos y la infraestructura en la nube.
- Spring Boot es un marco de código abierto que se creó sobre Spring Boot Framework en Java.

Repositorio de código

El código de este patrón está disponible en el repositorio E2E de Mainframe Transformation GitHub . Este patrón utiliza la aplicación de AWS CardDemomainframe de código abierto como aplicación de ejemplo.

Prácticas recomendadas

- Asigne la propiedad total del código y los recursos destinados a la migración.
- Desarrolle y pruebe una prueba de concepto antes de escalar a una migración completa.
- Garantice la implicación de todas las partes interesadas.
- Establezca canales de comunicación claros.
- Defina y documente los requisitos para un producto mínimo viable (MVP).

- Establezca criterios de éxito claros.

Epics

Preparación y carga del código de la aplicación del mainframe

Tarea	Descripción	Habilidades requeridas
Crear un bucket.	Cree un bucket de Amazon S3 en la misma Cuenta de AWS región en la que AWS Transform está activado. Este depósito se utiliza para almacenar el código de la aplicación del mainframe, los datos y los scripts adicional es necesarios para crear y ejecutar la aplicación. AWS Transform utiliza este depósito para almacenar el código refactorizado y otros archivos asociados a la transformación. Para obtener instrucciones, consulte Crear un bucket en la documentación de Amazon S3.	AWS general, administrador de AWS
Configure los permisos de CORS para el bucket.	Al configurar su depósito para el AWS Transform acceso, debe configurar el uso compartido de recursos de origen cruzado (CORS) para el depósito. Si no se ha configurado correctamente, es posible que no pueda utilizar las funciones de visualización en línea o de comparación de	AWS general, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	archivos de AWS Transform . Para obtener instrucciones sobre cómo configurar CORS para un bucket, consulte Uso compartido de recursos entre orígenes en el bucket de Amazon S3. Para conocer la política, consulta los permisos CORS del bucket de S3 en la documentación. AWS Transform	
Prepare el código de la aplicación del mainframe de ejemplo.	1. Introduzca el siguiente comando para clonar el CardDemorepositorio en su estación de trabajo local: `git clone https://github.com/aws-samples/aws-mainframe-modernization-carddemo.git` 2. Comprima la carpeta `aws-mainframe-modernization-carddemo` en un archivo ZIP. 3. Cargue el archivo ZIP en el bucket de Amazon S3 que creó. Para más instrucciones, consulte Cargar objetos en la documentación de Amazon S3.	AWS general, desarrollador de aplicaciones

Transformación de la aplicación del mainframe

Tarea	Descripción	Habilidades requeridas
Configure el AWS Transform trabajo.	1. Acceda a la aplicación AWS Transform web iniciando sesión con sus credencia les. 2. Cree un nuevo espacio de trabajo siguiendo las instrucciones que se indican en la AWS Transform documentación sobre cómo configurar su espacio de trabajo. 3. En la página de inicio de tu espacio de trabajo, selecciona AWS Transform Solicitar la creación de un trabajo. 4. A continuación, seleccion e Modernización del mainframe como tipo de trabajo. 5. En la ventana de chat, introduzca Transformar código en Java. 6. Revise el tipo de trabajo, el nombre y el objetivo sugeridos. Para confirmarlo, introduzca Sí. 7. Seleccione Crear tarea.	Desarrollador de aplicaciones, propietario de la aplicación
Configure un conector.	1. Configure un conector con el bucket de Amazon S3 que creó. Para obtener	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	instrucciones, consulta Cómo configurar un conector en la AWS Transform documentación. Cuando se le solicite, escriba la ruta del archivo zip `aws-mainframe-modernization-carddemo` en el bucket de Amazon S3. 2. Espere a que el análisis finalice.	

Tarea	Descripción	Habilidades requeridas
Transforme el código.	1. Revise los resultados del análisis del código según las instrucciones de la AWS Transform documentación sobre cómo analizar el código. 2. Refactoriza el código del mainframe según las instrucciones de Refactorización del código de la documentación. AWS Transform Para la aplicación de CardDemo mainframe de ejemplo, puede aceptar la configuración predeterminada. 3. Espere a que finalice la refactorización. 4. Seleccione Ver resultados para ver la ruta del código refactorizado en el bucket de Amazon S3. Tome nota de esta ruta de archivo. La necesitará más adelante.	Desarrollador de aplicaciones, propietario de la aplicación

Implementación de la infraestructura mediante Terraform

Tarea	Descripción	Habilidades requeridas
Actualice las plantillas.	1. Introduzca el siguiente comando para clonar el repositorio Mainframe	AWS general, administrador de AWS

Tarea	Descripción	Habilidades requeridas

	Transformation E2E en la estación de trabajo local:
	`git clone https://github.com/aws-samples/sample-mainframe-transformation-e2e.git`
	2. Introduzca el comando siguiente para obtener la dirección IP pública actual:
	`curl checkip.amazonaws.com`
	3. Escriba el siguiente comando para navegar al directorio infra:
	`cd mainframe-transformation-e2e/infra`
	4. Abra el archivo `variables.tf` .
	5. Reemplace `YOUR_IP_ADDRESS_HERE` por su dirección IP.
	6. Si tiene una zona alojada pública, siga estos pasos:
	a. Sustituya `hosted_zone_name` por el nombre de la zona alojada.
	b. Establece `hosted_zone_enabled` en `true`.	

Tarea	Descripción	Habilidades requeridas

	Si no tiene una zona alojada pública, siga estos pasos:
	a. Introduzca los siguientes comandos para generar un certificado autofirmado:
	`openssl genrsa 2048 > my-private-key.pem`
	`openssl req -new -x509 -nodes -sha256 -days 365 -key my-private-key.pem -outform PEM -out my-certificate.pem`
	b. Introduzca el siguiente comando para importar el certificado a AWS Certificate Manager (ACM):
	`aws acm import-certificate \`
	`--certificate fileb://my-certificate.pem \`
	`--private-key fileb://my-private-key.pem`
	El resultado de este comando incluye el nombre de recurso	

Tarea	Descripción	Habilidades requeridas
	de Amazon (ARN) del certificado importado. c. Reemplace `self_signed_cert_arn` por el ARN del certificado. d. Establece `hosted_zone_enabled` en `false`. 7. Cambie `aws_region` por la región de destino. El valor predeterminado es `us-east-1` . 8. Guarde y cierre el archivo `variables.tf` . **Note** En el caso de los entornos de producción o similares a los de producción, configure componentes de seguridad adicionales. Por ejemplo, habilite las protecciones de AWS WAF para el equilibrador de carga de aplicación.	

Tarea	Descripción	Habilidades requeridas

Implemente la infraestructura.	1. Introduzca el comando siguiente para inicializar Terraform:
	`terraform init`
	2. Introduzca el comando siguiente para generar un plan de ejecución:
	`terraform plan`
	3. Revise el plan y valide los recursos y los component es de infraestructura que se van a crear.
	4. Introduzca el siguiente comando para implementar la infraestructura:
	`terraform apply`
	5. Cuando se le solicite, introduzca sí para confirmar la implementación.
	6. Espere hasta que se complete la implement ación.
		Terraform

Instalación y configuración de Apache Tomcat en la instancia de Amazon EC2

Tarea	Descripción	Habilidades requeridas
Instale el software necesario.	1. Conéctese a la instancia de Amazon EC2 mediante	Desarrollador de aplicación, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas

	AWS Systems Manager Session Manager.
	2. Ingrese el comando siguiente para cambiar al usuario raíz:
	`sudo su -`
	3. Escriba el siguiente comando para navegar al directorio `scripts`:
	`cd /opt/scripts`
	4. Revise el script install_software.sh. Este script instala Java 17, Apache Maven y Apache Tomcat 10.0.23.
	5. Actualice los scripts según sea necesario para su caso de uso.
	6. Introduzca el siguiente comando para convertir el script en ejecutable:
	`chmod +x install_software.sh`
	7. Introduzca el siguiente comando para ejecutar el script:
	`./install_software.sh`	

Tarea	Descripción	Habilidades requeridas

Verifique la instalación del software.	1. Introduzca el siguiente comando para iniciar el servidor de Tomcat:
	`/opt/tomcat/apache-tomcat-10.0.23/bin/startup.sh`
	2. Introduzca el siguiente comando para verificar la respuesta del servidor web:
	`curl http://localhost:8080`
	La salida debe confirmar que Tomcat atiende una página HTML.
		Desarrollador de aplicación, ingeniero de migraciones

Compilación y empaquetado del código de la aplicación modernizada

Tarea	Descripción	Habilidades requeridas
Descargue y extraiga el código generado.	1. Introduzca el siguiente comando para convertir el script download_and_extract.sh en ejecutable. Este script descarga el código refactorizado y la biblioteca de tiempo de ejecución de Gapwalk almacenados en el bucket de Amazon S3:	Desarrollador de aplicación, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas

	`chmod +x /opt/scripts/download_and_extract.sh`
	2. Ingrese el comando siguiente para ejecutar el script . Sustituya `<file_path>` por la ruta del archivo generated.zip en el bucket de Amazon S3:
	`./download_and_extract.sh <file_path>`
	Note
	La ruta del archivo suele ser `s3://<bucket-name>/transform_output/<aws_transform_job_id>/code transformation/generated.zip` .
	3. Introduzca el siguiente comando para ir a la carpeta `shared`:
	`cd /opt/runtime/velocity/shared`	

Tarea	Descripción	Habilidades requeridas

	4. Introduzca el siguiente comando para copiar el script deploy-velocity-runtime.sh:
	`cp /opt/scripts/deploy-velocity-runtime.sh .`
	5. Introduzca el siguiente comando para convertir el script copiado en ejecutable:
	`chmod +x deploy-velocity-runtime.sh`
	6. Ingrese el comando siguiente para ejecutar el script . Este script copia todas las dependencias del archivo de aplicaciones web (WAR) necesarias presentes en los archivos del modelo de objetos del proyecto (POM) en la carpeta del repositorio:
	`./deploy-velocity-runtime.sh`
	7. Verifique que la ejecución se haya realizado correctamente: compruebe que no haya errores y que las dependencias de WAR necesarias se hayan	

Tarea	Descripción	Habilidades requeridas
	instalado en el repositorio local de Maven.	

Tarea	Descripción	Habilidades requeridas

Compile la aplicación modernizada.	1. Introduzca el siguiente comando para navegar al directorio del proyecto `app-pom`:
	`cd /opt/codebase/app-pom/`
	2. Introduzca el siguiente comando para instalar Maven:
	`mvn clean install`
	3. Espere a que se completen la instalación y la compilación.
	Note
	Al ejecutar este comando para la CardDemo aplicación, es posible que aparezcan mensajes de advertencia para el `app-web` proyecto. Puede obviar estas advertencias transquilamente.
	4. Tras completar correctamente la compilación, confirme la presencia de `app-service/target`
		Desarrollador de aplicación, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	`/app-service-1.0.0.war` y `app-web/target/app-web-1.0.0.war` . **Important** No reinicie el servidor de Tomcat en este momento. Se producirían errores debido a la ausencia de las bases de datos necesarias. Para poder reiniciar el servidor, primero debe configurar la base de datos.	

Migración de la base de datos

Tarea	Descripción	Habilidades requeridas
Cree la base de datos y los esquemas JICS.	1. Introduzca el siguiente comando para cambiar el nombre de la carpeta `csd commands` por `csd_commands` . Esto eliminará los espacios del nombre de la carpeta: `mv /opt/codebase/extra/csd\ commands/ /`	Desarrollador de aplicación, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas

	`opt/codebase/extra/csd_commands`
	2. Introduzca el siguiente comando para ir al directorio `scripts`:
	`cd /opt/scripts`
	3. Introduzca el siguiente comando para convertir el script de migración de la base de datos en ejecutable:
	`chmod +x database_migration_setup.sh`
	4. Introduzca los siguientes comandos para configurar las siguientes variables como parámetros:
	`RDS_ENDPOINT=<database_endpoint>`
	`SECRET_NAME=<secret_name>`
	`JICS_SQL_SCRIPT_DIR=/opt/runtime/velocity/jics/sql/jics.sql`
	`INIT_JICS_SQL_SCRIPT_DIR=/opt/codebase/extra/csd_commands/sql/aws-mainframe-modernization-carddemo-main/app/csd/initJics.sql`	

Tarea	Descripción	Habilidades requeridas

	Donde:
	• `<database_endpoint>` es el punto de conexión de la base de datos de Amazon RDS que implementó a través de Terraform.
	• `<secret_name>` es el nombre del AWS Secrets Manager secreto que desplegaste a través de Terraform.
	5. Introduzca el siguiente comando para ejecutar el script de migración de la base de datos:
	`./database_migration_setup.sh $RDS_ENDPOINT $SECRET_NAME $JICS_SQL_SCRIPT_DIR $INIT_JICS_SQL_SCRIPT_DIR`
	6. Introduzca el siguiente comando para conectarse a la base de datos desde la instancia de Amazon EC2:
	`psql -h <Your Amazon RDS Endpoint> -U foo -p 5432 postgres`	

Tarea	Descripción	Habilidades requeridas
	7. Cuando se le solicite, introduzca las credenciales de la base de datos.	

Valide la creación de la base de datos.	1. Introduzca el siguiente comando para ver todas las bases de datos:
	`\l`
	2. Introduzca el siguiente comando para cambiar a la base de datos `jics`:
	`\c jics`
	3. Introduzca el siguiente comando para revisar una lista de las tablas creadas:
	`\dt`
		Desarrollador de aplicación, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas

Migre los datos a la base de datos de JICS.	1. Introduzca el siguiente comando para convertir el script execute_listcat_sql.sh en ejecutable:
	`chmod +x execute_listcat_sql.sh`
	2. Introduzca el siguiente comando para configurar la variable `PATH_TO_LISTCAT_SQL_FILES`, que es el directorio que contiene los archivos SQL de LISTCAT:
	`PATH_TO_LISTCAT_SQL_FILES=/opt/codebase/extra/listcat/sql/cluster/aws-mainframe-modernization-carddemo-main/app/catlg`
	3. Asegúrese de que las variables `RDS_ENDPOINT`, `SECRET_NAME` y `PATH_TO_LISTCAT_SQL_FILES` estén configuradas correctamente de acuerdo con las instrucciones anteriores.
	4. Introduzca el siguiente comando para ejecutar el script execute_listcat_sql.sh:
		Desarrollador de aplicación, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	`./execute_listcat_sql.sh $RDS_ENDPOINT $SECRET_NAME $PATH_TO_LISTCAT_SQL_FILES` Este script actualiza las propiedades del archivo VSAM en la base de datos de JICS y ejecuta las consultas necesarias para modificar la base de datos.	

Instalación de la aplicación modernizada

Tarea	Descripción	Habilidades requeridas

Instale la aplicación modernizada en la instancia de Amazon EC2.	1. Introduzca el siguiente comando para convertir el script application_installer.sh en ejecutable:
	
	`chmod +x /opt/scripts/application_installer.sh`
	
	2. Introduzca los siguientes comandos para configurar las siguientes variables como parámetros:
	
	`RDS_ENDPOINT=<database_endpoint>`
	`SECRET_NAME=<secret_name>`
		Desarrollador de aplicaciones, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	AIX_JSON_FILE_PATH=/opt/codebase/extra/csd_commands/json/aws-mainframe-modernization-carddemo-main/jicsFileAix.json LISTCAT_JSON_FILES_DIR=/opt/codebase/extra/listcat/json/cluster/default/aws-mainframe-modernization-carddemo-main/app/catlg S3_PATH_FOR_EBCDIC_DATA_FILES=s3://<bucket_name>/transform-output/<job_id>/inputs/aws-mainframe-modernization-carddemo-main/app/data/EBCDIC Donde: • <database_endpoint> es el punto de conexión de la base de datos de Amazon RDS que implementó a través de Terraform. • <secret_name> es el nombre del AWS Secrets Manager secreto que desplegaste a través de Terraform. • <bucket_name> es el nombre del bucket de Amazon S3 que contiene	

Tarea	Descripción	Habilidades requeridas

	la aplicación moderniza da.
	• <job_id>es el identific ador del AWS Transform trabajo.
	3. Introduzca el siguiente comando para ejecutar el script application_instal ler.sh:
	`./application_inst aller.sh $RDS_ENDP OINT $SECRET_NAME $AIX_JSON_FILE_PAT H $LISTCAT_JSON_FILE S_DIR $S3_PATH_ FOR_EBCDIC_DATA_FI LES`
	4. En la `/opt/tomcat/ apache-tomcat-1 0.0.23/workingdir/ config` carpeta, en el application-utility-pgmarchivo.yml, cambie el parámetro de codificación por el siguiente:
	`encoding : CP1047`
	Note
	Al refactorizar las aplicaciones AWS Transform automáticamente	

Tarea	Descripción	Habilidades requeridas
	mediante AWS Blu Age, se configura la aplicación y su entorno de ejecución mediante archivos YAML. Por ejemplo, puede configura r el registro en el archivo application-main.yml correspon diente a la aplicació n. Para obtener más información sobre las propiedad es disponibles, consulte Habilitar propiedades para AWS Blu Age Runtime.	

Tarea	Descripción	Habilidades requeridas

Reinicie el servidor de Tomcat.	1. Introduzca el siguiente comando para ir al directorio de trabajo:
	`cd /opt/tomcat/apache-tomcat-10.0.23/workingdir`
	2. Introduzca los siguientes comandos para detener e iniciar el servidor de Tomcat:
	`/opt/tomcat/apache-tomcat-10.0.23/bin/shutdown.sh`
	`/opt/tomcat/apache-tomcat-10.0.23/bin/startup.sh`
	3. Introduzca el siguiente comando para supervisar los registros de arranque del servicio de Tomcat:
	`tail -f /opt/tomcat/apache-tomcat-10.0.23/logs/catalina.out`
		Desarrollador de aplicaciones, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Migre el conjunto de datos de VSAM.	1. Abra la consola de Amazon EC2. 2. En el panel de navegación, elija Load balancers (Balanceadores de carga). 3. Seleccione el equilibrador de carga que se creó a través de Terraform. 4. Busque el nombre del sistema de nombres de dominio (DNS) del equilibrador de carga de aplicación, como `application-load-balancer-<id>.<region>.elb.amazonaws.com` . 5. En el navegador, navegue hasta `http://<dns_name>/gapwalk-application/scripts/data-load` , donde `<dns_name>` es el nombre de DNS del equilibrador de carga de aplicación. Esto inicia el script de carga de datos. 6. Espere a que el script finalice. Cuando termine, el navegador mostrará LISTO. 7. En la instancia de Amazon EC2, abra un nuevo terminal.	Desarrollador de aplicación, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas

	8. Introduzca el siguiente comando para conectarse a la base de datos de Amazon RDS y sustituya `<database_endpoint>` por su valor:
	`psql -h <database_endpoint> -U foo -p 5432 postgres`
	9. Cuando se le solicite, escriba las credenciales para conectarse a la base de datos.
	10. Introduzca el siguiente comando para ver todas las bases de datos:
	`\l`
	11. Introduzca el siguiente comando para cambiar a la base de datos `bluesam`:
	`\c bluesam`
	12. Introduzca el siguiente comando para revisar una lista de las tablas creadas:
	`\dt`
	13. Introduzca el siguiente comando para validar la carga de datos:	

Tarea	Descripción	Habilidades requeridas
	`SELECT * FROM public.aws_m2_carddemo_usrsec_vsam_ksds;` La salida debe mostrar 10 registros devueltos.	

Tarea	Descripción	Habilidades requeridas
Actualice los parámetros en los scripts de Groovy.	1. Introduzca el siguiente comando para ir al directorio del script: `cd /opt/tomcat/apache-tomcat-10.0.23/webapps/workingdir/scripts` 2. En todos los archivos de Groovy que contengan referencias a archivos planos, actualice las siguientes configuraciones de archivos: • Ruta del archivo local: la ruta al archivo plano del directorio local de la instancia de Amazon EC2. • Tipo de sistema de archivos: el sistema de archivos que contiene los archivos planos. • Tamaño de registro: el tamaño del archivo plano. Como referencia, consulte el script de ejemplo DUSRSECJ.jcl.groovy en el repositorio de código. 3. Guardar y cerrar los archivos.	Desarrollador de aplicaciones

Pruebe la aplicación

Tarea	Descripción	Habilidades requeridas
Pruebe la aplicación modernizada.	1. Acceda a la aplicación en línea a través del equilibrador de carga de aplicación (`http://<your-load-balancer-dns>`) o a través de la zona alojada (`https://myhostedzone.dev/`). 2. Para el ID de transacción, introduzca `CC00`. 3. Para el nombre de usuario, introduzca `USER0001`. 4. Para la contraseña, introduzca `PASSWORD`. Tras iniciar sesión correctamente, aparece el menú principal.	Desarrollador, ingeniero de pruebas
Compruebe los scripts del lote.	1. Acceda a los scripts a través del equilibrador de carga de aplicación (`http://<your-load-balancer-dns>/gapwalk-application/scripts`) o a través de la zona alojada (`https://myhostedzone.dev/gapwalk-application/scripts`).	Desarrollador, ingeniero de pruebas

Tarea	Descripción	Habilidades requeridas
	2. Elija un script para ejecutarlo, como el script DUSRSECJ.jcl.groovy. 3. Compruebe que el script se ejecute correctamente. A continuación, se presenta una salida de muestra tras ejecutar el script correctam ente. `{ "exitCode": 0, "stepName": "STEP03", "program": "IDCAMS", "status": "Succeeded" }`	

Limpieza

Tarea	Descripción	Habilidades requeridas
Prepárese para eliminar la infraestructura.	1. Introduzca el siguiente comando para eliminar la protección de eliminación de la instancia de Amazon RDS: `aws rds modify-db-instance \ --db-instance-identifier <your-db-instance-name> \ --no-deletion-protection \ --apply-immediately`	AWS general

Tarea	Descripción	Habilidades requeridas

	2. Introduzca el siguiente comando para eliminar la protección de eliminación del equilibrador de carga de aplicación:
	
	`aws elbv2 modify-load-balancer-attributes \ --load-balancer-arn <your-load-balancer-arn> \ --attributes Key=deletion_protection.enabled,Value=false`
	
	3. Introduzca los siguientes comandos para eliminar el contenido de los buckets de Amazon S3:
	
	`ACCOUNT_NUMBER=$(aws sts get-caller-identity --query Account --output text)`
	`aws s3 rm s3://mf-carddemo-$ACCOUNT_NUMBER --recursive`
	`aws s3 rm s3://mf-carddemo-logs-$ACCOUNT_NUMBER --recursive`	

Tarea	Descripción	Habilidades requeridas

Configurar la infraestructura.	**Important**
	Estos pasos eliminará n sus recursos de forma permanente. Asegúrese de haber realizado una copia de seguridad de todos los datos importantes antes de continuar.
	
	1. Introduzca el siguiente comando para ir a la carpeta `infra`:
	`cd /mainframe-transformation-e2e/infra`
	2. Introduzca el siguiente comando para eliminar la infraestructura:
	`terraform destroy --auto-approve`
		AWS general

Resolución de problemas

Problema	Solución
Autenticación de Terraform	1. Asegúrese de que las AWS credenciales estén configuradas correctamente. 2. Compruebe que ha seleccionado el AWS perfil correcto.

Problema	Solución
	3. Confirme que tenga los permisos necesario s.
Errores relacionados con Tomcat	1. Consulte catalina.out en `/opt/tomcat/apache-tomcat-10.0.23/logs` para ver si hay alguna excepción. 2. Introduzca el siguiente comando para cambiar la propiedad de la carpeta de Tomcat al usuario de Tomcat: `chown -R tomcat:tomcat /opt/tomcat/*`
El nombre de la URL no se carga	Asegúrese de que el grupo de seguridad del equilibrador de carga de aplicación tenga su dirección IP en la regla de entrada como origen.
Problema de autenticación en el registro de Tomcat	Confirme que la contraseña secreta de la base de datos AWS Secrets Manager y la contraseñ a del archivo server.xml coinciden.

Recursos relacionados

AWS Guía prescriptiva

- Modernice la aplicación de CardDemo mainframe con AWS Transform

AWS documentación de servicio

- AWS Consola de administración de Blue Age Blusam
- Requisitos de configuración de la infraestructura para AWS Blu Age Runtime (no gestionada)
- Incorporación de AWS Blu Age Runtime
- Modernización de las aplicaciones de mainframe

- Configure la configuración de AWS Blu Age Runtime

AWS publicaciones de blog

- Acelere su proceso de modernización del mainframe con agentes de IA con AWS Transform

Modernice la administración de la producción del mainframe AWS mediante Rocket Enterprise Server y LRS X PageCenter

Shubham Roy, Amazon Web Services

Abraham Rondon, Micro Focus

Guy Tucker, Levi, Ray and Shoup Inc

Resumen

Al modernizar la administración de la producción de su mainframe, puede ahorrar costos, mitigar la deuda técnica que implica el mantenimiento de los sistemas heredados y mejorar la resiliencia y la agilidad mediante las tecnologías nativas de la DevOps nube de Amazon Web Services (AWS). Este patrón muestra cómo modernizar las cargas de trabajo de administración de la producción de mainframe críticas para la empresa en la nube de AWS. El modelo utiliza Rocket Enterprise Server como entorno de ejecución para una aplicación de mainframe modernizada, con Levi, Ray & Shoup, Inc. (LRS) VPSX/MFI (Micro Focus Interface) como servidor de impresión y LRS X como servidor de archivos. PageCenter El LRS PageCenter X ofrece soluciones de administración de resultados para ver, indexar, buscar, archivar y proteger el acceso a los resultados empresariales.

El patrón se basa en el enfoque de modernización del mainframe a través de redefinir la plataforma. Las aplicaciones de mainframe se migran mediante AWS Mainframe Modernization a Amazon Elastic Compute Cloud (Amazon EC2). Las cargas de trabajo de administración de resultados de mainframe se migran a Amazon EC2, y una base de datos de mainframe, como IBM Db2 (para), funciona con z/OS, is migrated to Amazon Relational Database Service (Amazon RDS). The LRS Directory Integration Server (LRS/DIS AWS Directory Service para Microsoft Active Directory para la autenticación y autorización del flujo de trabajo de administración de resultados.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una carga de trabajo de administración de la producción de mainframe.
- Conocimientos básicos sobre cómo volver a compilar y entregar una aplicación de mainframe que se ejecute en Rocket Enterprise Server. Para obtener más información, consulte la ficha técnica de Rocket Enterprise Server en la documentación de Rocket Software.

- Conocimientos básicos de las soluciones y los conceptos de impresión en la nube de LRS. Para obtener más información, consulte Output Modernization (Modernización de la producción) en la documentación del LRS.
- Software y licencia de Rocket Enterprise Server. Para obtener más información, contacte con Rocket Software.
- VPSX/MFI, LRS PageCenterX, LRS/Queue, and LRS/DISSoftware y licencias de LRS. Para obtener más información, póngase en contacto con LRS. Debe proporcionar los nombres de host de las EC2 instancias en las que se instalarán los productos LRS.

Nota: Para obtener más información sobre las consideraciones de configuración de las cargas de trabajo de administración de la salida de mainframe, consulte Consideraciones en la sección Información adicional de este patrón.

Versiones de producto

- Rocket Enterprise Server 10.0
- LRS VPSX/MFI
- LRS PageCenter X V1R3 o posterior

Arquitectura

Pila de tecnología de origen

- Sistema operativo: IBM z/OS
- Lenguaje de programación: Common Business-Oriented Language (COBOL), Job Control Language (JCL) y Customer Information Control System (CICS)
- Base de datos: IBM Db2 para z/OS, base de datos del Sistema de Gestión de la Información de IBM (IMS) y Método de acceso al almacenamiento virtual (VSAM)
- Seguridad: Resource Access Control Facility (RACF), CA Top Secret for z/OS y Access Control Facility 2 () ACF2
- Soluciones de impresión y archivado: productos de impresión y z/OS salida para mainframes de IBM (IBM Infoprint Server for z/OS, LRS y CA Deliver) y soluciones de archivado (CA Deliver, ASG Mobius o CA Bundle)

Arquitectura de origen

El diagrama siguiente muestra una arquitectura de estado actual tipo para una carga de trabajo de administración de la producción de mainframe.

El diagrama muestra el siguiente flujo de trabajo:

1. Los usuarios llevan a cabo transacciones comerciales en un sistema de participación (SoE) que se basa en una aplicación CICS de IBM escrita en COBOL.
2. El SoE invoca el servicio de mainframe, que registra los datos de las transacciones comerciales en una base de datos (SoR) como IBM Db2 for z/OS. system-of-records
3. El SoR conserva los datos comerciales del SoE.
4. El programador de trabajos por lotes inicia un trabajo por lotes para generar resultados de impresión.
5. El trabajo por lotes extrae los datos de la base de datos. Formatea los datos de acuerdo con los requisitos comerciales y, a continuación, genera producción empresarial, como extractos de facturación, tarjetas de identidad o extractos de préstamos. Por último, el trabajo por lotes dirige la producción a la administración de la producción para formatear, publicar y almacenar los resultados en función de los requisitos empresariales.
6. La administración de la producción recibe los resultados del trabajo por lotes. La gestión de salida indexa, organiza y publica la salida en un destino específico del sistema de gestión de salida, como las soluciones LRS PageCenter X (como se demuestra en este patrón) o CA View.
7. Los usuarios pueden ver, buscar y recuperar los resultados.

Pila de tecnología de destino

- Sistema operativo: Windows Server que se ejecuta en Amazon EC2
- Informática — Amazon EC2
- Almacenamiento: Amazon Elastic Block Store (Amazon EBS) y FSx Amazon para Windows File Server
- Lenguaje de programación: COBOL, JCL y CICS
- Bases de datos: Amazon RDS
- Seguridad: AWS Managed Microsoft AD
- Impresión y archivado: solución de impresión LRS (VPSX) y archivado (PageCenterX) en AWS

- Entorno de tiempo de ejecución de mainframe: Rocket Enterprise Server

Arquitectura de destino

El diagrama siguiente muestra una arquitectura para una carga de trabajo de administración de la producción de mainframe que se implementa en la nube de AWS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El programador de trabajos por lotes inicia un trabajo por lotes para generar la producción, como extractos de facturación, tarjetas de identificación o extractos de préstamos.
2. El trabajo por lotes del mainframe (rediseñado para Amazon EC2) utiliza el tiempo de ejecución de Rocket Enterprise Server para extraer datos de la base de datos de la aplicación, aplicar lógica empresarial a los datos y formatear los datos. A continuación, envía los datos a un destino de salida mediante el módulo de salida de la impresora de Rocket Software (documentación de OpenText Micro Focus).
3. La base de datos de la aplicación (un SoR que se ejecuta en Amazon RDS) conserva los datos para su impresión.
4. La solución de VPSX/MFI impresión LRS se implementa en Amazon EC2 y sus datos operativos se almacenan en Amazon EBS. LRS VPSX/MFI utiliza el agente de TCP/IP-based LRS/Queue transmisión para recopilar los datos de salida a través de la API JES Print Exit de Rocket Software.

   LRS VPSX/MFI realiza el preprocesamiento de datos, como la traducción de EBCDIC a ASCII. También realiza tareas más complejas, como la conversión de flujos de datos exclusivos de computadoras centrales, como IBM Advanced Function Presentation (AFP) y Xerox Line Conditioned Data Stream (LCDS), en flujos de datos más comunes de visualización e impresión, como el lenguaje de comandos de impresora (PCL) y el PDF.

   Durante el período de mantenimiento del LRS PageCenter X, el LRS conserva la cola de salida y VPSX/MFI sirve de respaldo para la cola de salida. El LRS VPSX/MFI conecta y envía la salida al LRS PageCenter X mediante el protocolo. LRS/Queue LRS/Queue realiza un intercambio de información sobre la preparación y la finalización de los trabajos para garantizar que se produzca la transferencia de datos.

   Notas:

Para obtener más información sobre los datos de impresión que se transmiten desde Rocket Software Print Exit a LRS/Queue los mecanismos de procesamiento por lotes de mainframe VPSX/MFI compatibles con el LRS, consulte Captura de datos de impresión en la sección de información adicional.

El LRS VPSX/MFI puede realizar comprobaciones de estado a nivel de flota de impresoras. Para obtener más información, consulte Printer-fleet health checks (Comprobaciones de estado de la flota de impresoras) en la sección Additional information (Información adicional) de este patrón.

5. La solución de administración de salida LRS PageCenter X se implementa en Amazon EC2 y sus datos operativos se almacenan en Amazon FSx for Windows File Server. LRS PageCenter X proporciona un sistema central de gestión de informes de todos los archivos importados a LRS PageCenter X y permite a todos los usuarios acceder a los archivos. Los usuarios pueden ver el contenido de un archivo específico o realizar búsquedas de criterios coincidentes en varios archivos.

   El LRS/NetX componente es un servidor de aplicaciones web multiproceso que proporciona un entorno de ejecución común para la aplicación LRS PageCenter X y otras aplicaciones LRS. El componente LRS/Web Connect está instalado en el servidor web y proporciona un conector desde el servidor web al servidor de aplicaciones LRS/NetX web.
6. El LRS PageCenter X proporciona almacenamiento para los objetos del sistema de archivos. Los datos operativos del LRS PageCenter X se almacenan en Amazon FSx for Windows File Server.
7. AWS Managed Microsoft AD lleva a cabo la autenticación y la autorización de la administración de la producción con LRS/DIS.

> **Note**
>
> La solución de destino no suele requerir cambios en la aplicación para adaptarse a los lenguajes de formato de mainframe, como IBM AFP o Xerox LCDS.

Arquitectura de infraestructura de AWS

El diagrama siguiente muestra una arquitectura de infraestructura de AWS segura y de alta disponibilidad para una carga de trabajo de administración de la producción de mainframe.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El programador de lotes inicia el proceso por lotes y se implementa EC2 en Amazon en varias zonas de disponibilidad para una alta disponibilidad (HA).

> **Note**
>
> Este patrón no incluye la implementación del programador de lotes. Para obtener más información acerca de la implementación, consulte la documentación del proveedor de software del programador.

2. El trabajo por lotes dela computadora central (escrito en un lenguajes de programación como JCL o COBOL) utiliza la lógica empresarial básica para procesar y generar la producción de impresión, como extractos de facturación, tarjetas de identificación y extractos de préstamos. El trabajo por lotes se implementa en Amazon en EC2 dos zonas de disponibilidad para alta disponibilidad. Utiliza la API Print Exit de Rocket Software para enrutar la salida de impresión al LRS VPSX/MFI para el preprocesamiento de los datos.
3. El servidor de VPSX/MFI impresión LRS se implementa en Amazon en dos zonas EC2 de disponibilidad para HA (par redundante activo-en espera). Utiliza Amazon EBS como almacén de datos operativos. El Network Load Balancer realiza una comprobación del estado de las instancias VPSX/MFI EC2 LRS. Si una instancia activa está en mal estado, el equilibrador de carga dirige el tráfico a las instancias activas en espera de la otra zona de disponibilidad. Las solicitudes de impresión se conservan en la cola de trabajos del LRS de forma local en cada una de las instancias. EC2 En caso de producirse un error, se debe reiniciar la instancia errónea antes de que los servicios de LRS puedan reanudar el procesamiento de la solicitud de impresión.

> **Note**
>
> El LRS también VPSX/MFI puede realizar comprobaciones de estado a nivel de flota de impresoras. Para obtener más información, consulte Printer-fleet health checks (Comprobaciones de estado de la flota de impresoras) en la sección Additional information (Información adicional) de este patrón.

4. La administración de salida del LRS PageCenter X se implementa en Amazon en EC2 dos zonas de disponibilidad para HA (par redundante activo-en espera). Utiliza Amazon FSx for Windows File Server como almacén de datos operativos. Si una instancia activa se encuentra en mal estado, el balanceador de cargas comprueba el estado de las instancias LRS PageCenter X y dirige el tráfico a las EC2 instancias en espera de la otra zona de disponibilidad.

5. Un Network Load Balancer proporciona un nombre DNS para integrar el VPSX/MFI servidor LRS con LRS X. PageCenter

> **Note**
>
> El LRS PageCenter X admite un balanceador de carga de capa 4.

6. LRS PageCenter X utiliza Amazon FSx for Windows File Server como almacén de datos operativo implementado en dos zonas de disponibilidad para alta disponibilidad. LRS PageCenter X solo entiende los archivos que se encuentran en el recurso compartido de archivos, no en una base de datos externa.
7. AWS Managed Microsoft AD se utiliza con LRS/DIS para realizar la autenticación y la autorización del flujo de trabajo de administración de resultados. Para obtener más información, consulte Print output authentication and authorization (Autenticación y autorización de la producción de impresión) en la sección Additional information (Información adicional).

Tools (Herramientas)

Servicios de AWS

- AWS Directory Service para Microsoft Active Directory permite que las cargas de trabajo compatibles con un directorio y los recursos de AWS utilicen Active Directory administrado en la nube de AWS.
- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento a nivel de bloques para utilizarlos con instancias de Amazon Elastic Compute Cloud (Amazon). EC2
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos. Por ejemplo, puede distribuir el tráfico entre EC2 instancias, contenedores y direcciones IP de Amazon en una o más zonas de disponibilidad. Este patrón utiliza un equilibrador de carga de red.
- Amazon FSx proporciona sistemas de archivos que admiten los protocolos de conectividad estándares del sector y ofrecen alta disponibilidad y replicación en todas las regiones de AWS. Este patrón usa Amazon FSx for Windows File Server.

- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.

Otras herramientas

- El software LRS PageCenter X proporciona una solución escalable de administración de contenido de documentos e informes que ayuda a los usuarios a obtener el máximo valor de la información mediante funciones automatizadas de indexación, cifrado y búsqueda avanzada.
- La LRS VPSX/MFI (interfaz Micro Focus), desarrollada conjuntamente por LRS y Rocket Software, captura la salida de una bobina JES de Rocket Software y la envía de forma fiable a un destino de impresión específico.
- LRS/Queue is a transmission agent that's TCP/IP based. LRS VPSX/MFI uses LRS/Queuepara recopilar o capturar datos de impresión a través de la interfaz de programación JES Print Exit de Rocket Software.
- LRS Directory Integration Server (LRS/DIS) es un directorio de integración que se utiliza para la autenticación y la autorización durante el flujo de trabajo de impresión.
- Rocket Enterprise Server es un entorno de implementación de aplicaciones para aplicaciones de mainframe. Proporciona el entorno en tiempo de ejecución para las aplicaciones de mainframe que se migran o crean con cualquier versión de Rocket Enterprise Developer.

Epics

Configuración del tiempo de ejecución de Rocket e implementación de una aplicación por lotes para mainframe

Tarea	Descripción	Habilidades requeridas
Configure el tiempo de ejecución e implemente una aplicación de demostración.	Para configurar Rocket Enterprise Server en Amazon EC2 e implementar la aplicación de BankDemo demostración de Rocket Software, siga las instrucciones de la guía de usuario de AWS Mainframe Modernization.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	La BankDemo aplicación es una aplicación por lotes para mainframe que crea y, a continuación, inicia la impresión.	

Configurar un servidor de impresión LRS en Amazon EC2

Tarea	Descripción	Habilidades requeridas
Crea una instancia de Amazon EC2 Windows.	Para lanzar una instancia de Amazon EC2 Windows, sigue las instrucciones de Lanzar una EC2 instancia de Amazon en la EC2 documentación de Amazon. Utilice el mismo nombre de host que utilizó para la licencia de producto de LRS. La instancia debe cumplir los siguientes requisitos de hardware y software para LRS VPSX/MFI: • CPU: doble núcleo • RAM: 16 GB • Unidad: 500 GB • EC2 Instancia mínima: `m5.xlarge` • Sistema operativo Windows • Software: Internet Informati on Services (IIS) o Apache	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Note Los requisitos de hardware y software anteriores están pensados para una flota de impresoras pequeña (entre 500 y 1000). Para conocer todos los requisito s, consulte a sus personas de contacto en LRS y AWS. 1. Al crear la instancia de Windows, confirme que el EC2 nombre de host es el mismo que se utilizó para la licencia del producto LRS. 2. Conéctate a tu EC2 instancia siguiendo las instrucciones del paso 2: Conéctate a tu instancia en la EC2 documentación de Amazon. 3. En el menú de Windows Start (Inicio), busque y abra Server Manager (Administ rador de servidores). 4. En Server Manager, seleccione Dashboard (Panel de control), Quick Start (Inicio rápido), Add	

Tarea	Descripción	Habilidades requeridas
	roles and features(Agregar funciones y características) y, a continuación, Server roles (Roles de nivel de servidor). 5. En Funciones de servidor, selecciona WebServer (IIS) y, a continuación, seleccion a Desarrollo de aplicacio nes. 6. En Desarrollo de aplicacio nes, seleccione la casilla de verificación CGI. 7. Para instalar CGI, siga las instrucciones del asistente en Add roles and features (Agregar roles y caracterí sticas) de Windows Server Manager. 8. Abra el puerto 5500 en el firewall de Windows de la EC2 instancia para LRS/ Queue comunicarse.	

Tarea	Descripción	Habilidades requeridas
Instale LRS VPSX/MFI en la EC2 instancia.	1. Conéctese a su EC2 instancia. 2. Abra el enlace a la página de descarga del producto que se muestra en el mensaje de correo electrónico de LRS que habrá recibido. **Note** Los productos de LRS se distribuyen mediante transferencia de archivos electrónica (EFT). 3. Descargue LRS VPSX/MFI y descomprima el archivo (carpeta predeterminada:). `c:\LRS` 4. Para instalar LRS VPSX/MFI, inicie el instalador de producto de LRS desde la carpeta descomprimida. 5. En el menú Select Feature (Seleccionar característica), seleccione VPSX® Server y, a continuación, Next (Siguiente) para iniciar el proceso de instalación. Cuando se complete la instalación, recibirá un mensaje de confirmación.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Instale LRS/Queue.	1. Conéctate a tu EC2 instancia de Rocket Enterprise Server. 2. Abra el enlace a la página de descarga del producto LRS que se incluye en el mensaje de correo electrónico de LRS que habrá recibido, descargue LRS/Queue y, a continuación, descomprima el archivo. 3. Vaya a la ubicación en la que descargó los archivos y, a continuación, inicie el instalador de producto de LRS para instalar LRS/Queue. 4. Siga las instrucciones del instalador de producto de LRS para completar el proceso de instalación.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Instale LRS/DIS.	El LRS/DIS producto suele estar incluido en la instalación del LRS VPSX. Sin embargo, si LRS/DIS no se instaló junto con el LRS VPSX, siga los siguientes pasos para instalarlo: 1. Conéctese a su VPSX/MFI EC2 instancia de LRS. 2. Abra el enlace a la página de descarga del producto LRS que se incluye en el mensaje de correo electrónico de LRS que habrá recibido, descargue LRS/DIS y, a continuación, descomprima el archivo. 3. Vaya a la ubicación en la que descargó los archivos y, a continuación, inicie el instalador de producto de LRS. 4. En el instalador de producto de LRS, amplíe LRS Misc Tools, seleccione LRS DIS y, a continuación, Next (Siguiente). 5. Siga el resto de las instrucciones del instalador del producto de LRS para completar el proceso de instalación.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Crear un grupo de destino.	Cree un grupo de destino siguiendo las instrucciones de Create a target group for your Network Load Balancer (Crear un grupo de destino para el equilibrador de carga de red). Al crear el grupo de destino, registre la VPSX/MFI EC2 instancia de LRS como destino: 1. En la página Especific ar detalles del grupo, seleccione un Tipo de destino y luego, Instancias. 2. En Protocol, seleccione TCP. 3. En Puerto, seleccione 5500. 4. En la página Registrar destinos, en la sección Instancias disponibles, seleccione la instancia de LRS. VPSX/MFI EC2	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Crear un equilibrador de carga de red.	Para crear el equilibrador de carga de red, siga las instrucciones de la documentación de Elastic Load Balancing (Equilibrio de carga elástico). Su Network Load Balancer dirige el tráfico de Rocket Enterprise Server a la instancia de VPSX/MFI EC2 LRS. Al crear el equilibrador de carga de red, elija los valores siguientes en la página Listeners and Routing (Oyentes y enrutamiento): 1. En Protocol, seleccione TCP. 2. En Puerto, seleccione 5500. 3. En Default action (Acción predeterminada), seleccione Forward to (Reenviar a) para el grupo de destino que ha creado.	Arquitecto de la nube

Integre Rocket Enterprise Server con un VPSX/MFI de LRS/Queue LRS

Tarea	Descripción	Habilidades requeridas
Configure Rocket Enterprise Server para la integración. LRS/Queue	1. Conéctate a tu EC2 instancia de Rocket Enterprise Server siguiendo	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	las instrucciones de la EC2 documentación de Amazon. 2. En el menú Inicio de Windows, abra la interfaz de usuario de administr ación de Rocket Enterprise Server. 3. En la barra de menús, seleccione NATIVE. 4. En el panel de navegació n, seleccione Directory Server y, a continuación, BANKDEMO para su región de Enterprise Server. 5. En General, busque el panel de navegació n izquierdo, despláces e hacia abajo hasta la sección Additional para configurar las variables del entorno (`LRSQ_ADDR ESS` , `LRSQ_PORT` , `LRSQ_COMMAND`) de modo que apunten a LRSQ. • Para LRSQ_ADDRESS, escriba la dirección IP o el nombre DNS del equilibrador de carga de red que creó anteriorm ente. • Para LRSQ_PORT, especifique VPSX LRSQ Listener Port (5500).	

Tarea	Descripción	Habilidades requeridas
	• Para LRSQ_COMMAND, especifique la ubicación de la ruta del ejecutable de LRSQ. **Note** Actualmente, LRS admite un límite máximo de 50 caracteres para los nombres de DNS. Si el nombre DNS tiene más de 50 caractere s, puede utilizar la dirección IP del equilibrador de carga de red como alternativa.	

Tarea	Descripción	Habilidades requeridas
Configura Rocket Enterprise Server para la VPSX/MFI integración con LRS.	1. Copie la `VPSX_MFI_R2` carpeta del VPSX/MFI instalador del LRS a la ubicación del servidor Rocket Enterprise en. `C\BANKDEMO\print` 2. Conéctate a tu EC2 instancia de Rocket Enterprise Server siguiendo las instrucciones de la EC2 documentación de Amazon. 3. En el menú Inicio de Windows, abra la interfaz de usuario de administración de Rocket Enterprise Server. 4. En la barra de menús, seleccione NATIVE. 5. En el panel de navegación, seleccione Directory Server y, a continuación, BANKDEMO. 6. En BANKDEMO, seleccione JES. 7. En JES Program Path, agregue la ruta `DLL(VPSX_MFI_R2)` de `C\BANKDEMO\print` .	Arquitecto de la nube

Configurar la cola de impresión y los usuarios de impresión

Tarea	Descripción	Habilidades requeridas
Asocie el módulo OpenText Micro Focus Print Exit al proceso de ejecución del servidor de la impresora por lotes de Micro Focus Enterprise Server.	1. Conéctate a tu EC2 instancia de Rocket Enterprise Server siguiendo las instrucciones de la EC2 documentación de Amazon. 2. En el menú Inicio de Windows, abra la interfaz de usuario de administración de Rocket Focus Enterprise Server. 3. En la barra de menús, seleccione NATIVE. 4. En el panel de navegación, seleccione Directory Server y, a continuación, BANKDEMO. 5. En BANKDEMO, seleccione JES y desplácese hacia abajo hasta Printers (Impresoras). 6. En Impresoras, asocie el módulo Print Exit de Rocket Software (LRSPRTE6 para Batch) al proceso de ejecución del servidor (SEP) de la impresora por lotes de Rocket Enterprise Server. Esto permite enrutar la salida de impresión a LRS VPSX/MFI.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Para obtener más información sobre la configuración, consulte Uso de la salida en la documentación de OpenText Micro Focus.	

Tarea	Descripción	Habilidades requeridas
Cree una cola de salida de impresión en LRS VPSX/MFI e intégrela con LRS X. PageCenter	1. Conéctese a su VPSX/MFI EC2 instancia de LRS. 2. En el menú Start (Inicio) de Windows, abra VPSX Web Interface. 3. En el panel de navegación, seleccione Printers (Impresoras). 4. Seleccione Add (Agregar) y, después, Add Printer (Agregar impresora). 5. En la página Printer Configuration (Configuración de la impresora), busque Printer Name (Nombre de impresora) y especifique Local. 6. Para el ID de VPSX, introduzca. VPS1 7. Para CommType, seleccione TCPIP/LRSQ. 8. En Host/Dirección IP, introduzca la dirección IP del Network Load Balancer que se encuentra al frente de las instancias LRS X. PageCenter EC2 9. Para Remote port (Puerto remoto), especifique 5800. 10. En Remote Queue, introduzca el nombre de la carpeta de documentos del LRS PageCenter X	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	en la que se almacenará la salida. 11. Elija Agregar.	

Tarea	Descripción	Habilidades requeridas
Cree un usuario de impresión en LRS VPSX/MFI.	1. Conéctese a su VPSX/MFI EC2 instancia de LRS. 2. En el menú Start (Inicio) de Windows, abra VPSX Web Interface. 3. En el panel de navegación, seleccione Security y, a continuación, la opción Users (Usuarios). 4. En la columna Nombre de usuario, seleccione admin y, a continuación, seleccione Copiar. 5. En la ventana Mantenimiento del perfil de usuario, en Nombre de usuario, introduzca un nombre de usuario (por ejemplo, PrintUser). 6. En Descripción, escriba una descripción breve (por ejemplo, Usuario para impresión de prueba). 7. Seleccione Update (Actualizar). Esto crea un usuario de impresión (por ejemplo, PrintUser). 8. En el panel de navegación, busque User y seleccione el nuevo usuario que ha creado.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	9. En el menú Command (Comandos), seleccione Security (Seguridad). 10. En la página Reglas de seguridad, seleccione todas las opciones de seguridad de la impresora y seguridad laboral aplicables y, a continuación, seleccione Guardar. 11. Para agregar el nuevo usuario de impresión al grupo Administrator, acceda al panel de navegación, seleccione Security y, a continuación, Configure (Configurar). 12. En la ventana Configuración de seguridad, añada su nuevo usuario de impresión a la columna Administrador.	

Configurar un servidor LRS PageCenter X en Amazon EC2

Tarea	Descripción	Habilidades requeridas
Crea una instancia de Amazon EC2 Windows.	Para lanzar una instancia de Amazon EC2 Windows, sigue las instrucciones del paso 1: lanzar una instancia de la EC2 documentación de Amazon. Utilice el mismo nombre de	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	host que utilizó para la licencia de producto de LRS. La instancia debe cumplir los siguientes requisitos de hardware y software para LRS PageCenter X: • CPU: doble núcleo • RAM: 16 GB • Unidad: 500 GB • EC2 Instancia mínima: `m5.xlarge` • Sistema operativo Windows • Software: IIS o Apache **Note** Los requisitos de hardware y software anteriores están pensados para una flota de impresoras pequeña (entre 500 y 1000). Para conocer todos los requisito s, consulte a sus personas de contacto en LRS y AWS. 1. Al crear la instancia de Windows, confirme que el EC2 nombre de host es el	

Tarea	Descripción	Habilidades requeridas
	mismo que se utilizó para la licencia del producto LRS. 2. Conéctate a tu EC2 instancia siguiendo las instrucciones de la EC2 documentación de Amazon. 3. En el menú de Windows Start (Inicio), busque y abra Server Manager (Administ rador de servidores). 4. En Server Manager, seleccione Dashboard (Panel de control), Quick Start (Inicio rápido), Add roles and features(Agregar funciones y características) y, a continuación, Server roles (Roles de nivel de servidor). 5. En Funciones de servidor, elija WebServer (IIS) y, a continuación, Desarrollo de aplicaciones. 6. En Desarrollo de aplicacio nes, seleccione la casilla de verificación CGI. 7. Para instalar CGI, siga las instrucciones del asistente en Add roles and features (Agregar roles y caracterí sticas) de Windows Server Manager.	

Tarea	Descripción	Habilidades requeridas
	8. Abre el puerto 5800 para el TCP/IP tráfico entrante en el firewall de Windows de la EC2 instancia. El LRS VPSX usa el TCPIP/LRSQ protocolo del puerto 5800 para comunicarse con el LRS X. PageCenter	

Tarea	Descripción	Habilidades requeridas
Instale PageCenter LRS X en la instancia. EC2	1. Conéctese a su EC2 instancia. 2. Abra el enlace a la página de descarga del producto que se muestra en el mensaje de correo electrónico de LRS que habrá recibido. **Note** Los productos de LRS se distribuyen mediante transferencia de archivos electrónica (EFT). 3. Descarga LRS PageCenter X y descomprime el archivo (carpeta predeterminada:`c:\LRS`). 4. Para instalar LRS PageCenter X, inicie el instalador de productos LRS desde la carpeta descomprimida. 5. En el menú Seleccionar funciones, seleccione PageCenterX y, a continuación, elija Siguiente para iniciar el proceso de instalación. Cuando se complete la instalación,	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	recibirá un mensaje de confirmación.	

Tarea	Descripción	Habilidades requeridas
Instale LRS/DIS.	El LRS/DIS producto suele incluirse en la instalación del LRS VPSX. Sin embargo, si LRS/DIS no se instaló junto con el LRS VPSX, siga los siguientes pasos para instalarl o: 1. Conéctese a su EC2 instancia LRS PageCenter X. 2. Abra el enlace a la página de descarga del producto LRS que se incluye en el correo electrónico de LRS que habrá reqcibido , descargue LRS/DIS y, a continuación, descomprima el archivo. 3. Vaya a la ubicación en la que descargó los archivos y, a continuación, inicie el instalador de producto de LRS. 4. En el instalador de producto de LRS, amplíe LRS Misc Tools, seleccione LRS DIS y, a continuación, Next (Siguiente). 5. Siga el resto de las instrucci ones del instalador del producto de LRS para completar el proceso de instalación.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Crear un grupo de destino.	Cree un grupo de destino siguiendo las instrucciones de Create a target group for your Network Load Balancer (Crear un grupo de destino para el equilibrador de carga de red). Al crear el grupo objetivo, registre la EC2 instancia LRS PageCenter X como destino: 1. En la página Especific ar detalles del grupo, seleccione un Tipo de destino y luego, Instancias. 2. En Protocol, seleccione TCP. 3. En Puerto, seleccione 5800. 4. En la página Registrar destinos, en la sección Instancias disponibles, seleccione la instancia LRS PageCenter X. EC2	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Crear un equilibrador de carga de red.	Para crear el equilibrador de carga de red, siga las instrucciones de la documentación de Elastic Load Balancing (Equilibrio de carga elástico). Su Network Load Balancer enruta el tráfico de LRS VPSX/MFI a la instancia de PageCenter LRS X. EC2 Al crear el equilibrador de carga de red, elija los valores siguientes en la página Listeners and Routing (Oyentes y enrutamiento): 1. En Protocol, seleccione TCP. 2. En Puerto, seleccione 5800. 3. En Default action (Acción predeterminada), seleccione Forward to (Reenviar a) para el grupo de destino que ha creado.	Arquitecto de la nube

Configure las funciones de administración de salida en LRS X PageCenter

Tarea	Descripción	Habilidades requeridas
Habilite la función de importación en LRS X. PageCenter	Puede utilizar la función de importación de LRS PageCenter X para reconocer las salidas que llegan al LRS PageCenter X mediante	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	criterios como el nombre del trabajo o el ID del formulario. A continuación, puede enrutar los resultados a carpetas específicas del LRS X. PageCenter Para habilitar la importación, siga estos pasos: 1. Conéctate a tu EC2 instancia LRS PageCenter X siguiendo las instrucciones de la EC2 documentación de Amazon. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En Folder Explorer (Explorador de carpetas), seleccione Admin. 4. En la página Configuration, seleccione Advanced, Import parameter (Parámetro de importación). 5. En la sección Import parameter, active la casilla Advanced Import (Importación avanzada). 6. Para confirmar los cambios, seleccione Update (Actualizar).	

Tarea	Descripción	Habilidades requeridas
Configure la política de conservación de documentos.	LRS PageCenter X utiliza una política de retención de documentos para decidir durante cuánto tiempo se debe conservar un documento en LRS X. PageCenter Para configurar la política de conservación de documentos, siga los pasos siguientes: 1. Conéctese a su EC2 instancia LRS PageCenter X. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En Folder Explorer (Explorador de carpetas), seleccione Admin. 4. En la página de administración, elija List/General Administrador del grupo de archivos y, a continuación, elija Política de retención. 5. En la sección Retention policy, seleccione Add para crear una política de conservación. 6. En la página Retention Policy Information, especifique un nombre en Retention policy name, una descripción en Description y el	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	periodo de retención en Document retention. 7. Seleccione Ok (Aceptar) para guardar la nueva política.	

Tarea	Descripción	Habilidades requeridas
Cree una regla para enrutar el documento de salida a una carpeta específica de LRS X. PageCenter	En LRS PageCenter X, Destination determina la ruta de la carpeta a la que se enviará la salida cuando Report Definition invoque este destino. Para este ejemplo, cree una carpeta basada en la carpeta de Form ID en la definición del informe y guarde el resultado en esa carpeta. 1. Conéctese a su EC2 instancia LRS PageCenter X. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En Folder Explorer (Explorador de carpetas) , seleccione Admin, Advanced Import (Importac ión avanzada) y Destination (Destino). 4. En la sección Destination, seleccione Add (Agregar) para abrir el formulario Destination Maintenan ce (Mantenimiento del destino). 5. En el formulario de Destination Maintenance, especifique los valores siguientes:	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	• Destination name: Form (Formulario) • Description: Una descripción del destino, como Form-based folder structure (Estructura de carpeta basada en formularios) • Destination type: Folder (Carpeta) • Parámetros de carpeta: ruta de importación de la carpeta (la ruta de la carpeta que se creará en PageCenter X cuando llegue el documento; por ejemplo, la ruta **`/Test/&FORM/&IMPORTDATE/&IMPORTTIME`** creará una **`Test`** carpeta base, una subcarpeta basada en el nombre del ID del formulario, una subcarpeta en función de la fecha de importación y **`STD`**, por último, una subcarpeta en función de la hora de importación) • Document name (Nombre del documento): El nombre dinámico que se asigna a un documento cuando se guarda en la carpeta.	

Tarea	Descripción	Habilidades requeridas
	6. En la lista desplegable, seleccione una política de conservación. A modo de ejemplo, seleccione Year1 para retener el documento durante 1 año. 7. Seleccione Ok (Aceptar) para guardar los cambios.	

Tarea	Descripción	Habilidades requeridas
Cree una definición de informe.	1. Conéctese a su EC2 instancia LRS PageCenter X. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En Folder Explorer (Explorador de carpetas) , seleccione Admin, Advanced Import (Importación avanzada), Report Definition (Definición de informe) y, a continuación, Add (Agregar). 4. En la página Report definition maintenance (Mantenimiento de la definición del informe), busque la pestaña General y especifique el Report Definition Name (nombre de la definición de informe). 5. En la pestaña General, busque Fields (Campos), donde puede especificar criterios de selección como Job Name (Nombre del trabajo), Form (Formulario), Class (Clase) y Author (Autor). Así, por ejemplo, puede especificar un Job Name de MFIDEMO. El valor Job Name será el nombre del trabajo por lotes	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	que generará la salida de impresión. 6. En la pestaña Destination, busque Available Destination (Destino disponible) y seleccione el destino creado anteriormente (Form). 7. Seleccione Add (Agregar) para agregar el destino del Form (Formulario) como Assigned destination (Destino asignado). **Note** Este ejemplo incluye una definición de informe en la que una salida generada por el MFIDEMO y enviada al LRS PageCenter X se guarda en la estructura de carpetas definida en la definición de destino.	

Configurar la autenticación y autorización para administración de la producción

Tarea	Descripción	Habilidades requeridas
Cree un dominio de AWS Managed Microsoft AD con usuarios y grupos.	1. Para crear un directorio en AWS Managed Microsoft AD, siga las instrucciones de Create your AWS Managed Microsoft AD Directory. 2. Para implementar una EC2 instancia (administrador de Active Directory) e instalar herramientas de Active Directory para administrar su AD de Microsoft administrado por AWS, siga las instrucciones del paso 3: Implementar una EC2 instancia para administrar su AD de Microsoft administrado por AWS. 3. Para conectarte a tu EC2 instancia, sigue las instrucciones de la EC2 documentación de Amazon. **Note** Cuando te conectes a la EC2 instancia, en la ventana de seguridad de Windows, introduce las credenciales de administrador del directorio que	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	creaste en el paso 1. 4. Una vez que haya iniciado sesión, en el menú Inicio, bajo Herramientas administrativas de Windows, seleccione Usuarios y equipos de Active Directory. 5. Para crear un usuario de impresión en el dominio de Active Directory, siga las instrucciones de Crear un usuario.	
Une las EC2 instancias a un dominio de Microsoft AD administrado por AWS.	Une las EC2 instancias LRS VPSX/MFI y LRS PageCenter X a tu dominio de AWS Managed Microsoft AD de forma automática (documentación del AWS Knowledge Center) o manualmente (documentación de AWS Directory Service).	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Configure e integre LRS/DIS con AWS Managed Microsoft AD para la EC2 instancia LRS PageCenter X.	1. Conéctese a su EC2 instancia LRS PageCenter X. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En Folder Explorer (Explorador de carpetas), seleccione Admin. 4. En la página Configuration, busque la sección Security Parameters y, en Security Type, seleccione LRS/DIS. 5. Especifique sus preferenc ias para el resto de las opciones en la sección Parámetros de seguridad. 6. En el menú Inicio de Windows, abra la carpeta PageCenterX, seleccione Server Start y, a continuac ión, seleccione Server Stop. 7. Inicie sesión en LRS PageCenter X con su nombre de usuario y contraseña de Active Directory.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Configure un grupo de importación para importar la salida de LRS VPSX a LRS X. PageCenter	1. Conéctese a su EC2 instancia LRS PageCenter X. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En Folder Explorer (Explorador de carpetas), seleccione Admin, Security admin y Groups. 4. En la sección “Groups”, seleccione Add para abrir el formulario Group preferenc e. 5. En el formulario Group preference, especifique los valores de Group name y Description. 6. Expanda General options y, a continuación, seleccione la casilla Import. 7. Seleccione Ok (Aceptar) para guardar los cambios.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Agregue una regla de seguridad a Import group (Grupo de importación).	1. Abra el menú contextual (haga clic con el botón derecho) de Import group. 2. Seleccione Advance (Avanzado)y, a continuación, Security. 3. En la sección Security (Seguridad), seleccione Import (Importar) y marque la casilla de verificación Subfolder (Subcarpeta). 4. Seleccione Apply (Aplicar) para guardar los cambios.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Cree un usuario en LRS PageCenter X para importar la salida desde LRS VPSX/MFI.	Al crear un usuario en LRS PageCenter X para importar la salida, el nombre de usuario debe ser el mismo que el ID de VPSX de la cola de salida de impresión en LRS VPSX/MFI. En este ejemplo, el ID de VPSX es. VPS1 1. Conéctese a su EC2 instancia LRS PageCenter X. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En Folder Explorer (Explorador de carpetas), seleccione Admin, Security admin y User. 4. Seleccione Add (Agregar) para abrir el formulario User profile maintenance (Mantenimiento del perfil de usuario). 5. En Mantenimiento del perfil de usuario, introduzca VPS1el nombre de usuario.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Agregue el usuario de importación de LRS PageCenter X al grupo de importación exclusiva.	Para conceder los permisos necesarios para la importación de documentos de LRS VPSX a LRS PageCenter X, haga lo siguiente: 1. Conéctese a su EC2 instancia LRS PageCenter X. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En Folder Explorer (Explorador de carpetas), seleccione Admin, Security admin y Groups. 4. En la sección Groups, abra el menú contextual (haga clic con el botón derecho) para el grupo Import only (Solo de importación) y, a continuación, seleccione Advance, Security. 5. En la página Registros de seguridad de carpetas (ImportOnly), seleccione la pestaña Usuario. 6. En la pestaña Usuario, en Nombre, seleccione el usuario VPS1en la lista desplegable y elija Aplicar.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Configure LRS/DIS con AWS Managed Microsoft AD para la VPSX/MFI EC2 instancia de LRS.	1. Conéctese a su VPSX/MFI EC2 instancia de LRS. 2. En el menú Start (Inicio) de Windows, abra VPSX Web Interface. 3. En el panel de navegación, seleccione Security y, a continuación, la opción Configure (Configurar). 4. En la página Security Configuration, busque la sección Security Parameters y, en Security Type, seleccione LRS/DIS (External). 5. Especifique sus preferencias para el resto de las opciones en la sección Parámetros de seguridad. 6. En el menú Start (Inicio) de Windows, abra la carpeta LRS Output Management, seleccione Server Start (Inicio del servidor) y, a continuación, Server Stop. 7. Inicie sesión en LRS VPSX/MFI con su nombre de usuario y contraseña de Active Directory.	Arquitecto de la nube

Configure Amazon FSx for Windows File Server como almacén de datos operativos para LRS X PageCenter

Tarea	Descripción	Habilidades requeridas
Cree un sistema de archivos para LRS X. PageCenter	Para utilizar Amazon FSx for Windows File Server como almacén de datos operativo para LRS PageCenter X en un entorno Multi-AZ, siga las instrucciones del paso 1: Cree su sistema de archivos.	Arquitecto de la nube
Asigne el archivo compartido a la instancia de LRS X. PageCenter EC2	Para asignar el recurso compartido de archivos creado en el paso anterior a la EC2 instancia LRS PageCenter X, siga las instrucciones del paso 2: Asigne el recurso compartido de archivos a una EC2 instancia que ejecute Windows Server.	Arquitecto de la nube
Asigne el directorio de control y el directorio de carpetas maestras de LRS PageCenter X a la unidad compartida FSx de red Amazon.	1. Conéctate a tu EC2 instancia LRS PageCenter X siguiendo las instrucciones de la EC2 documentación de Amazon. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En Folder Explorer (Explorador de carpetas), seleccione Admin, Configuration. 4. En la página Configuration, seleccione Directories y,	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	a continuación, Control Directory (Directorio de control). 5. En Control Directories, especifique `\\FSx file share DNS name\share\cntl` . 6. En Master Folder Directory (Directorio de carpetas maestras), especifique `\\FSx file share DNS name\share\mstr` .	

Pruebe un flujo de trabajo de administración de la producción

Tarea	Descripción	Habilidades requeridas
Inicie una solicitud de impresión por lotes desde la BankDemo aplicación Rocket Software.	1. Abre el emulador de terminal 3270 en tu instancia de Rocket Enterprise Server EC2 . 2. Conéctese a la BankDemo aplicación ejecutando el comando `connect 127.0.0.1:9278` . 3. En la interfaz de línea de BankDemo comandos, para ID de usuario, escriba B0001. En Password (Contraseña), especifique una clave que no esté en blanco.	Ingeniero de pruebas

Tarea	Descripción	Habilidades requeridas
	4. Para la opción Request printed statement(s) (Solicitar extractos impresos), escriba X en la línea en blanco. 5. En la sección Send statement by (Enviar extracto por), para Mail, escriba Y (Sí) y, a continuación, pulse F10.	

Tarea	Descripción	Habilidades requeridas
Compruebe el resultado de impresión en el LRS X. PageCenter	1. Conéctate a tu EC2 instancia LRS PageCenter X siguiendo las instrucciones de la EC2 documentación de Amazon. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En el panel de navegación, abra la carpeta Test, la carpeta STD y, a continuación, la carpeta con la fecha de ejecución de la tarea, por ejemplo `08-03-2023` (MM-DD-AAAA). **Note** Es la misma estructura de carpetas que se define en la historia Cree una regla para enrutar el documento de salida a una carpeta específica en LRS X. PageCenter 4. Abra el archivo `formtest-STD.txt` . Ya puede ver el resultado impreso de un extracto de cuenta con columnas	Ingeniero de pruebas

Tarea	Descripción	Habilidades requeridas
	para Account No. (Número de cuenta), Description, Date, Amount (Importe) y Balance (Saldo). Para ver un ejemplo, consulte el archivo `batch_print_output` adjunto de este patrón.	

Recursos relacionados

- LRS
- Advanced Function Presentation data stream (Flujo de datos de presentación de funciones avanzadas) (Documentación de IBM)
- Flujo de datos condicionado por línea (LCDS) (documentación de Compart)
- Empowering Enterprise Mainframe Workloads on AWS with Micro Focus (Capacitación de cargas de trabajo de mainframe empresarial en AWS) (publicación de blog)
- Modernize your mainframe online printing workloads on AWS (Modernice las cargas de trabajo de impresión online de mainframe en AWS) (Recomendaciones de AWS)
- Modernize your mainframe batch printing workloads on AWS (Modernice las cargas de trabajo de impresión por lotes de mainframe en AWS) (Recomendaciones de AWS)

Información adicional

Consideraciones

Durante su proceso de modernización, podría considerar la posibilidad de utilizar una amplia variedad de configuraciones para los procesos en línea y por lotes de mainframe, así como para la producción que generan. Todos los clientes y proveedores que utilizan la plataforma de mainframe la han personalizado con requisitos particulares que afectan directamente a la impresión. Así, por ejemplo, su plataforma actual podría incorporar el flujo de datos AFP de IBM o las pantallas LCD de Xerox en el flujo de trabajo actual. Además, los caracteres de control de carro de mainframe y las palabras del comando de canal pueden afectar al aspecto de la página impresa y requerir un manejo

especial. Como parte del proceso de planificación de la modernización, le recomendamos evaluar y comprender las configuraciones de su entorno de impresión específico.

Captura de datos de impresión

Rocket Software Print Exit pasa la información necesaria para que LRS VPSX/MFI procese eficazmente el archivo de bobina. La información consta de campos incluidos en los bloques de control correspondientes, como los siguientes:

- JOBNAME
- OWNER (USERID)
- DESTINATION
- FORM
- FILENAME
- WRITER

El LRS VPSX/MFI admite los siguientes mecanismos de procesamiento por lotes de ordenadores centrales para capturar datos de Rocket Enterprise Server:

- print/spool Procesamiento COBOL POR LOTES mediante sentencias z/OS JCL SYSOUT estándar. DD/OUTPUT
- print/spool Procesamiento por lotes de COBOL mediante sentencias z/OS JCL CA-SPOOL SUBSYS DD estándar.
- IMS/COBOL print/spoolprocesamiento mediante la interfaz CBLTDLI. Para obtener una lista completa de los métodos y ejemplos de programación compatibles, consulte la documentación de LRS que se incluye con la licencia del producto.

Comprobaciones de estado de la flota de impresoras

El LRS VPSX/MFI (LRS LoadX) puede realizar controles de estado exhaustivos, incluida la gestión de los dispositivos y la optimización operativa. La administración de dispositivos puede detectar un error en un dispositivo de impresión y dirigir la solicitud de impresión a una impresora en buen estado. Para obtener más información sobre las comprobaciones de estado exhaustivas de las flotas de impresoras, consulte la documentación de LRS que se incluye con la licencia del producto.

Autenticación y autorización de impresoras

LRS/DIS enables LRS applications to authenticate user IDs and passwords by using Microsoft Active Directory or a Lightweight Directory Access Protocol (LDAP) server. In addition to basic print authorization, LRS/DIStambién puede aplicar controles de seguridad de impresión de nivel granular en los siguientes casos de uso:

- Gestione quién puede examinar el trabajo de impresión.
- Gestione el nivel de navegación de los trabajos de otros usuarios.
- Gestione las tareas operativas, por ejemplo, la seguridad en el nivel de comandos, como retener o liberar, purgar, modificar, copiar y redirigir. La seguridad se puede configurar mediante el ID de usuario o el grupo, de forma similar a un grupo de seguridad de Active Directory o a un grupo LDAP.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Modernice las cargas de trabajo de impresión por lotes de mainframe AWS mediante Rocket Enterprise Server y LRS VPSX/MFI

Shubham Roy y Kevin Yung, Amazon Web Services

Abraham Rondon, Micro Focus

Guy Tucker, Levi, Ray and Shoup Inc

Resumen

Este patrón le muestra cómo modernizar las cargas de trabajo de impresión por lotes de mainframe críticas para la empresa en la nube de Amazon Web Services (AWS) mediante Rocket Enterprise Server como entorno de ejecución para una aplicación de mainframe modernizada y LRS VPSX/MFI (Micro Focus Interface) como servidor de impresión. El patrón se basa en el enfoque de modernización del mainframe a través de redefinir la plataforma. Con este enfoque, migra los trabajos por lotes de su mainframe a Amazon Elastic Compute Cloud (Amazon EC2) y migra su base de datos de mainframe, como IBM (DB2 forz/OS, to Amazon Relational Database Service (Amazon RDS). The authentication and authorization for the modernized print workflow is performed by AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD. The LRS Directory Information Server (LRS/DIS), integrada con AWS Managed Microsoft AD. Al modernizar sus cargas de trabajo de impresión por lotes, puede reducir los costos de infraestructura de TI, mitigar la carga técnica que supone el mantenimiento de los sistemas heredados, eliminar los silos de datos, aumentar la agilidad y la eficiencia con un DevOps modelo y aprovechar los recursos bajo demanda y la automatización en la nube de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una carga de trabajo de gestión de producción o impresión de mainframe
- Conocimientos básicos sobre cómo recompilar y entregar una aplicación de mainframe ejecutada en Rocket Enterprise Server (para obtener más información, consulte la hoja de datos de Rocket Enterprise Server en la documentación de Rocket).
- Conocimientos básicos de las soluciones y los conceptos de impresión en la nube de LRS
- Software y licencia de Rocket Enterprise Server (para obtener más información, póngase en contacto con el departamento de ventas de Rocket).

- VPSX/MFI, LRS/Queue, and LRS/DISSoftware y licencias de LRS (para obtener más información, póngase en contacto con el departamento de ventas de LRS).

> **Note**
>
> Para obtener más información sobre las consideraciones de configuración de las cargas de trabajo de administración de la producción de mainframe, consulte Consideraciones en la sección Información adicional de este patrón.

Versiones de producto

- Rocket Enterprise Server 6.0 (actualización de producto 7)
- LRS VPSX/MFI V1R3 o superior

Arquitectura

Pila de tecnología de origen

- Sistema operativo: IBM z/OS
- Lenguaje de programación: Common Business-Oriented Language (COBOL), Job Control Language (JCL) y Customer Information Control System (CICS)
- Base de datos: IBM DB2 for z/OS y Virtual Storage Access Method (VSAM)
- Seguridad: Resource Access Control Facility (RACF), CA Top Secret for z/OS y Access Control Facility 2 () ACF2
- Gestión de impresión y salida: productos de z/OS impresión para mainframes de IBM (IBM Tivoli Output Manager for z/OS, LRS y CA View)

Pila de tecnología de destino

- Sistema operativo: Microsoft Windows Server que se ejecuta en Amazon EC2
- Informática — Amazon EC2
- Lenguaje de programación: COBOL, JCL y CICS
- Bases de datos: Amazon RDS
- Seguridad: AWS Managed Microsoft AD

- Administración de impresión y producción: solución de impresión LRS en AWS
- Entorno de tiempo de ejecución de mainframe: Rocket Enterprise Server

Arquitectura de origen

El diagrama siguiente muestra una arquitectura de estado actual tipo para una carga de trabajo de administración de la producción de mainframe:

El diagrama muestra el siguiente flujo de trabajo:

1. Los usuarios llevan a cabo transacciones comerciales en un sistema de participación (SoE) que se basa en una aplicación CICS de IBM escrita en COBOL.
2. El SoE invoca el servicio de mainframe, que registra los datos de las transacciones comerciales en una base de datos system-of-records (SoR), como IBM DB2 for z/OS.
3. El SoR conserva los datos comerciales del SoE.
4. El programador de trabajos por lotes inicia un trabajo por lotes para generar resultados de impresión.
5. El trabajo por lotes extrae datos de la base de datos, formatea los datos de acuerdo con los requisitos comerciales y, a continuación, genera producción empresarial, como extractos de facturación, tarjetas de identificación o extractos de préstamos. Por último, el trabajo por lotes dirige la producción a la administración de la impresión para procesar y enviar los resultados en función de los requisitos empresariales.
6. La gestión de los resultados de producción recibe la producción de impresión del trabajo por lotes y, a continuación, la envía a un destino específico, como el correo electrónico, un archivo compartido que emplee un FTP seguro, una impresora física que use soluciones de impresión LRS (como se demuestra en este patrón) o IBM Tivoli.

Arquitectura de destino

El diagrama siguiente muestra una arquitectura para una carga de trabajo de administración de la producción de mainframe que se implementa en la nube de AWS:

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El programador de trabajos por lotes inicia un trabajo por lotes para generar la producción, como extractos de facturación, tarjetas de identificación o extractos de préstamos.
2. El trabajo por lotes del mainframe (rediseñado a Amazon EC2) utiliza el tiempo de ejecución de Rocket Enterprise Server para extraer datos de la base de datos de la aplicación, aplicar lógica empresarial a los datos, formatear los datos y, a continuación, enviarlos a un destino de impresión mediante Rocket Software Print Exit (documentación de Micro Focus).
3. La base de datos de la aplicación (un SoR que se ejecuta en Amazon RDS) conserva los datos para su impresión.
4. La solución de VPSX/MFI impresión LRS se implementa en Amazon EC2 y sus datos operativos se almacenan en Amazon Elastic Block Store (Amazon EBS). LRS VPSX/MFI utiliza el agente TCP/IP-based LRS/Queue de transmisión para recopilar datos de impresión a través de la API JES Print Exit de Rocket Software y entregar los datos a un destino de impresión específico.

> **Note**
>
> La solución de destino no suele requerir cambios en la aplicación para adaptarla a los lenguajes de formato de mainframe, como IBM Advanced Function Presentation (AFP) o Xerox Line Condition Data Stream (LCDS). Para obtener más información sobre el uso de Rocket Software para la migración y modernización de aplicaciones de mainframe en AWS, consulte la entrada en el blog Empowering Enterprise Mainframe Workloads on AWS with Micro Focus.

Arquitectura de infraestructura de AWS

El diagrama siguiente muestra una arquitectura de infraestructura de AWS segura y de alta disponibilidad para una carga de trabajo de administración de la producción de mainframe:

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El programador de lotes inicia el proceso por lotes y se implementa EC2 en Amazon en varias zonas de disponibilidad para una alta disponibilidad (HA).

> **Note**
>
> Este patrón no incluye la implementación del programador de lotes. Para obtener más información acerca de la implementación, consulte la documentación del proveedor de software del programador.

2. El trabajo por lotes de la computadora central (escrito en un lenguajes de programación como JCL o COBOL) utiliza la lógica empresarial básica para procesar y generar la producción de impresión, como extractos de facturación, tarjetas de identificación y extractos de préstamos. El trabajo se implementa en Amazon en dos zonas de EC2 disponibilidad para alta disponibilidad y utiliza Rocket Software Print Exit para enrutar los resultados de impresión a LRS VPSX/MFI para que los impriman los usuarios finales.
3. LRS VPSX/MFI usa un comando. TCP/IP-based LRS/Queue transmission agent to collect or capture print data from the Rocket Software JES Print Exit programming interface. Print Exit passes the necessary information to enable LRS VPSX/MFI to effectively process the spool file and dynamically build LRS/Queue A continuación, los comandos se ejecutan mediante una función estándar integrada de Rocket Software.

> **Note**
>
> Para obtener más información sobre los datos de impresión que se transmiten desde Rocket Software Print Exit a LRS/Queue los mecanismos de procesamiento por lotes de ordenadores centrales VPSX/MFI compatibles con el LRS, consulte Captura de datos de impresión en la sección de información adicional de este patrón.

4.
> **Note**
>
> Un Network Load Balancer proporciona un nombre DNS para integrar Rocket Enterprise Server con el LRS VPSX/MFI. : LRS VPSX/MFI supports a Layer 4 load balancer. The Network Load Balancer also does a basic health check on LRS VPSX/MFI y enruta el tráfico a los destinos registrados que están en buen estado.

5.
> **Note**
>
> El servidor de VPSX/MFI impresión LRS se implementa en Amazon en EC2 dos zonas de disponibilidad para alta disponibilidad y utiliza Amazon EBS como almacén de datos

operativos. El LRS VPSX/MFI admite los modos de servicio activo-activo y activo-pasivo. Esta arquitectura utiliza varios AZs en un par activo-pasivo como modo de espera activo y activo. El Network Load Balancer realiza una comprobación del estado de las VPSX/MFI EC2 instancias LRS y enruta el tráfico a las instancias en espera activas de la otra zona de disponibilidad si una instancia activa se encuentra en mal estado. Las solicitudes de impresión se conservan en la cola de trabajos del LRS de forma local en cada una de las instancias. EC2 En caso de recuperación, se debe reiniciar una instancia fallida para que los servicios de LRS reanuden el procesamiento de la solicitud de impresión. : LRS también VPSX/MFI puede realizar comprobaciones de estado a nivel de flota de impresoras. Para obtener más información, consulte Comprobaciones de estado de la flota de impresoras en la sección de Información adicional de este patrón.

6. AWS Managed Microsoft AD se integra LRS/DIS para realizar la autenticación y autorización del flujo de trabajo de impresión. Para obtener más información, consulte Autenticación y autorización de impresión en la sección de Información adicional de este patrón.
7. LRS VPSX/MFI utiliza Amazon EBS para el almacenamiento en bloque. Puede hacer copias de seguridad de los datos de Amazon EBS de EC2 las instancias activas en Amazon S3 como point-in-time instantáneas y restaurarlos en volúmenes de EBS activos en espera. Para automatizar la creación, retención y eliminación de instantáneas de volúmenes de Amazon EBS, puede usar Amazon Data Lifecycle Manager para establecer la frecuencia de las instantáneas automatizadas y restaurarlas en función de sus necesidades de RTO/RPO.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento a nivel de bloque para usarlos con instancias. EC2 Los volúmenes de EBS se comportan como dispositivos de bloques sin formatear. Puede montar estos volúmenes como dispositivos en sus instancias.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede usar Amazon EC2 para lanzar tantos o tan pocos servidores virtuales como necesite, y puede ampliarlos de manera horizontal o horizontal.
- Amazon Relational Database Service (Amazon RDS) es un servicio web que facilita la configuración, el funcionamiento y la escala de una base de datos relacional en la nube de AWS. Proporciona una capacidad rentable y de tamaño ajustable para una base de datos relacional y se ocupa de las tareas comunes de administración de bases de datos.

- AWS Directory Service para Microsoft Active Directory, también conocido como AWS Managed Microsoft AD, permite que las cargas de trabajo compatibles con un directorio y los recursos de AWS utilicen Microsoft Active Directory en la nube de AWS.

Otras herramientas

- LRS VPSX/MFI (Micro Focus Interface), una interfaz desarrollada conjuntamente por LRS y Rocket Software, captura la producción de una bobina de Rocket Enterprise Server JES y la entrega de forma fiable a un destino de impresión específico.
- El servidor de información de directorio LRS (LRS/DIS) se utiliza para la autenticación y la autorización durante el flujo de trabajo de impresión.
- TCP/IP-based LRS/Queue transmission agent is used by LRS VPSX/MFIpara recopilar o capturar datos de impresión a través de la interfaz de programación JES Print Exit de Rocket Software.
- Rocket Enterprise Server es un entorno de implementación de aplicaciones para aplicaciones de mainframe. Proporciona el entorno de ejecución para las aplicaciones de mainframe que se migran o crean con cualquier versión de Rocket Software Enterprise Developer.

Epics

Configura Rocket Enterprise Server en Amazon EC2 e implementa una aplicación por lotes para mainframe

Tarea	Descripción	Habilidades requeridas
Configure Rocket Enterpris e Server e implemente una aplicación de demostración.	Configure Rocket Enterpris e Server en Amazon y EC2, a continuación, despliegue la aplicación de BankDemo demostración de Rocket Software en Amazon EC2. La BankDemo aplicación es una aplicación por lotes para ordenadores centrales que crea y, a continuación, inicia la impresión.	Arquitecto de la nube

Configurar un servidor de impresión LRS en Amazon EC2

Tarea	Descripción	Habilidades requeridas
Obtenga una licencia de producto LRS para imprimir.	Para obtener una licencia de producto LRS para LRSVPSX/MFI, LRS/Queue, and LRS/DIS, póngase en contacto con el equipo de gestión de producción de LRS. Debe proporcionar los nombres de host de las EC2 instancias en las que se instalarán los productos de LRS.	Responsable de compilación
Cree una instancia de Amazon EC2 Windows para instalar LRS VPSX/MFI.	Para lanzar una instancia de Amazon EC2 Windows, sigue las instrucciones de Lanzar una EC2 instancia de Amazon en la EC2 documentación de Amazon. La instancia debe cumplir los siguientes requisitos de hardware y software para LRS VPSX/MFI: • CPU: doble núcleo • RAM: 16 GB • Unidad: 500 GB • EC2 Instancia mínima: m5.xlarge • Sistema operativo: Windows/Linux • Software: Servicio de Información de Internet (IIS) o Apache	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Note Los requisitos de hardware y software anteriores están pensados para una flota de impresoras pequeña (entre 500 y 1000). Para conocer todos los requisito s, consulte a sus personas de contacto en LRS y AWS. Cuando cree la instancia de Windows, haga lo siguiente: 1. Confirme que el nombre de EC2 host es el mismo nombre de host utilizado para la licencia del producto LRS. 2. Para activar CGI en Amazon EC2 , sigue estos pasos: a. Conéctese a su EC2 instancia siguiendo las instrucciones de	

Tarea	Descripción	Habilidades requeridas
Instala LRS VPSX/MFI en la EC2 instancia.	1. Conéctate a tu EC2 instancia siguiendo las instrucciones del paso 2: Conéctate a tu instancia en la EC2 documentación de Amazon. 2. **Note** Abra el enlace a la página de descarga del producto que se incluye en el correo electrónico de LRS que debería haber recibido. : Los productos de LRS se distribuyen mediante transfere ncia de archivos electrónica (EFT). 3. Descarga LRS VPSX/MFI y descomprime el archivo (carpeta predeterminada:`c:\LRS`). 4. Inicie el instalador de productos LRS desde la carpeta descomprimida para instalar LRS VPSX/MFI. 5. En el menú Seleccionar características, seleccione VPSX® Server (V1R3.022) y, a continuación, seleccion	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	e Siguiente para iniciar el proceso de instalación. Cuando se complete la instalación, recibirá un mensaje de confirmación.	
Instale LRS/Queue.	1. Conéctate a tu EC2 instancia de Rocket Enterprise Server siguiendo las instrucciones del paso 2: Conéctate a tu instancia en la EC2 documentación de Amazon. 2. Abra el enlace a la página de descarga del producto LRS desde el correo electrónico de LRS que debería recibir, descargue LRS/Queue y, a continuación, descomprima el archivo. 3. Vaya a la ubicación en la que descargó los archivos y, a continuación, inicie el instalador del producto LRS para instalar LRS/Queue.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Instale LRS/DIS.	1. Conéctate a tu VPSX/MFI EC2 instancia de LRS siguiendo las instrucciones del paso 2: Conéctate a tu instancia en la EC2 documentación de Amazon. 2. Abra el enlace a la página de descarga del producto LRS que se incluye en el correo electrónico de LRS que habrá recibido, descargue LRS/DIS y, a continuación, descomprima el archivo. 3. Vaya a la ubicación en la que descargó los archivos y, a continuación, inicie el instalador de producto de LRS. 4. En el instalador de producto de LRS, amplíe LRS Misc Tools, seleccione LRS DIS y, a continuación, Siguiente. 5. Siga el resto de las instrucciones del instalador del producto de LRS para completar el proceso de instalación.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Cree un grupo objetivo y registre LRS VPSX/MFI EC2 como objetivo.	Cree un grupo de destino siguiendo las instrucciones de Crear un grupo de destino para el equilibrador de carga de red en la documentación en el equilibrador de carga de red elástico. Al crear el grupo de destino, haga lo siguiente: 1. En la página Especific ar detalles del grupo, seleccione un Tipo de destino y luego, Instancias. 2. En Protocol, seleccione TCP. 3. En Puerto, seleccione 5500. 4. En la página Registrar destinos, en la sección Instancias disponibles, seleccione las instancias del LRS. VPSX/MFI EC2	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Crear un equilibrador de carga de red.	Siga las instrucciones de Crear un equilibrador de carga de red en la documentación de Elastic Load Balancing. Su Network Load Balancer dirige el tráfico de Rocket Enterprise Server a LRS. VPSX/MFI EC2 Al crear el equilibrador de carga de red, siga los pasos siguientes en la página Listeners and Routing (Oyentes y enrutamiento): 1. En Protocol, seleccione TCP. 2. En Puerto, seleccione 5500. 3. En Default action (Acción predeterminada), seleccione Forward to (Reenviar a) para el grupo de destino que ha creado.	Arquitecto de la nube

Integre Rocket Enterprise Server con LRS y LRS/Queue VPSX/MFI

Tarea	Descripción	Habilidades requeridas
Configure Rocket Enterprise Server para la integración. LRS/Queue	1. Conéctate a tu EC2 instancia de Rocket Enterprise Server siguiendo las instrucciones del paso 2: Conéctate a tu instancia en la EC2 documentación de Amazon.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	2. En el menú Inicio de Windows, abra la interfaz de usuario de administración de Rocket Enterprise Server. 3. En la barra de menús, seleccione NATIVE. 4. En el panel de navegación, seleccione Directory Server y, a continuación, BANKDEMO. 5. En General , busque el panel de navegación izquierdo, despláce hacia abajo hasta la sección Adicional para configurar las variables del entorno (LRSQ_ADDRESS, LRSQ_PORT, LRSQ_COMMAND) de modo que dirijan hacia LRSQ. 6. Para LRSQ_ADDRESS, escriba la dirección IP o el nombre DNS del equilibrador de carga de red que creó anteriormente. 7. Para LRSQ_PORT, especifique VPSX LRSQ Listener Port (5500). 8. Para LRSQ_COMMAND, especifique la ubicación de la ruta del ejecutable de LRSQ.	

Tarea	Descripción	Habilidades requeridas
	Note Actualmente, LRS admite un límite máximo de 50 caracteres para los nombres de DNS, pero este aspecto cambiará en el futuro. Si el nombre DNS tiene más de 50 caracteres, puede utilizar la dirección IP del equilibrador de carga de red como alternativa.	

Tarea	Descripción	Habilidades requeridas
Configura Rocket Enterprise Server para la VPSX/MFI integración con LRS.	1. Copie la `VPSX_MFI_R2` carpeta del VPSX/MFI instalador del LRS a la ubicación del servidor Rocket Enterprise en. `C\BANKDEMO\print` 2. Conéctate a tu EC2 instancia de Rocket Enterprise Server siguiendo las instrucciones del paso 2: Conéctate a tu instancia en la EC2 documentación de Amazon. 3. En el menú Inicio de Windows, abra la interfaz de usuario de administración de Rocket Enterprise Server. 4. En la barra de menús, seleccione NATIVE. 5. En el panel de navegación, seleccione Directory Server y, a continuación, BANKDEMO. 6. En BANKDEMO, seleccione JES. 7. En JES Program Path, agregue la ruta `DLL(VPSX_MFI_R2)` de `C\BANKDEMO\print` .	Arquitecto de la nube

Configuración de impresoras y usuarios de impresión en Rocket Enterprise Server y LRS VPSX/MFI

Tarea	Descripción	Habilidades requeridas
Asocie el módulo de Rocket Software Print Exit al proceso de ejecución del servidor de la impresora por lotes de Rocket Enterprise Server.	1. Conéctate a tu EC2 instancia de Rocket Enterprise Server siguiendo las instrucciones del paso 2: Conéctate a tu instancia en la EC2 documentación de Amazon. 2. En el menú Inicio de Windows, abra la interfaz de usuario de administr ación de Rocket Enterprise Server. 3. En la barra de menús, seleccione NATIVE. 4. En el panel de navegació n, seleccione Directory Server y, a continuación, BANKDEMO. 5. En BANKDEMO, seleccion e JES y desplácese hacia abajo hasta Printers (Impresoras). 6. En Impresoras, asocie el módulo Print Exit de Rocket Software (LRSPRTE6 para Batch) al proceso de ejecución del servidor (SEP) de la impresora por lotes de Rocket Enterprise Server. Esto permite enrutar la salida	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	de impresión a LRS VPSX/MFI. 7. Inicie sesión en la interfaz de usuario de Enterprise Server Administration. Para obtener más información sobre la configuración, consulte Using the Exit (Uso de la salida) en la documentación de Micro Focus.	

Tarea	Descripción	Habilidades requeridas
Añada una impresora en LRS VPSX/MFI.	1. Conéctate a tu VPSX/MFI EC2 instancia de LRS siguiendo las instrucciones del paso 2: Conéctate a tu instancia en la EC2 documentación de Amazon. 2. Abra la interfaz web de VPSX desde el menú Inicio de Windows. 3. En el panel de navegación, seleccione Impresoras. 4. Seleccione Add (Agregar) y, después, Add Printer (Agregar impresora). 5. En la página Printer Configuration (Configuración de la impresora), busque Printer Name (Nombre de impresora) y especifique Local. 6. Para el ID de VPSX, introduzca. VPS1 7. Para CommType, seleccione TCPIP/LRSQ. 8. En Host/Dirección IP, introduzca la dirección IP de la impresora física que desee agregar. 9. En Dispositivo, introduzca el nombre de su dispositivo. 10. Seleccione Controlador de Windows o Controlador de Linux/Mac.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	11. Elija Agregar.	

Tarea	Descripción	Habilidades requeridas
Cree un usuario de impresión en LRS VPSX/MFI.	1. Conéctate a tu VPSX/MFI EC2 instancia de LRS siguiendo las instrucciones del paso 2: Conéctate a tu instancia en la EC2 documentación de Amazon. 2. Abra la interfaz web de VPSX desde el menú Inicio de Windows. 3. En el panel de navegación, elija Seguridad y luego elija la opción Usuarios. 4. En la columna Nombre de usuario, seleccione admin y, a continuación, seleccione Copiar. 5. En la ventana Mantenimiento del perfil de usuario, en Nombre de usuario, introduzca un nombre de usuario (por ejemplo, PrintUser). 6. En Descripción, escriba una descripción breve (por ejemplo, Usuario para impresión de prueba). 7. Seleccione Update (Actualizar). Esto crea un usuario de impresión (por ejemplo, PrintUser). 8. En el panel de navegación, en Usuario, seleccion	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	e el nuevo usuario que ha creado. 9. En el menú Comandos, seleccione Seguridad. 10. En la página Reglas de seguridad, seleccione todas las opciones de seguridad de la impresora y seguridad laboral aplicables y, a continuación, seleccione Guardar. 11. Para añadir el nuevo usuario de impresión al grupo Administrador, vaya al panel de navegación, seleccione Seguridad y, a continuación, seleccione Configurar. 12. En la ventana Configuración de seguridad, añada su nuevo usuario de impresión a la columna Administrador.	

Configure imprimir autenticación y autorización

Tarea	Descripción	Habilidades requeridas
Cree un dominio de AWS Managed Microsoft AD con usuarios y grupos.	1. Para crear un directorio Active en AWS Managed Microsoft AD, siga las instrucciones de ree su directorio de AWS	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Managed Microsoft AD en la documentación de AWS Directory Service. 2. Implemente una EC2 instancia (administrador de Active Directory) e instale las herramientas de Active Directory para administr ar su AD de Microsoft administrado por AWS siguiendo las instrucciones del paso 3: Implementar una EC2 instancia para administrar su AD de Microsoft administrado por AWS que aparecen en la documentación de AWS Directory Service. 3. **Note** Conéctate a tu EC2 instancia siguiendo las instrucciones del paso 2: Conéctate a tu instancia en la EC2 documenta ción de Amazon. : Cuando te conectes a la EC2 instancia , introduce tus credenciales de administrador (para el directorio que creaste en el primer	

Tarea	Descripción	Habilidades requeridas
	paso) en la ventana de seguridad de Windows. 4. En el menú Inicio de Windows, bajo Herramientas administrativas de Windows, seleccione Usuarios y equipos de Active Directory. 5. Cree un usuario de impresión en el dominio de Active Directory siguiendo los pasos de Crear un usuario de la documentación de AWS Directory Service.	
Une LRS VPSX/MFI EC2 a un dominio de Microsoft AD gestionado por AWS.	Une LRS VPSX/MFI EC2 a tu dominio de Microsoft AD gestionado por AWS de forma automática (documentación del AWS Knowledge Center) o manualmente (documentación de AWS Directory Service).	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Configure e integre LRS/DIS con AWS Managed Microsoft AD.	1. Conéctate a tu VPSX/MFI EC2 instancia de LRS siguiendo las instrucciones del paso 2: Conéctate a tu instancia en la EC2 documentación de Amazon. 2. En el menú Start (Inicio) de Windows, abra VPSX Web Interface. 3. En el panel de navegación, seleccione Seguridad y, a continuación, la opción Configurar. 4. En la página Security Configuration, busque la sección Security Parameters y, en Security Type, seleccione Internal. 5. Especifique sus preferencias para el resto de las opciones en la sección Parámetros de seguridad. 6. En el menú Start (Inicio) de Windows, abra la carpeta LRS Output Management, seleccione Server Start y, a continuación, Server Stop. 7. Inicie sesión en LRS VPSX/MFI con su nombre de usuario y contraseña de Active Directory.	Arquitecto de la nube

Pruebe un flujo de trabajo de impresión

Tarea	Descripción	Habilidades requeridas
Inicie una solicitud de impresión por lotes desde la BankDemo aplicación Rocket Software.	1. Abre el emulador de terminal 3270 en tu EC2 instancia de Rocket Enterprise Server. 2. Conéctese a la BankDemo aplicación ejecutando el siguiente comando: `connect 127.0.0.1 :9278` 3. En la interfaz de línea de BankDemo comandos, para ID de usuario, escriba B0001. En Password (Contraseña), especifique una clave que no esté en blanco. 4. Para la opción Request printed statement(s) (Solicitar extractos impresos), escriba X en la línea en blanco. 5. En la sección Send statement by (Enviar extracto por), para Mail, escriba Y (Sí) y, a continuación, pulse F10.	Ingeniero de pruebas
Compruebe la producción de impresión en LRS VPSX/MFI.	1. Conéctate a tu VPSX/MFI EC2 instancia de LRS siguiendo las instrucciones del paso 2: Conéctate	Ingeniero de pruebas

Tarea	Descripción	Habilidades requeridas
	a tu instancia en la EC2 documentación de Amazon. 2. En el menú Start (Inicio) de Windows, abra VPSX Web Interface. 3. En el panel de navegació n, seleccione Impresoras y, a continuación, seleccione Cola de producción. 4. En la columna ID de bobina, seleccione la ID de bobina de la solicitud en la cola de impresora. 5. En la pestaña Acciones, en la columna COMANDO, seleccione Examinar. Ya puede ver el resultado impreso de un extracto de cuenta con columnas para Account No. (Número de cuenta), Description, Date, Amount (Importe) y Balance (Saldo). Para ver un ejemplo, consulte el archivo adjunto batch_print_output para este patrón.	

Recursos relacionados

- Modernización de la producción de LRS (documentación de LRS)
- Controles ANSI y de carro de máquinas (documentación de IBM)
- Palabras de comando de canal (documentación de IBM)

- Empowering Enterprise Mainframe Workloads on AWS with Micro Focus (Capacitación de cargas de trabajo de mainframe empresarial en AWS) (publicación de blog de socio de AWS)
- Cree un PAC para servidores empresariales de Micro Focus con Amazon EC2 Auto Scaling y Systems Manager (documentación de AWS Prescriptive Guidance)
- Flujo de datos de Presentación de funciones avanzadas (AFP) (documentación de IBM)
- Flujo de datos condicionado por línea (LCDS) (documentación de Compart)

Información adicional

Consideraciones

Durante su proceso de modernización, podría considerar la posibilidad de utilizar una amplia variedad de configuraciones para los procesos en línea y por lotes de mainframe, así como para la producción que generan. Todos los clientes y proveedores que utilizan la plataforma de mainframe la han personalizado con requisitos particulares que afectan directamente a la impresión. Por ejemplo, su plataforma actual puede incorporar Advanced Function Presentation (AFP) de IBM o Line Condition Data Stream (LCDS) de Xerox en el flujo de trabajo actual. Además, los caracteres de control de carro de mainframe y las palabras de comando de canal pueden afectar al aspecto de la página impresa y pueden requerir un tratamiento especial. Como parte del proceso de planificación de la modernización, le recomendamos evaluar y comprender las configuraciones de su entorno de impresión específico.

Captura de datos de impresión

Rocket Software Print Exit transmite la información necesaria para que LRS VPSX/MFI pueda procesar de forma eficaz el archivo de impresión. La información consta de campos incluidos en los bloques de control correspondientes, como los siguientes:

- JOBNAME
- OWNER (USERID)
- DESTINATION
- FORM
- FILENAME
- WRITER

El LRS VPSX/MFI admite los siguientes mecanismos de procesamiento por lotes de mainframe para capturar datos de Rocket Enterprise Server.

- print/spool Procesamiento COBOL POR LOTES mediante sentencias JCL SYSOUT estándar z/OS DD/OUTPUT
- print/spool Procesamiento de COBOL POR LOTES utilizando sentencias JCL CA-SPOOL SUBSYS DD estándar z/OS
- IMS/COBOL print/spoolprocesamiento mediante la interfaz CBLTDLI (para obtener una lista completa de los métodos y ejemplos de programación compatibles, consulte la documentación del LRS que se incluye con la licencia del producto).

Comprobación de estado de la flota de impresoras

El LRS VPSX/MFI (LRS LoadX) puede realizar controles de estado exhaustivos, como la gestión de los dispositivos y la optimización operativa. La administración de dispositivos puede detectar un error en un dispositivo de impresión y dirigir la solicitud de impresión a una impresora en buen estado. Para obtener más información sobre las comprobaciones de estado exhaustivas de las flotas de impresoras, consulte la documentación de LRS que se incluye con la licencia del producto.

Imprimir autenticación y autorización

LRS/DIS enables LRS applications to authenticate user IDs and passwords by using Microsoft Active Directory or an LDAP server. In addition to basic print authorization, LRS/DIStambién puede aplicar controles de seguridad de impresión de nivel granular en los siguientes casos de uso:

- Gestione quién puede examinar el trabajo de impresión.
- Gestione el nivel de navegación de los trabajos de otros usuarios.
- Gestione las tareas operativas. Por ejemplo, la seguridad en el nivel de comandos, como retener o liberar, purgar, modificar, copiar y redirigir. La seguridad se puede configurar mediante el ID de usuario o el grupo, (similar a un grupo AD o a un grupo LDAP).

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Modernización del mainframe: DevOps adelante AWS con Rocket Software Enterprise Suite

Kevin Yung, Amazon Web Services

Resumen

Desafíos de los clientes

Las organizaciones que ejecutan aplicaciones principales en hardware de mainframe suelen enfrentarse a algunos desafíos cuando el hardware necesita escalar verticalmente para satisfacer las demandas de las innovaciones digitales. Estos desafíos incluyen las siguientes limitaciones.

- Los entornos de desarrollo y prueba de los mainframe no se pueden escalar debido a la inflexibilidad de los componentes de hardware de los mainframes y al elevado costo que supone cambiarlos.
- El desarrollo de mainframes se enfrenta a una escasez de personal cualificado, ya que los nuevos desarrolladores no están familiarizados con las herramientas tradicionales de desarrollo de mainframes ni están interesados en ellas. La tecnología moderna, como los contenedores, los canales de integration/continuous entrega continua (CI/CD) y los marcos de prueba modernos, no están disponibles para el desarrollo de mainframes.

Resultados del patrón

Para abordar estos desafíos, Amazon Web Services (AWS) y Rocket Software Micro Focus, un socio de AWS Partner Network (APN), han colaborado para crear este patrón. La solución está diseñada para ayudarle a lograr los siguientes resultados.

- Mejora de la productividad de los desarrolladores. Los desarrolladores pueden disponer de nuevas instancias de desarrollo de mainframe en cuestión de minutos.
- Uso del Nube de AWS para crear nuevos entornos de prueba de mainframe con una capacidad prácticamente ilimitada.
- Aprovisionamiento rápido de una nueva infraestructura de mainframe CI/CD . El aprovisionamiento se AWS puede completar en una hora utilizando y. AWS CloudFormation AWS Systems Manager
- Uso nativo de AWS DevOps herramientas para el desarrollo de mainframes, incluidas AWS CodeBuild, AWS CodeCommit AWS CodePipeline AWS CodeDeploy, y Amazon Elastic Container Registry (Amazon ECR).

- Transforme el desarrollo tradicional en cascada en un desarrollo ágil en proyectos de mainframe.

Resumen de tecnologías

En este patrón, la pila de destino contiene los siguientes componentes.

Componentes lógicos	Soluciones de implementación	Description (Descripción)
Repositorios de código fuente	AccuRev Servidor de software Rocket CodeCommit, Amazon ECR	Administración del código fuente: la solución utiliza dos tipos de código fuente: • Código fuente de mainframe , por ejemplo, COBOL y JCL. • AWS plantillas de infraestr uctura y scripts de automatiz ación Ambos tipos de código fuente necesitan control de versiones , pero se administran de forma diferente SCMs. El código fuente desplegad o en el mainframe o en los servidores empresariales de Rocket Software se administr a en Rocket Software Micro Focus AccuRev Server. AWS las plantillas y los scripts de automatización se gestionan en CodeCommit. Amazon ECR se utiliza para los repositorios de imágenes de Docker.

Instancias de desarrolladores empresariales	Amazon Elastic Compute Cloud (Amazon EC2), desarrollador empresarial de Rocket Software para Eclipse	Los desarrolladores de mainframe pueden desarroll ar código en Amazon EC2 mediante Rocket Software Enterprise Developer for Eclipse. Esto elimina la necesidad de depender del hardware del mainframe para escribir y probar el código.
Administración de licencias de Rocket Software Enterprise Suite	Rocket Software Enterprise Suite License Manager	Para la administración y la gobernanza centralizadas de las licencias de Rocket Software Enterprise Suite, la solución utiliza Rocket Software Enterprise Suite License Manager para alojar la licencia requerida.
Canalización de CI/CD	CodePipeline, CodeBuild CodeDeploy, Rocket Software Enterprise Developer en un contenedor, Rocket Software Enterprise Test Server en un contenedor, Rocket Software Micro Focus Enterprise Server	Los equipos de desarrollo de mainframes necesitan CI/CD canalizaciones para realizar la compilación de código, las pruebas de integración y las pruebas de regresión. En un contenedor de CodePipeline forma nativa AWS, CodeBuild pueden trabajar con Rocket Software Enterprise Developer y Enterprise Test Server en un contenedor.

Requisitos previos y limitaciones

Requisitos previos

Name	Description (Descripción)
py3270	py3270 es una interfaz de Python para x3270, un emulador de terminal IBM 3270. Proporcio na una API para un subproceso x3270 o s3270.
x3270	x3270 es un emulador de terminal IBM 3270 para el sistema X Window y Windows. El desarrollador lo puede utilizar para realizar pruebas unitarias a nivel local.
Robot-Framework-Mainframe-3270-Library	Mainframe3270 es una biblioteca para Robot Framework basada en el proyecto py3270.
Rocket Software Verastream	Rocket Software Verastream es una plataform a de integración que permite probar los activos del mainframe del mismo modo que se prueban las aplicaciones móviles, las aplicaciones web y los servicios web SOA.
Instalador y licencia de Rocket Software Unified Functional Testing (UFT)	Rocket Software Unified Functional Testing es un software que automatiza las pruebas funcionales y de regresión para aplicaciones y entornos de software.
Instalador y licencia de Rocket Software Enterprise Server	Enterprise Server proporciona el tiempo de ejecución para las aplicaciones de mainframe.
Instalador y licencia de Rocket Software Enterprise Test Server	Rocket Software Enterprise Test Server es un entorno de prueba de aplicaciones de mainframe de IBM.
AccuRev Instalador y licencia de Rocket Software para servidores, e AccuRev instalador y licencia de Rocket Software Micro Focus para sistemas operativos Windows y Linux	AccuRev proporciona administración de código fuente (SCM). El AccuRev sistema está diseñado para que lo utilice un equipo de personas que están desarrollando un conjunto de archivos.

Instalador, revisión y licencia de Rocket Software Enterprise Developer for Eclipse	Enterprise Developer proporciona a los desarrolladores de mainframe una plataform a para desarrollar y mantener las principales aplicaciones de mainframe en línea y por lotes.

Limitaciones

- No se admite la creación de una imagen de Docker de Windows en CodeBuild. Este problema notificado necesita el apoyo de los equipos de Windows Kernel/HCS y Docker. La solución alternativa consiste en crear un manual de procedimientos de imágenes de Docker mediante Systems Manager. Este patrón utiliza la solución alternativa para compilar imágenes de contenedor de Rocket Software Enterpise Developer for Eclipse y Rocket Software Micro Focus Enterprise Test Server.
- Windows aún no admite la conectividad de nube privada virtual (VPC) desde CodeBuild , por lo que el patrón no utiliza Rocket Software License Manager para administrar las licencias en los contenedores OpenText Rocket Software Enterprise Developer y Rocket Software Enterprise Test Server.

Versiones de producto

- La versión 5.5 o posterior de Rocket Software Enterprise Developer
- La versión 5.5 o posterior de Rocket Software Enterprise Test Server
- La versión 5.5 o posterior de Rocket Software Enterprise Server
- Rocket Software AccuRev 7.x o posterior
- Imagen base de Docker de Windows para Rocket Software Enterprise Developer y Enterprise Test Server: microsoft/dotnet-framework-4.7.2-runtime
- Imagen base de Linux Docker para el AccuRev cliente: amazonlinux:2

Arquitectura

Entorno de mainframe

En el desarrollo de mainframe convencional, los desarrolladores necesitan usar hardware de mainframe para desarrollar y probar programas. Se enfrentan a limitaciones de capacidad, por

ejemplo, la restricción de millones de instrucciones por segundo (MIPS) para el dev/test entorno, y deben confiar en las herramientas disponibles en los ordenadores centrales.

En muchas organizaciones, el desarrollo de mainframes sigue la metodología de desarrollo en cascada, y los equipos utilizan ciclos largos para publicar los cambios. Estos ciclos de lanzamiento suelen ser más largos que los del desarrollo de productos digitales.

El siguiente diagrama muestra varios proyectos de mainframe que comparten el hardware de mainframe para su desarrollo. En el caso del hardware de mainframe, resulta caro escalar horizontalmente un entorno de desarrollo y pruebas para más proyectos.

Arquitectura de AWS

Este patrón extiende el desarrollo de mainframe a la Nube de AWS. En primer lugar, utiliza AccuRev SCM para alojar el código fuente del mainframe. AWS Luego, permite que Enterprise Developer y Enterprise Test Server estén disponibles para compilar y probar el código del mainframe en AWS.

En las siguientes secciones se describen los tres componentes principales del patrón.

1. SCM

En AWS, el patrón se utiliza AccuRev para crear un conjunto de espacios de trabajo SCM y un control de versiones para el código fuente del mainframe. Su arquitectura basada en flujos permite el desarrollo de mainframes paralelos para varios equipos. Para combinar un cambio, AccuRev utiliza el concepto de promoción. Para añadir ese cambio a otros espacios de trabajo, AccuRev utiliza el concepto de actualización.

A nivel de proyecto, cada equipo puede crear una o más secuencias para realizar un seguimiento de los cambios AccuRev a nivel de proyecto. Se denominan flujos de proyectos. Estos flujos del proyecto se heredan del mismo flujo principal. El flujo principal se usa para combinar los cambios de los diferentes flujos del proyecto.

Cada flujo de proyectos puede promover el código y se ha configurado un activador de promoción posterior para iniciar el proceso de AWS CI/CD. AccuRev La versión correcta para el cambio de flujo de un proyecto se puede convertir en su flujo principal para realizar más pruebas de regresión.

Por lo general, el flujo principal se denomina flujo de integración del sistema. Cuando hay un ascenso de un flujo de proyectos a un flujo de integración de sistemas, una activación posterior a la promoción inicia otro CI/CD proceso para ejecutar pruebas de regresión.

Además del código de mainframe, este patrón incluye AWS CloudFormation plantillas, documentos de automatización de Systems Manager y scripts. Siguiendo las infrastructure-as-code mejores prácticas, se controlan las versiones en ellas. CodeCommit

Si necesita volver a sincronizar el código del mainframe con un entorno de mainframe para su despliegue, Rocket Software proporciona la solución Enterprise Sync, que sincroniza el código del SCM con el AccuRev SCM del mainframe.

2. Entornos de desarrollo y pruebas

En una organización grande, escalar más de cien o incluso más de mil desarrolladores de mainframe es todo un desafío. Para abordar esta restricción, el patrón utiliza instancias de Amazon EC2 Windows para el desarrollo. En las instancias, están instaladas las herramientas Enterprise Developer for Eclipse. El desarrollador puede realizar todas las pruebas y depuraciones del código del mainframe de forma local en la instancia.

AWS Systems Manager Los documentos de State Manager y Automation se utilizan para automatizar el aprovisionamiento de instancias para desarrolladores. El tiempo medio para crear una instancia de desarrollador es de 15 minutos. Se han preparado el software y las configuraciones siguientes:

- AccuRev Cliente de Windows para extraer y guardar el código fuente AccuRev
- Herramienta Enterprise Developers for Eclipse, para escribir, probar y depurar el código de mainframe de forma local
- Marcos de pruebas de código abierto, pruebas de desarrollo impulsado por el comportamiento (BDD) de Python, marco de prueba Behave, py3270 y el emulador x3270 para crear scripts para probar aplicaciones
- Una herramienta de desarrollo de Docker para crear la imagen de Docker de Enterprise Test Server y probar la aplicación en el contenedor de Docker de Enterprise Test Server

En el ciclo de desarrollo, los desarrolladores utilizan la EC2 instancia para desarrollar y probar el código del mainframe de forma local. Cuando los cambios locales se prueban correctamente, los desarrolladores promueven el cambio en el AccuRev servidor.

3. CI/CD oleoductos

En este patrón, las CI/CD canalizaciones se utilizan para las pruebas de integración y las pruebas de regresión antes del despliegue en el entorno de producción.

Como se explica en la sección SCM, AccuRev utiliza dos tipos de flujos: un flujo de proyecto y un flujo de integración. Cada transmisión está conectada a canalizaciones. CI/CD Para realizar la integración entre el AccuRev servidor y AWS CodePipeline, el patrón utiliza un script AccuRev posterior a la promoción para crear un evento que inicie el CI/CD.

Por ejemplo, cuando un desarrollador promueve un cambio en el flujo de un proyecto AccuRev, inicia un script posterior a la promoción para que se ejecute en Server. AccuRev A continuación, el script carga los metadatos del cambio a un bucket de Amazon Simple Storage Service (Amazon S3) para crear un evento de Amazon S3. Este evento iniciará la ejecución de una canalización CodePipeline configurada.

El mismo mecanismo de inicio de eventos se utiliza para el flujo de integración y sus canalizaciones asociadas.

En el CI/CD proceso, se CodePipeline utiliza CodeBuild con el contenedor de clientes de AccuRev Linux para extraer el código más reciente de las AccuRev transmisiones. Luego, la canalización comienza CodeBuild a usar el contenedor de Windows para Enterprise Developer para compilar el código fuente y a usar el contenedor de Windows de Enterprise Test Server CodeBuild para probar las aplicaciones de mainframe.

Las CI/CD canalizaciones se crean mediante CloudFormation plantillas y el plano se utilizará para nuevos proyectos. Al usar las plantillas, un proyecto tarda menos de una hora en crear una nueva CI/CD canalización. AWS

Para ampliar la capacidad de prueba de su ordenador central AWS, el patrón incluye el conjunto de DevOps pruebas de Rocket Software, Verastream y el servidor UFT. Con las DevOps herramientas modernas, puede ejecutar tantas pruebas como necesite. AWS

En el siguiente diagrama se muestra un ejemplo de entorno de desarrollo de AWS mainframe con Rocket Software activado.

Pila de tecnología de destino

En esta sección se ofrece una visión más detallada de la arquitectura de cada componente del patrón.

1. Repositorio de código fuente: SCM AccuRev

AccuRev SCM está configurado para administrar las versiones del código fuente del mainframe. Para una alta disponibilidad, AccuRev admite los modos principal y de réplica. Los operadores pueden realizar una conmutación por error a la réplica cuando realizan tareas de mantenimiento en el nodo principal.

Para acelerar la respuesta de la CI/CD canalización, el patrón utiliza Amazon CloudWatch Events para detectar los cambios en el código fuente e iniciar el inicio de la canalización.

1. La canalización se ha configurado para que utilice un origen de Amazon S3.
2. Se configura una regla de CloudWatch eventos para capturar los eventos de S3 de un bucket de S3 de origen.
3. La regla de CloudWatch eventos establece un objetivo para la canalización.
4. AccuRev SCM está configurado para ejecutar un script posterior a la promoción de forma local una vez finalizada la promoción.
5. AccuRev SCM genera un archivo XML que contiene los metadatos de la promoción y el script carga el archivo XML en el depósito S3 de origen.
6. Tras la carga, el bucket de S3 de origen envía los eventos para que coincidan con la regla de CloudWatch eventos, y esta última inicia la CloudWatch ejecución de la canalización.

Cuando la canalización se ejecuta, inicia un CodeBuild proyecto para utilizar un contenedor cliente de AccuRev Linux para extraer el código más reciente del mainframe de una transmisión asociada. AccuRev

El siguiente diagrama muestra la configuración de un AccuRev servidor.

2. Plantilla para desarrolladores empresariales

El patrón utiliza EC2 plantillas de Amazon para simplificar la creación de la instancia de desarrollador. Al usar State Manager, puede aplicar la configuración de software y licencia a EC2 las instancias de manera coherente.

La EC2 plantilla de Amazon incluye su configuración de contexto de VPC y su configuración de instancia predeterminada, y cumple con los requisitos de etiquetado empresarial. Al usar una plantilla, un equipo puede crear sus propias instancias de desarrollo nuevas.

Cuando se inicia una instancia de desarrollador, mediante la asociación con etiquetas, Systems Manager usa State Manager para aplicar la automatización. La automatización incluye los siguientes pasos generales.

1. Instale el software Enterprise Developer e instale las revisiones.
2. Instale el AccuRev cliente para Windows.
3. Instale el script preconfigurado para que los desarrolladores se unan a la AccuRev transmisión. Inicialice los espacios de trabajo de Eclipse.
4. Instale las herramientas de desarrollo, incluidas x3270, py3270 y Docker.
5. Configure los ajustes de la licencia para que apunten a un equilibrador de carga de License Manager.

El siguiente diagrama muestra una instancia de desarrollador empresarial creada por la EC2 plantilla de Amazon, con el software y la configuración aplicados a la instancia por State Manager. Las instancias de desarrollador empresarial se conectan AWS License Manager para activar su licencia.

3. Canalización de CI/CD

Como se explicó en la sección de AWS arquitectura, en el patrón hay canalizaciones a nivel de proyecto y CI/CD canalizaciones de integración de sistemas. Cada equipo de proyecto de mainframe crea una canalización o varias CI/CD canalizaciones para crear los programas que está desarrollando en un proyecto. Estas CI/CD canalizaciones de proyectos extraen el código fuente de una transmisión asociada. AccuRev

En un equipo de proyecto, los desarrolladores promocionan su código en la AccuRev transmisión asociada. A continuación, la promoción inicia la canalización del proyecto para compilar el código y ejecutar las pruebas de integración.

Cada CI/CD canalización de CodeBuild proyectos utiliza proyectos con la imagen Amazon ECR de la herramienta para desarrolladores empresariales y la imagen Amazon ECR de la herramienta Enterprise Test Server.

CodePipeline y CodeBuild se utilizan para crear las canalizaciones. CI/CD Como CodeBuild no CodePipeline hay comisiones ni compromisos por adelantado, solo pagas por lo que utilizas. En

comparación con el hardware de mainframe, la AWS solución reduce considerablemente el tiempo de aprovisionamiento del hardware y reduce el coste del entorno de pruebas.

En el desarrollo moderno, se utilizan múltiples metodologías de prueba. Por ejemplo, el desarrollo basado en pruebas (TDD), el BDD y Robot Framework. Con este patrón, los desarrolladores pueden usar estas herramientas modernas para realizar pruebas de mainframe. Por ejemplo, si utiliza x3270, py3270 y la herramienta de prueba Behave python, puede definir el comportamiento de una aplicación en línea. También puede utilizar la estructura robotizada Build mainframe 3270 en estos procesos. CI/CD

El siguiente diagrama muestra el proceso de transmisión del equipo. CI/CD

El siguiente diagrama muestra el informe de CI/CD prueba del proyecto elaborado por CodePipeline Mainframe3270 Robot Framework.

El siguiente diagrama muestra el informe de CI/CD prueba del proyecto elaborado por Py3270 y CodePipeline Behave BDD.

Una vez superadas las pruebas a nivel de proyecto, el código probado se transfiere manualmente al flujo de integración de SCM. AccuRev Puede automatizar este paso una vez que los equipos confíen en la cobertura de las pruebas de su cartera de proyectos.

Cuando se promueve el código, el proceso de integración del CI/CD sistema comprueba el código fusionado y realiza pruebas de regresión. El código fusionado se promueve desde todos los flujos de proyectos paralelos.

En función de la precisión del entorno de pruebas, los clientes pueden disponer de más CI/CD procesos de integración de sistemas en un entorno diferente, por ejemplo, UAT (preproducción).

En el patrón, las herramientas utilizadas en la canalización de integración de sistemas son Enterprise Test Server, UFT Server y Verastream. Todas estas herramientas pueden desplegarse en el contenedor Docker y utilizarse con ellas. CodeBuild

Tras probar satisfactoriamente los programas del mainframe, el artefacto se almacena, con el control de versiones, en un bucket de S3.

El siguiente diagrama muestra una CI/CD canalización de integración del sistema.

Una vez que el artefacto se haya probado satisfactoriamente en las CI/CD canalizaciones de integración del sistema, podrá promocionarse para su despliegue en producción.

Si necesita volver a implementar el código fuente en el mainframe, Rocket Software ofrece la solución Enterprise Sync para sincronizar el código fuente desde el mainframe AccuRev Endeavour.

El siguiente diagrama muestra un proceso de producción que CI/CD despliega el artefacto en servidores empresariales. En este ejemplo, CodeDeploy organiza el despliegue del artefacto de mainframe probado en Enterprise Server.

Además del tutorial de arquitectura en CI/CD proceso, consulte la entrada del AWS DevOps blog Automatice miles de pruebas de mainframe AWS con Micro Focus Enterprise Suite para obtener más información sobre las pruebas de aplicaciones de mainframe en y. CodeBuild CodePipeline (Micro Focus ahora es Rocket Software). Consulte la entrada del blog para conocer las mejores prácticas y los detalles sobre cómo realizar pruebas de mainframe en. AWS

Tools (Herramientas)

AWS herramientas de automatización

- CloudFormation
- CloudWatch Eventos de Amazon
- AWS CodeBuild
- AWS CodeDeploy
- AWS CodePipeline
- Amazon ECR
- Amazon S3
- AWS Secrets Manager
- AWS Systems Manager

Herramientas de Rocket Software

- Rocket Enterprise Developer for Eclipse
- Rocket Enterprise Test Server

- Rocket Enterprise Server (implementación en producción)
- Software Rocket AccuRev
- Rocket Software Enterprise Suite License Manager
- Rocket Software Verastream Host Integrator
- Rocket Software UFT One

Otras herramientas

- x3270
- py3270
- Robot-Framework-Mainframe-3270-Library

Epics

Cree la infraestructura AccuRev SCM

Tarea	Descripción	Habilidades requeridas
Implemente un servidor AccuRev SCM principal mediante. CloudFormation		AWS CloudFormation
Cree el usuario AccuRev administrador.	Inicie sesión en el servidor AccuRev SCM y ejecute el comando CLI para crear un usuario administrador.	AccuRev Administrador del servidor SCM
Crea AccuRev transmisiones.	Cree AccuRev flujos que hereden de los flujos superiores en secuencia: flujos de producción, integración de sistemas y equipos.	AccuRev Administrador de SCM
Cree las cuentas de inicio de AccuRev sesión del desarrollador.	Utilice los comandos CLI de AccuRev SCM para crear cuentas de inicio de sesión	AccuRev Administrador de SCM

Tarea	Descripción	Habilidades requeridas
	de AccuRev usuarios para desarrolladores de mainframe.	

Cree la plantilla de EC2 lanzamiento de Amazon para desarrolladores empresariales

Tarea	Descripción	Habilidades requeridas
Implemente la plantilla de EC2 lanzamiento de Amazon utilizando CloudFormation.	Se usa CloudFormation para implementar una plantilla de EC2 lanzamiento de Amazon para instancias de Enterprise Developer. La plantilla incluye un documento de Automatiz ación de Systems Manager para la instancia de Rocket Enterprise Developer.	AWS CloudFormation
Crea la instancia de Enterpris e Developer a partir de la EC2 plantilla de Amazon.		Habilidades de desarrollador de mainframe y inicio de sesión en la consola de AWS

Creación de la imagen de Docker de la herramienta Enterprise Developer

Tarea	Descripción	Habilidades requeridas
Crear la imagen de Docker de la herramienta Enterprise Developer.	Utilice el comando de Docker y el Dockerfile de la herramien ta Enterprise Developer para crear la imagen de Docker.	Docker
Cree el repositorio de Docker en Amazon ECR.	En la consola de Amazon ECR, cree el repositorio para la imagen de Docker de Enterprise Developer.	Amazon ECR

Tarea	Descripción	Habilidades requeridas
Enviar la imagen de Docker de la herramienta Enterprise Developer a Amazon ECR.	Ejecute el comando push de Docker para enviar la imagen de Docker de la herramien ta para desarrolladores empresariales y guardarla en el repositorio de Docker de Amazon ECR.	Docker

Creación de la imagen de Docker de Enterprise Test Server

Tarea	Descripción	Habilidades requeridas
Crear la imagen de Docker de Enterprise Test Server.	Utilice el comando de Docker y el Dockerfile de Enterpris e Test Server para crear la imagen de Docker.	Docker
Cree el repositorio de Docker en Amazon ECR.	En la consola de Amazon ECR, cree el repositorio de Amazon ECR para la imagen de Docker de Enterprise Test Server.	Amazon ECR
Enviar la imagen de Docker de Enterprise Test Server a Amazon ECR.	Ejecute el comando push de Docker para enviar y guardar la imagen de Docker del Enterprise Test Server en Amazon ECR.	Docker

Crea la CI/CD canalización de transmisión del equipo

Tarea	Descripción	Habilidades requeridas
Crea el CodeCommit repositorio.	En la CodeCommit consola, cree un repositorio basado en Git para la infraestructura y el CloudFormation código.	AWS CodeCommit
Cargue la CloudFormation plantilla y el código de automatización en el CodeCommit repositorio.	Ejecuta el comando Git push para cargar la CloudFormation plantilla y el código de automatización en el repositorio.	Git
Implemente la CI/CD canalización de transmisiones en equipo mediante CloudFormation.	Usa la CloudFormation plantilla preparada para implementar una CI/CD canalización de transmisión en equipo.	AWS CloudFormation

Cree la CI/CD canalización de integración del sistema

Tarea	Descripción	Habilidades requeridas
Crear la imagen de Docker de UFT.	Utilice el comando de Docker y el Dockerfile de UFT para crear la imagen de Docker.	Docker
Crear el repositorio de Docker en Amazon ECR para la imagen de UFT.	En la consola de Amazon ECR, cree el repositorio de Docker para la imagen de UFT.	Amazon ECR
Enviar la imagen de Docker de UFT a Amazon ECR.	Ejecute el comando push de Docker para enviar y guardar la imagen de Docker del	Docker

Tarea	Descripción	Habilidades requeridas
	Enterprise Test Server en Amazon ECR.	
Crear la imagen de Docker de Verastream.	Utilice el comando de Docker y el Dockerfile de Verastrea m para crear la imagen de Docker.	Docker
Crear el repositorio de Docker en Amazon ECR para la imagen de Verastream.	En la consola de Amazon ECR, cree el repositorio de Docker para la imagen de Verastream.	Amazon ECR
Implemente la CI/CD canalización de integración del sistema mediante CloudForm ation.	Utilice la CloudFormation plantilla preparada para implementar una CI/CD canalización de integración de sistemas.	AWS CloudFormation

Cree una CI/CD canalización de despliegue de producción

Tarea	Descripción	Habilidades requeridas
Implemente Enterprise Server mediante el AWS Quick Start.	Para implementar Enterprise Server mediante CloudForm ation, inicie Enterprise Server en AWS Quick Start.	AWS CloudFormation
Implemente una CI/CD canalización de despliegue en producción.	En la CloudFormation consola, utilice la CloudFormation plantilla para implementar una CI/CD canalización de despliegue de producción.	AWS CloudFormation

Recursos relacionados

Referencias

- AWS DevOps Blog - Automatice miles de pruebas de mainframe AWS con Micro Focus Enterprise Suite (Micro Focus ahora es Rocket Software).
- repositorio py3270/py3270 GitHub
- Repositorio de bibliotecas GitHub Altran-PT-GDC/Robot-Framework-Mainframe-3270
- ¡Bienvenido a Behave!
- Blog de socios de la APN - Etiqueta: Micro Focus (Micro Focus ahora es Rocket Software)
- Lanzamiento de una instancia desde una plantilla de lanzamiento

AWS Marketplace

- Rocket Software UFT One

AWS Quick Start (Inicio rápido)

- Rocket Enterprise Server en AWS

Modernizar las cargas de trabajo de impresión en línea de mainframe en AWS mediante Micro Focus Enterprise Server y LRS VPSX/MFI

Shubham Roy y Kevin Yung, Amazon Web Services

Abraham Rondon, Micro Focus

Guy Tucker, Levi, Ray and Shoup Inc

Resumen

Este patrón le muestra cómo modernizar sus cargas de trabajo de impresión online de mainframe críticas para la empresa en la nube de Amazon Web Services (AWS) mediante el uso de Micro Focus Enterprise Server como entorno de ejecución para una aplicación de mainframe modernizada y LRS VPSX/MFI (Micro Focus Interface) como servidor de impresión. El patrón se basa en el enfoque de modernización del mainframe a través de redefinir la plataforma. Con este enfoque, migra su aplicación en línea de mainframe a Amazon Elastic Compute Cloud (Amazon EC2) y migra su base de datos de mainframe, como IBM (DB2 forz/OS, to Amazon Relational Database Service (Amazon RDS). The authentication and authorization for the modernized print workflow is performed by AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD. The LRS Directory Information Server (LRS/DIS), integrada con AWS Managed Microsoft AD para la autenticación y autorización del flujo de trabajo de impresión. Al modernizar sus cargas de trabajo de impresión en línea, puede reducir los costos de infraestructura de TI, mitigar la carga técnica que supone el mantenimiento de los sistemas heredados, eliminar los silos de datos, aumentar la agilidad y la eficiencia con un DevOps modelo y aprovechar los recursos bajo demanda y la automatización en la nube de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una carga de trabajo de impresión en línea o administración de producción de mainframe
- Conocimientos básicos sobre cómo recompilar y entregar una aplicación de mainframe ejecutada en Micro Focus Enterprise Server (para obtener más información, consulte la hoja de datos de Enterprise Server en la documentación de Micro Focus).
- Conocimientos básicos de las soluciones y conceptos de impresión en la nube de LRS (para obtener más información, consulte Modernización de la producción en la documentación de LRS).

- Software y licencia de Micro Focus Enterprise Server (para obtener más información, póngase en contacto con el departamento de ventas de Micro Focus).
- VPSX/MFI, LRS/Queue, and LRS/DISSoftware y licencias de LRS (para obtener más información, póngase en contacto con el departamento de ventas de LRS).

> **Note**
>
> Para obtener más información sobre las consideraciones de configuración de las cargas de trabajo de impresión en línea de mainframe, consulte Consideraciones en la sección Información adicional de este patrón.

Versiones de producto

- Micro Focus Enterprise Server 8.0 o posterior
- LRS VPSX/MFI V1R3 o posterior

Arquitectura

Pila de tecnología de origen

- Sistema operativo: IBM z/OS
- Lenguaje de programación – Common Business-Oriented Language (COBOL), y Customer Information Control System (CICS)
- Base de datos: z/OS IBM DB2 para el sistema de gestión de la información (IMS) y el método de acceso al almacenamiento virtual (VSAM) de IBM
- Seguridad: Resource Access Control Facility (RACF), CA Top Secret para z/OS y Access Control Facility 2 () ACF2
- Gestión de impresión y salida: productos de z/OS impresión para mainframes de IBM (IBM Infoprint Server for z/OS, LRS y CA View)

Pila de tecnología de destino

- Sistema operativo: Microsoft Windows Server que se ejecuta en Amazon EC2
- Informática — Amazon EC2

- Lenguaje de programación – COBOL y CICS
- Bases de datos: Amazon RDS
- Seguridad: AWS Managed Microsoft AD
- Administración de impresión y producción: solución de impresión LRS en AWS
- Entorno de tiempo de ejecución de mainframe – Micro Focus Enterprise Server

Arquitectura de origen

En el siguiente diagrama se muestra una arquitectura de estado actual típica para una carga de trabajo de impresión en línea de mainframe.

El diagrama muestra el siguiente flujo de trabajo:

1. Los usuarios llevan a cabo transacciones comerciales en un sistema de participación (SoE) que se basa en una aplicación CICS de IBM escrita en COBOL.
2. El SoE invoca el servicio de mainframe, que registra los datos de las transacciones comerciales en una base de datos system-of-records (SoR), como IBM DB2 for z/OS.
3. El SoR conserva los datos comerciales del SoE.
4. Un usuario inicia una solicitud para generar un resultado de impresión desde el CICS SoE, que inicia una solicitud de transacción de impresión para procesar la solicitud de impresión.
5. La aplicación de transacciones de impresión (como un programa CICS y COBOL) extrae los datos de la base de datos, los formatea de acuerdo con los requisitos empresariales y genera resultados empresariales (datos impresos), como extractos de facturación, tarjetas de identidad o extractos de préstamos. A continuación, la aplicación envía una solicitud de impresión mediante el método de acceso virtual a las telecomunicaciones (VTAM). Un servidor de z/OS impresión (como IBM Infoprint Server) utiliza NetSpool o un componente VTAM similar para interceptar las solicitudes de impresión y, a continuación, crea conjuntos de datos de salida de impresión en la bobina de JES mediante los parámetros de salida de JES. Los parámetros de salida del JES especifican la información de enrutamiento que el servidor de impresión utiliza para transmitir la salida a una impresora de red determinada. El término VTAM se refiere al servidor de z/OS comunicaciones y al elemento de servicios de la arquitectura de red del sistema (SNA) de z/OS.
6. El componente de transmisión de la producción de impresión transmite los conjuntos de datos de impresión de salida desde la bobina JES a impresoras o servidores de impresión remotos, como LRS (como se demuestra en este patrón), IBM Infoprint Server o destinos de correo electrónico.

Arquitectura de destino

El siguiente diagrama muestra una arquitectura para una carga de trabajo de impresión en línea de mainframe que se implementa en la nube de AWS:

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario inicia una solicitud de impresión desde una interfaz de usuario en línea (CICS) para crear la producción de impresión, como extractos de facturación, tarjetas de identificación o extractos de préstamos.
2. La aplicación en línea de mainframe (rediseñada para Amazon EC2) utiliza el tiempo de ejecución de Micro Focus Enterprise Server para extraer datos de la base de datos de la aplicación, aplicar lógica empresarial a los datos, formatear los datos y, a continuación, enviar los datos a un destino de impresión mediante Micro Focus CICS Print Exit (DFHUPRNT).
3. La base de datos de la aplicación (un SoR que se ejecuta en Amazon RDS) conserva los datos para su impresión.
4. La solución de VPSX/MFI impresión LRS se implementa en Amazon EC2 y sus datos operativos se almacenan en Amazon Elastic Block Store (Amazon EBS). LRS VPSX/MFI usa un TCP/IP-based LRS/Queue transmission agent to collect print data through the Micro Focus CICS Print Exit API (DFHUPRNT) and deliver the data to a specified printer destination. The original TERMID (TERM) that's used in the modernized CICS application is used as the VPSX/MFI nombre de cola.

> **Note**
>
> La solución de destino no suele requerir cambios en la aplicación para adaptarla a los lenguajes de formato de mainframe, como IBM Advanced Function Presentation (AFP) o Xerox Line Condition Data Stream (LCDS). Para obtener más información sobre el uso de Micro Focus para la migración y modernización de aplicaciones de mainframe en AWS, consulte Potenciar las cargas de trabajo de mainframe empresarial en AWS con Micro Focus en la documentación de AWS.

Arquitectura de infraestructura de AWS

El siguiente diagrama muestra una arquitectura de infraestructura de AWS segura y de alta disponibilidad para una carga de trabajo de impresión en línea de mainframe:

En el diagrama, se muestra el siguiente flujo de trabajo:

1. La aplicación en línea para mainframe (escrita en un lenguaje de programación como CICS o COBOL) utiliza la lógica empresarial básica para procesar y generar la producción de impresión, como extractos de facturación, tarjetas de identidad y extractos de préstamos. La aplicación en línea se implementa en Amazon en dos zonas EC2 de disponibilidad (AZ) para una alta disponibilidad (HA) y utiliza Micro Focus CICS Print Exit para enrutar los resultados de impresión a LRS VPSX/MFI para que los impriman los usuarios finales.
2. LRS utiliza un comando. VPSX/MFI TCP/IP-based LRS/Queue transmission agent to collect or capture print data from the Micro Focus online Print Exit programming interface. Online Print Exit passes the necessary information to enable LRS VPSX/MFI to effectively process the print file and dynamically build LRS/Queue

> **Note**
>
> Para obtener más información sobre los distintos métodos de programación de aplicaciones CICS para la impresión y sobre su compatibilidad con Micro Focus Enterprise Server y LRS VPSX/MFI, consulte Captura de datos de impresión en la sección Información adicional de este patrón.

3.

> **Note**
>
> Un Network Load Balancer proporciona un nombre DNS para integrar Micro Focus Enterprise Server con LRS VPSX/MFI. : LRS VPSX/MFI supports a Layer 4 load balancer. The Network Load Balancer also does a basic health check on LRS VPSX/MFI y enruta el tráfico a los destinos registrados que están en buen estado.

4. El servidor de VPSX/MFI impresión LRS se implementa en Amazon en EC2 dos zonas de disponibilidad para alta disponibilidad y utiliza Amazon EBS como almacén de datos operativos. El LRS VPSX/MFI admite los modos de servicio activo-activo y activo-pasivo. Esta arquitectura utiliza varias zonas de disponibilidad en un par activo-pasivo como activo y modo de espera activa. El Network Load Balancer realiza una comprobación del estado de las VPSX/MFI EC2 instancias LRS y enruta el tráfico a las instancias activas en espera en otra zona de disponibilidad si una instancia activa se encuentra en mal estado. Las solicitudes de impresión se conservan en la cola de trabajos del LRS de forma local en cada una de las instancias. EC2 En caso de recuperación,

se debe reiniciar una instancia fallida para que los servicios de LRS reanuden el procesamiento de la solicitud de impresión.

> **Note**
>
> El LRS también VPSX/MFI puede realizar comprobaciones de estado a nivel de flota de impresoras. Para obtener más información, consulte Comprobaciones de estado de la flota de impresoras en la sección de Información adicional de este patrón.

5. AWS Managed Microsoft AD se integra LRS/DIS para llevar a cabo la autenticación y autorización del flujo de trabajo de impresión. Para obtener más información, consulte Autenticación y autorización de impresión en la sección de Información adicional de este patrón.
6. LRS VPSX/MFI utiliza Amazon EBS para el almacenamiento en bloque. Puede hacer copias de seguridad de los datos de Amazon EBS de EC2 las instancias activas en Amazon S3 como point-in-time instantáneas y restaurarlos en volúmenes de EBS activos en espera. Para automatizar la creación, retención y eliminación de instantáneas de volúmenes de Amazon EBS, puede usar Amazon Data Lifecycle Manager para establecer la frecuencia de las instantáneas automatizadas y restaurarlas en función de sus necesidades de RTO/RPO.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento a nivel de bloques para su uso con las instancias de Amazon. EC2 Los volúmenes de EBS se comportan como dispositivos de bloques sin formatear. Puede montar estos volúmenes como dispositivos en sus instancias.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- AWS Directory Service para Microsoft Active Directory (AD), también conocido como AWS Managed Microsoft Active Directory, permite que sus cargas de trabajo compatibles con directorios y los recursos de AWS utilicen Active Directory administrado en AWS.

Otras herramientas

- LRS VPSX/MFI (Micro Focus Interface), una interfaz desarrollada conjuntamente por LRS y Micro Focus, captura la producción de una bobina JES de Micro Focus Enterprise Server y la entrega de forma fiable a un destino de impresión específico.
- El servidor de información de directorio LRS (LRS/DIS) se utiliza para la autenticación y la autorización durante el flujo de trabajo de impresión.
- LRS/Queue is a TCP/IP-based LRS/Queue transmission agent, used by LRS VPSX/MFI, para recopilar o capturar datos de impresión a través de la interfaz de programación Print Exit en línea de Micro Focus.
- Micro Focus Enterprise Server es un entorno de implementación de aplicaciones para aplicaciones de mainframe. Proporciona el entorno de ejecución para las aplicaciones de mainframe que se migran o crean con cualquier versión de Micro Focus Enterprise Developer.

Epics

Configure Micro Focus Enterprise Server en Amazon EC2 e implemente una aplicación en línea para mainframe

Tarea	Descripción	Habilidades requeridas
Configure Micro Focus Enterprise Server e implemente una aplicación en línea de demostración.	Configure Micro Focus Enterprise Server en Amazon y EC2, a continuación, despliegue la aplicación Micro Focus Account Demo (ACCT Demo) en Amazon EC2 siguiendo las instrucciones del Tutorial: CICS Support de la documentación de Micro Focus. La aplicación ACCT Demo es una aplicación en línea para mainframe (CICS) que	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	crea y, a continuación, inicia la producción de impresión.	

Configurar un servidor de impresión LRS en Amazon EC2

Tarea	Descripción	Habilidades requeridas
Obtenga una licencia de producto LRS para imprimir.	Para obtener una licencia de producto LRS para LRSVPSX/MFI, LRS/Queue, and LRS/DIS, póngase en contacto con el equipo de gestión de producción de LRS. Debe proporcionar los nombres de host de las EC2 instancias en las que se instalarán los productos de LRS.	Responsable de compilación
Cree una instancia de Amazon EC2 Windows para instalar LRS VPSX/MFI.	Para lanzar una instancia de Amazon EC2 Windows, sigue las instrucciones del paso 1: lanzar una instancia de la EC2 documentación de Amazon. La instancia debe cumplir los siguientes requisitos de hardware y software para LRS VPSX/MFI: • CPU: doble núcleo • RAM: 16 GB • Unidad: 500 GB • EC2 Instancia mínima: m5.xlarge	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	• Sistema operativo: Windows/Linux • Software: Servicio de Información de Internet (IIS) o Apache **Note** Los requisitos de hardware y software anteriores están pensados para una flota de impresoras pequeña (entre 500 y 1000). Para conocer todos los requisito s, consulte a sus personas de contacto en LRS y AWS. Cuando cree la instancia de Windows, haga lo siguiente: 1. Confirme que el nombre de EC2 host es el mismo nombre de host utilizado para la licencia del producto LRS. 2. Para activar CGI en Amazon EC2 , sigue estos pasos: a. Conéctate a tu EC2 instancia siguiendo las	

Tarea	Descripción	Habilidades requeridas
	instrucciones del paso 2: Conéctate a tu instancia en la EC2 documentación de Amazon. b. En el menú Inicio de Windows, busque y abra Server Manager. c. En el panel de Server Manager, elija Panel de control, Inicio rápido, Agregar roles y características. A continuación, seleccione Roles de servidor. d. En Funciones de servidor, selecciona WebServer (IIS) y, a continuación, seleccion a Desarrollo de aplicaciones. e. En Desarrollo de aplicaciones, seleccione la casilla CGI. f. Siga las instrucciones del asistente para Agregar roles y características de Windows Server Manager para instalar CGI. g. Abra el puerto 5500 en el firewall de Windows de la EC2 instancia para la	

Tarea	Descripción	Habilidades requeridas
	LRS/Queue comunicación.	

Tarea	Descripción	Habilidades requeridas
Instale LRS VPSX/MFI en la EC2 instancia.	1. Conéctate a tu EC2 instancia siguiendo las instrucciones del paso 2: Conéctate a tu instancia en la EC2 documentación de Amazon. 2. **Note** Abra el enlace a la página de descarga del producto que se incluye en el correo electrónico de LRS que debería haber recibido. : Los productos de LRS se distribuyen mediante transfere ncia de archivos electrónica (EFT). 3. Descarga LRS VPSX/MFI y descomprime el archivo (carpeta predeterminada:`c:\LRS`). 4. Inicie el instalador de productos LRS desde la carpeta descomprimida para instalar LRS VPSX/MFI. 5. En el menú Seleccionar características, seleccione VPSX® Server (V1R3.022) y, a continuación, seleccion	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	e Siguiente para iniciar el proceso de instalaci ón. Cuando se complete la instalación, recibirá un mensaje de confirmación.	
Instale LRS/Queue.	1. Conéctese a su EC2 instancia de Micro Focus Enterprise Server siguiendo las instrucciones del paso 2: Conéctese a su instancia en la EC2 documentación de Amazon. 2. Abra el enlace a la página de descarga del producto LRS desde el correo electrónico de LRS que debería recibir, descargue LRS/Queue y, a continuac ión, descomprima el archivo. 3. Vaya a la ubicación en la que descargó los archivos y, a continuación, inicie el instalador del producto LRS para instalar LRS/Queue.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Instale LRS/DIS.	1. Conéctate a tu VPSX/MFI EC2 instancia de LRS siguiendo las instrucciones del paso 2: Conéctate a tu instancia en la EC2 documentación de Amazon. 2. Abra el enlace a la página de descarga del producto LRS que se incluye en el correo electrónico de LRS que habrá recibido, descargue LRS/DIS y, a continuación, descomprima el archivo. 3. Vaya a la ubicación en la que descargó los archivos y, a continuación, inicie el instalador de producto de LRS. 4. En el instalador de producto de LRS, amplíe LRS Misc Tools, seleccione LRS DIS y, a continuación, Siguiente. 5. Siga el resto de las instrucciones del instalador del producto de LRS para completar el proceso de instalación.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Cree un grupo objetivo y registre LRS VPSX/MFI EC2 como destino.	Cree un grupo de destino siguiendo las instrucciones de Crear un grupo de destino para el equilibrador de carga de red en la documentación en el equilibrador de carga de red elástico. Al crear el grupo de destino, haga lo siguiente: 1. En la página Especific ar detalles del grupo, seleccione un Tipo de destino y luego, Instancias. 2. En Protocol, seleccione TCP. 3. En Puerto, seleccione 5500. 4. En la página Registrar destinos, en la sección Instancias disponibles, seleccione las instancias del LRS. VPSX/MFI EC2	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Crear un equilibrador de carga de red.	Siga las instrucciones de Crear un equilibrador de carga de red en la documentación de Elastic Load Balancing. Su Network Load Balancer dirige el tráfico de Micro Focus Enterprise Server a LRS. VPSX/MFI EC2 Al crear el equilibrador de carga de red, siga los pasos siguientes en la página Listeners and Routing (Oyentes y enrutamiento): 1. En Protocol, seleccione TCP. 2. En Puerto, seleccione 5500. 3. En Default action (Acción predeterminada), seleccione Forward to (Reenviar a) para el grupo de destino que ha creado.	Arquitecto de la nube

Integre Micro Focus Enterprise Server con LRS y LRS/Queue VPSX/MFI

Tarea	Descripción	Habilidades requeridas
Configure Micro Focus Enterprise Server para la integración. LRS/Queue	1. Conéctese a su EC2 instancia de Micro Focus Enterprise Server siguiendo las instrucciones del paso 2: Conéctese a su instancia	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	en la EC2 documentación de Amazon. 2. En el menú Start (Inicio) de Windows, abra la interfaz de usuario de administración de Micro Focus Enterprise Server. 3. En la barra de menús, seleccione NATIVE. 4. En el panel de navegación, seleccione Directory Server y, a continuación, BANKDEMO o su región de Enterprise Server. 5. En General en el panel de navegación izquierdo, despláce hacia abajo hasta la sección Adicional para configurar las variables de entorno (LRSQ_ADDRESS, LRSQ_PORT, LRSQ_COMMAND) para que dirijan hacia LRSQ. 6. Para LRSQ_ADDRESS, escriba la dirección IP o el nombre DNS del equilibrador de carga de red que creó anteriormente. 7. Para LRSQ_PORT, especifique VPSX LRSQ Listener Port (5500).	

Tarea	Descripción	Habilidades requeridas
	8. Para LRSQ_COMMAND, especifique la ubicación de la ruta del ejecutable de LRSQ. 9. **Note** Actualmente, LRS admite un límite máximo de 50 caracteres para los nombres de DNS, pero este aspecto cambiará en el futuro. Si el nombre DNS tiene más de 50 caracteres, puede utilizar la dirección IP del equilibrador de carga de red como alternativa.	

Tarea	Descripción	Habilidades requeridas
Haga que CICS Print Exit (DFHUPRNT) esté disponible para la inicialización de Micro Focus Enterprise Server.	1. Conéctese a su EC2 instancia de Micro Focus Enterprise Server siguiendo las instrucciones del paso 2: Conéctese a su instancia en la EC2 documentación de Amazon. 2. **Note** Copie CICS Print Exit (DFHUPRNT) de la carpeta VPSX/MFI ejecutable del LRS (denomina daVPSX_MFI_R2) a la ubicación de la instancia de Micro Focus Enterprise Server. EC2 Para los sistemas de 32 bits, la ubicación es `C:\Program Files (x86)\Micro Focus\Enterprise Server\bin` . Para los sistemas de 64 bits, la ubicación es `C:\Program Files (x86)\Micro Focus\Enterprise Server\bin64` .:	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Se debe cambiar el nombre del archivo `DFHUPRNT_64.dll` a `DFHUPRNT.dll` al copiarlo. Comprobar que Micro Focus Enterprise Server haya detectado CICS Print Exit (DFHUPRNT) 1. Detenga e inicie Micro Focus Enterprise Server. 2. En el panel de administración de Micro Focus Enterprise Server, abra Supervisar, Registros, Registros de consola. 3. Compruebe si aparece el siguiente mensaje en los registros de la consola: “El usuario de la impresora 3270 salió correctamente de DFHUPRNT y se instaló correctamente”.	

Tarea	Descripción	Habilidades requeridas
Defina el ID de terminal de la impresora CICS (TERMIDs) como Micro Focus Enterprise Server.	Habilitar la impresión 3270 en Micro Focus Enterprise Server 1. En el panel de administración de Micro Focus Enterprise Server, abra CICS, Recuros, Por grupo. 2. En el panel de navegación izquierdo, seleccione SIT (tabla de inicialización del sistema) y, a continuación, seleccione BNKCICV. 3. En la sección General, desplácese hacia abajo hasta 3270 y, a continuación, seleccione la casilla Imprimir 3270. Defina el terminal de la impresora CICS en Micro Focus Enterprise Server 1. En el panel de administración de Micro Focus Enterprise Server, abra CICS, Recursos, Por tipo. 2. En el panel de navegación izquierdo, seleccione Término y, a continuación, Nuevo. Se abre el formulario Crear recurso de terminal. 3. En Nombre, introduzca el nombre de la cola de impresión del LRS. (Nota:	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Este patrón utiliza "P275" como ID de terminal de la impresora CICS y la cola de impresión LRS VPSX). 4. Para Grupo, introduzca BANKTERM. 5. Para Instalación automátic a: Modelo, introduzca NO. 6. En Identificadores de terminal: tipo de terminal, introduzca. DFHPRT32 7. En Nombre de red, introduzca VTAMP275. 8. Para el Uso del terminal, seleccione la casilla En servicio. 9. Desplácese hasta la parte superior de la página y, a continuación, seleccione Guardar. 10. Elija Instalar. Se muestra un mensaje emergente que indica que la instalación se ha realizado correctamente.	

Configure impresoras y usuarios de impresión en Micro Focus Enterprise Server y LRS VPSX/MFI

Tarea	Descripción	Habilidades requeridas
Cree una cola de impresión en LRS VPSX.	1. Conéctate a tu VPSX/MFI EC2 instancia de LRS siguiendo las instrucci ones del paso 2: Conéctate	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	a tu instancia en la EC2 documentación de Amazon. 2. Abra la interfaz web de VPSX desde el menú Inicio de Windows. 3. En el panel de navegación, seleccione Impresoras. 4. Seleccione Agregar y, a continuación, Agregar impresora. 5. En la página de Configura ción de la impresora, en Nombre de impresora, introduzca P275. 6. Para el ID de VPSX, introduzca. VPS1 7. Para CommType, seleccion e TCPIP/LRSQ. 8. En Host/Dirección IP, introduzca la dirección IP de la impresora física que desee agregar. 9. En Dispositivo, introduzca el nombre de su dispositivo. 10. Seleccione Controlador de Windows o Controlador de Linux/Mac. 11. Elija Agregar.	

Tarea	Descripción	Habilidades requeridas
	Note La cola de impresión debe ser equivalente a la impresión TERMIDs creada en Micro Focus Enterprise Server.	

Tarea	Descripción	Habilidades requeridas
Cree un usuario de impresión en LRS VPSX/MFI.	1. Conéctate a tu VPSX/MFI EC2 instancia de LRS siguiendo las instrucciones del paso 2: Conéctate a tu instancia en la EC2 documentación de Amazon. 2. Abra la interfaz web de VPSX desde el menú Inicio de Windows. 3. En el panel de navegación, elija Seguridad y luego elija la opción Usuarios. 4. En la columna Nombre de usuario, seleccione admin y, a continuación, seleccione Copiar. 5. En la ventana Mantenimiento del perfil de usuario, en Nombre de usuario, introduzca un nombre de usuario (por ejemplo, PrintUser). 6. En Descripción, escriba una descripción breve (por ejemplo, Usuario para impresión de prueba). 7. Seleccione Update (Actualizar). Esto crea un usuario de impresión (por ejemplo, PrintUser). 8. En el panel de navegación, en Usuario, seleccion	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	e el nuevo usuario que ha creado. 9. En el menú Comandos, seleccione Seguridad. 10. En la página Reglas de seguridad, seleccione todas las opciones de seguridad de la impresora y seguridad laboral aplicables y, a continuación, seleccione Guardar. 11. Para añadir el nuevo usuario de impresión al grupo Administrador, vaya al panel de navegación, seleccione Seguridad y, a continuación, seleccione Configurar. 12. En la ventana Configuración de seguridad, añada su nuevo usuario de impresión a la columna Administrador.	

Configure imprimir autenticación y autorización

Tarea	Descripción	Habilidades requeridas
Cree un dominio de AWS Managed Microsoft AD con usuarios y grupos.	1. Para crear un directorio Active en AWS Managed Microsoft AD, siga las instrucciones de ree su directorio de AWS	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Managed Microsoft AD en la documentación de AWS Directory Service. 2. Implemente una EC2 instancia (administrador de Active Directory) e instale las herramientas de Active Directory para administr ar su AD de Microsoft administrado por AWS siguiendo las instrucciones del paso 3: Implementar una EC2 instancia para administrar su AD de Microsoft administrado por AWS que aparecen en la documentación de AWS Directory Service. 3. **Note** Conéctate a tu EC2 instancia siguiendo las instrucciones del paso 2: Conéctate a tu instancia en la EC2 documenta ción de Amazon. : Cuando te conectes a la EC2 instancia , introduce tus credenciales de administrador (para el directorio que creaste en el primer	

Tarea	Descripción	Habilidades requeridas
	paso) en la ventana de seguridad de Windows. 4. En el menú Inicio de Windows, bajo Herramientas administrativas de Windows, seleccione Usuarios y equipos de Active Directory. 5. Cree un usuario de impresión en el dominio de Active Directory siguiendo los pasos de Crear un usuario de la documentación de AWS Directory Service.	
Une LRS VPSX/MFI EC2 a un dominio de Microsoft AD gestionado por AWS.	Une LRS VPSX/MFI EC2 a tu dominio de Microsoft AD gestionado por AWS de forma automática (documentación del AWS Knowledge Center) o manualmente (documentación de AWS Directory Service).	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Configure e integre LRS/DIS con AWS Managed Microsoft AD.	1. Conéctate a tu VPSX/MFI EC2 instancia de LRS siguiendo las instrucciones del paso 2: Conéctate a tu instancia en la EC2 documentación de Amazon. 2. En el menú Inicio de Windows , abra la Interfaz web de VPSX. 3. En el panel de navegación, seleccione Seguridad y, a continuación, la opción Configurar. 4. En la página Security Configuration, busque la sección Security Parameters y, en Security Type, seleccione Internal. 5. Especifique sus preferencias para el resto de las opciones en la sección Parámetros de seguridad. 6. En el menú Start (Inicio) de Windows, abra la carpeta LRS Output Management, seleccione Server Start y, a continuación, Server Stop. 7. Inicie sesión en LRS VPSX/MFI con su nombre de usuario y contraseña de Active Directory.	Arquitecto de la nube

Probar un flujo de trabajo de impresión en línea

Tarea	Descripción	Habilidades requeridas
Inicie una solicitud de impresión en línea desde la aplicación Micro Focus ACCT Demo.	1. **Note** Abra el emulador de terminal TN327 0 en su EC2 instancia de Micro Focus Enterprise Server. (: Este patrón utiliza emuladores de terminal 3270). 2. Conéctate al emulador de terminal TN327 0 (Rumba). Para la Dirección del nombre de host, utilice 127.0.0.1. Para el Puerto Telnet, utilice 9270. 3. Tras conectarse a la pantalla 3270, presione CTL+SHIFT+Z para borrar la pantalla. 4. Para iniciar la aplicació n ACCT Demo, en una pantalla transparente, introduzca ACCT. Esto abre la pantalla principal de la aplicación ACCT Demo online (CICS). Nota: La pantalla principal incluye opciones de menú como el Archivo de cuenta, Para buscar por nombre,	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	introducir, Tipo de solicitud, Cuenta e Impresora. 5. Para enviar una solicitud de impresión desde la aplicación ACCT Demo Online (CICS), introduzc a P en el campo tipo de solicitud, 11111 en el campo cuenta y P275 en el campo impresora. Asegúrese de establece r el valor del campo de la impresora en el valor del ID de terminal de la impresora CICS. 6. Pulse Intro. El mensaje “Solicitud de impresión programada” se muestra en la parte inferior de la pantalla. Esto confirma que se generó una solicitud de impresión en línea desde la aplicación ACCT Demo y se envió a LRS VPS/MFI para su procesamiento de impresión.	

Tarea	Descripción	Habilidades requeridas
Compruebe la producción de impresión en LRS VPSX/MFI.	1. Conéctate a tu VPSX/MFI EC2 instancia de LRS siguiendo las instrucciones del paso 2: Conéctate a tu instancia en la EC2 documentación de Amazon. 2. En el menú Inicio de Windows, abra la Interfaz web de VPSX. 3. En el panel de navegación, seleccione Impresoras y, a continuación, seleccione Cola de producción. Busque la cola de impresión P275 que creó anteriormente para la impresión en línea. 4. Para la cola de impresión (P275), en la columna ID de bobina, seleccione el ID de bobina para la solicitud de la cola de impresoras. 5. En la pestaña Acciones, en la columna COMANDO, seleccione Examinar. Ahora puede ver el resultado de impresión de un extracto de cuenta con columnas para el número de cuenta, el apellido, el nombre, la dirección, el teléfono, el número de tarjetas emitidas, la	Ingeniero de pruebas

Tarea	Descripción	Habilidades requeridas
	fecha de emisión, el importe y el saldo. Para ver un ejemplo, consulte el archivo adjunto online_print_output para ver este patrón.	

Recursos relacionados

- Modernización de la producción de LRS (documentación de LRS)
- Conceptos de redes VTAM (documentación de IBM)
- Resumen de los tipos de unidades lógicas (LU) (documentación de IBM)
- Controles ANSI y de carro de máquinas (documentación de IBM)
- Capacitación de las cargas de trabajo de mainframe empresariales en AWS con Micro Focus (blog de AWS Partner Network)
- Cree un PAC para servidores empresariales de Micro Focus con Amazon EC2 Auto Scaling y Systems Manager (documentación de AWS Prescriptive Guidance)
- Flujo de datos de Presentación de funciones avanzadas (AFP) (documentación de IBM)
- Flujo de datos condicionado por línea (LCDS) (documentación de Compart)

Información adicional

Consideraciones

Durante su proceso de modernización, puede considerar una amplia variedad de configuraciones para los procesos en línea del mainframe y la producción que generan. Todos los clientes y proveedores que utilizan la plataforma de mainframe la han personalizado con requisitos particulares que afectan directamente a la impresión. Por ejemplo, su plataforma actual puede incorporar Advanced Function Presentation (AFP) de IBM o Line Condition Data Stream (LCDS) de Xerox en el flujo de trabajo actual. Además, los caracteres de control de carro de mainframe y las palabras de comando de canal pueden afectar al aspecto de la página impresa y pueden requerir un tratamiento especial. Como parte del proceso de planificación de la modernización, le recomendamos evaluar y comprender las configuraciones de su entorno de impresión específico.

Captura de datos de impresión

En esta sección se resumen los métodos de programación de aplicaciones CICS que puede utilizar en un entorno de mainframe de IBM para la impresión. Los VPSX/MFI componentes del LRS proporcionan técnicas que permiten a los mismos programas de aplicación crear datos de la misma manera. En la siguiente tabla se describe cómo se admite cada método de programación de aplicaciones en una aplicación CICS modernizada que se ejecuta en AWS y Micro Focus Enterprise Server con un servidor de impresión LRS VPSX/MFI .

Método	Description (Descripción)	Soporte para el método en un entorno modernizado
EXEC CICS SEND TEXT.. or EXEC CICS SEND MAP..	Estos métodos CICS y VTAM son responsables de crear y entregar los flujos de datos de impresión 3270/SCS a los dispositivos de impresión LUTYPE0 y a los dispositivos de impresión. LUTYPE1 LUTYPE3	La interfaz de programa de aplicación (API) Online Print Exit (DFHUPRNT) de Micro Focus permite procesar los datos de impresión al crear flujos de datos de impresión 3270/SCS mediante VPSX/MFI cualquiera de estos métodos.
EXEC CICS SEND TEXT.. or EXEC CICS SEND MAP.. (con software de mainframe de IBM de terceros)	Los métodos CICS y VTAM se encargan de crear y entregar los flujos de datos de impresión 3270/SCS a los dispositivos de impresión LUTYPE0 y a los dispositivos de impresión. LUTYPE1 LUTYPE3 Los productos de software de terceros intercept an los datos de impresión, los convierten en datos de formato de impresión estándar con un carácter de ASA/MCH control y colocan los datos en la bobina JES para	La API Print Exit online (DFHUPRNT) de Micro Focus permite procesar los datos de impresión antes de crear flujos de datos de impresión VPSX/MFI 3270/SCS mediante uno de estos métodos.

	que los procesen sistemas de impresión basados en ordenadores centrales que utilizan JES.	
EXEC CICS SPOOLOPEN	Los programas de aplicación CICS utilizan este método para escribir datos directamente en la bobina JES. A continuación, los datos están disponibles para ser procesados por sistemas de impresión basados en mainframe que utilizan JES.	Micro Focus Enterprise Server envía los datos a la bobina de Enterprise Server, donde los puede procesar VPSX/MFI Batch Print Exit (LRSPRTE6), que envía los datos a VPSX.
DRS/API	Se utiliza una interfaz de programación proporcionada por LRS para escribir los datos de impresión en JES.	VPSX/MFI proporciona una interfaz de reemplazo que envía los datos de impresión directamente al VPSX.

Comprobación de estado de la flota de impresoras

El LRS VPSX/MFI (LRS LoadX) puede realizar exhaustivas comprobaciones de estado, incluidas la gestión de los dispositivos y la optimización operativa. La administración de dispositivos puede detectar un error en un dispositivo de impresión y dirigir la solicitud de impresión a una impresora en buen estado. Para obtener más información sobre las comprobaciones de estado exhaustivas de las flotas de impresoras, consulte la documentación de LRS que se incluye con la licencia del producto.

Imprimir autenticación y autorización

LRS/DIS enables LRS applications to authenticate user IDs and passwords by using Microsoft Active Directory or an LDAP server. In addition to basic print authorization, LRS/DIStambién puede aplicar controles de seguridad de impresión de nivel granular en los siguientes casos de uso:

- Gestione quién puede examinar el trabajo de impresión.
- Gestione el nivel de navegación de los trabajos de otros usuarios.

- Gestione las tareas operativas. Por ejemplo, la seguridad a nivel de comandos, como retener o liberar, purgar, modificar, copiar y redirigir. La seguridad se puede configurar mediante el ID de usuario o el grupo (similar al grupo AD o al grupo LDAP).

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Mover los archivos de mainframe directamente a Amazon S3 mediante Transfer Family

Luis Gustavo Dantas, Amazon Web Services

Resumen

Como parte del proceso de modernización, puede afrontar el desafío de transferir archivos entre sus servidores en las instalaciones y la nube de Amazon Web Services (AWS). La transferencia de datos desde mainframes puede suponer un desafío importante, ya que los mainframes normalmente no pueden acceder a los almacenes de datos modernos como Amazon Simple Storage Service (Amazon S3), Amazon Elastic Block Store (Amazon EBS) o Amazon Elastic File System (Amazon EFS).

Muchos clientes utilizan recursos de almacenamiento provisional intermedios, como servidores Linux, Unix o Windows en las instalaciones, para transferir archivos a la nube de AWS. Puede evitar este método indirecto si utiliza AWS Transfer Family con el protocolo de File Transfer (SFTP) de Secure Shell (SSH) para cargar archivos de mainframe directamente a Amazon S3.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una nube privada virtual (VPC) con una subred a la que pueda acceder la plataforma antigua
- Un punto de conexión de Transfer Family para su VPC
- Archivos del método de acceso al almacenamiento virtual (VSAM) de mainframe convertidos en archivos de longitud fija secuenciales (documentación de IBM)

Limitaciones

- SFTP transfiere los archivos en modo binario de forma predeterminada, lo que significa que los archivos se cargan en Amazon S3 conservando la codificación EBCDIC. Si el archivo no contiene datos binarios o empaquetados, puede utilizar el sftp ascii subcommand (documentación de IBM) para convertir los archivos en texto durante la transferencia.
- Debe desempaquetar los archivos de mainframe (Recomendaciones de AWS) que contengan contenido empaquetado y binario para poder utilizar estos archivos en el entorno de destino.

- El tamaño de los objetos de Amazon S3 puede oscilar entre un mínimo de 0 bytes y un máximo de 5 TB. Para obtener más información sobre las capacidades de Amazon S3, consulte Amazon S3 FAQs.

Arquitectura

Pila de tecnología de origen

- Lenguaje de control de tareas (JCL)
- Intérprete de comandos e ISPF para z/OS Unix
- SFTP
- VSAM y archivos planos

Pila de tecnología de destino

- Transfer Family
- Amazon S3
- Amazon Virtual Private Cloud (Amazon VPC)

Arquitectura de destino

El diagrama siguiente muestra una arquitectura de referencia para usar Transfer Family con SFTP para cargar archivos de mainframe directamente a un bucket de S3.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Se utiliza un trabajo de JCL para transferir los archivos de mainframe del mainframe heredado a la nube de AWS a través de Direct Connect.
2. Direct Connect permite que el tráfico de la red permanezca en la red global de AWS y evite la Internet pública. Direct Connect también mejora la velocidad de la red, empezando en 50 Mbps y escalando verticalmente hasta 100 Gbps.
3. El punto de conexión de VPC permite las conexiones entre los recursos de la VPC y los servicios compatibles sin utilizar la Internet pública. El acceso a Transfer Family y Amazon S3 logra una alta disponibilidad al realizarse a través de las interfaces de red elásticas ubicadas en dos subredes privadas y zonas de disponibilidad.

4. Transfer Family autentica a los usuarios y usa SFTP para recibir los archivos del entorno heredado y moverlos a un bucket de S3.

Automatizar y escalar

Una vez implementado el servicio Transfer Family, puede transferir un número ilimitado de archivos desde el mainframe a Amazon S3 utilizando un trabajo de JCL como cliente SFTP. También puede automatizar la transferencia de archivos mediante el uso de un programador de trabajos por lotes del mainframe para ejecutar los trabajos de SFTP cuando esté todo a punto para transferir los archivos del mainframe.

Tools (Herramientas)

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.
- AWS Transfer Family le permite escalar de forma segura sus transferencias de business-to-business archivos recurrentes a Amazon S3 y Amazon EFS mediante los protocolos SFTP, FTPS y FTP.

Epics

Crear el bucket de S3 y la política de acceso

Tarea	Descripción	Habilidades requeridas
Cree el bucket de S3.	Cree un bucket de S3 para alojar los archivos que transfiera desde su entorno anterior.	AWS general
Cree una política y un rol de IAM.	Transfer Family utiliza el rol de AWS Identity and Access Management (IAM) para conceder acceso al bucket de	AWS general

Tarea	Descripción	Habilidades requeridas
	S3 que se creó con anteriori dad. Cree un rol de IAM que incluya la siguiente política de IAM: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "UserFolderListing", "Action": [ "s3:ListBucket", "s3:GetBucketLocation" ], "Effect": "Allow", "Resource": [ "arn:aws:s3:::<your-bucket-name>" ] }, { "Sid": "HomeDirObjectAccess", "Effect": "Allow", "Action": [ "s3:PutObject", "s3:GetObjectAcl",`	

Tarea	Descripción	Habilidades requeridas

	<pre>"s3:GetObject",
	
	"s3:DeleteObjectVersion",
	
	"s3:DeleteObject",
	
	"s3:PutObjectAcl",
	
	"s3:GetObjectVersion"
	],
	"Resource":
	"arn:aws:s3:::<your-bucket-name>/*"
	}
	]
	}</pre>
	Note
	Debe elegir el caso de uso de Transfer al crear el rol de IAM.	

Definir el servicio de transferencia

Tarea	Descripción	Habilidades requeridas
Cree el servidor SFTP.	1. Inicie sesión en la consola de administración de AWS, abra la consola Transfer Family y, a continuación, seleccione Create server (Crear servidor).	AWS general

Tarea	Descripción	Habilidades requeridas
	2. Seleccione únicamente SFTP (SSH File Transfer Protocol) - file transfer over Secure Shell protocol (SFTP [Protocolo de transferencia de archivos SSH]: transferencia de archivos a través del protocolo Secure Shell) y, a continuación, elija Next (Siguiente). 3. En Identity provider (Proveedor de identidad), seleccione Service managed (Administ rado por el servicio) y, a continuación, Next (Siguient e). 4. En Endpoint Type (Tipo de punto de conexión), seleccione VPC hosted (Alojado en VPC). 5. En Access (Acceso), seleccione Internal. 6. En VPC, elija su VPC. 7. En la sección Availability Zones (Zonas de disponibi lidad), seleccione sus zonas de disponibilidad y subredes. 8. En la sección Security Groups (Grupos de seguridad), seleccione su grupo de seguridad y, a	

Tarea	Descripción	Habilidades requeridas
	continuación, Next (Siguiente). 9. En Domain (Dominio, seleccione Amazon S3 y, a continuación, Next (Siguiente). 10. Deje las opciones predeterminadas en la página Configure additional details (Configurar detalles adicionales) y, a continuación, seleccione Next (Siguiente). 11. Seleccione Create server (Crear servidor). **Note** Para obtener más información sobre cómo configurar un servidor SFTP, consulte Create an SFTP-enabled server (Guía del usuario de AWS Transfer Family).	

Tarea	Descripción	Habilidades requeridas
Obtenga la dirección del servidor.	1. Abra la consola de Transfer Family y seleccione el ID de servidor en la columna Server ID. 2. En la sección Endpoint details (Detalles del punto de conexión), en Endpoint type (Tipo de punto de conexión), seleccione el ID del punto de conexión. Esto dirige a la consola de Amazon VPC. 3. En la pestaña Details (Detalles) de la consola de Amazon VPC, busque los nombres DNS junto a DNS names.	AWS general
Cree el par de claves del cliente SFTP.	Cree un key pair de claves SSH para Microsoft Windows o macOS/Linux/UNIX.	AWS general, SSH

Tarea	Descripción	Habilidades requeridas
Cree el servidor SFTP.	1. Abra la consola de Transfer Family, seleccione Servers en el panel de navegación y, a continuación, seleccione su servidor. 2. En la columna Server ID, seleccione el ID de servidor para su servidor y, a continuación, Add user (Agregar usuario). 3. En Username (Nombre de usuario), escriba un nombre de usuario que coincida con el nombre de usuario del par de claves SSH. 4. En Role, seleccione el rol de IAM que creó anteriormente. 5. En Home directory (Directorio principal), seleccione el bucket de S3 que creó anteriormente. 6. En SSH public keys (Claves SSH públicas), escriba el par de claves que creó anteriormente. 7. Elija Agregar.	AWS general

Transferir el archivo de mainframe

Tarea	Descripción	Habilidades requeridas

Envíe la clave privada SSH a la computadora central.	Utilice SFTP o SCP para enviar la clave privada SSH al entorno heredado.
	
	Ejemplo de SFTP:
	
	`sftp [USERNAME@mainframeIP]`
	`[password]`
	`cd [/u/USERNAME]`
	`put [your-key-pair-file]`
	
	Ejemplos de SCP:
	
	`scp [your-key-pair-file] [USERNAME@MainframeIP]:/[u/USERNAME]`
	
	A continuación, guarde la clave SSH en el sistema de archivos z/OS Unix con el nombre de usuario que ejecutará más adelante el trabajo de transferencia de archivos por lotes (por ejemplo,). `/u/CONTROLM`
	
	Note
	Para obtener más información sobre el shell de z/OS Unix, consulte Introducción a los z/OS shell
		Computadora central, shell de z/OS Unix, FTP, SCP

Tarea	Descripción	Habilidades requeridas
	(documentación de IBM).	

Tarea	Descripción	Habilidades requeridas

Cree el cliente SFTP de JCL.	Como los mainframes no tienen un cliente SFTP nativo, debe usar la utilidad BPXBATCH para ejecutar el cliente SFTP desde el shell de Unix. z/OS
	
	En el editor ISPF, cree el cliente SFTP JCL. Por ejemplo:
	
	`//JOBNAM JOB ...`
	`//************`
	`******************`
	`******************`
	`******************`
	`****`
	`//SFTP EXEC PGM=BPXBA`
	`TCH,REGION=0M`
	`//STDPARM DD *`
	`SH cp "//'MAINF`
	`RAME.FILE.NAME'"`
	` filename.txt;`
	`echo 'put filename.txt'`
	` > uplcmd;`
	`sftp -b uplcmd -i`
	` ssh_private_key_fi`
	`le ssh_username@<tran`
	`sfer service ip or`
	` DNS>;`
	`//SYSPRINT DD SYSOUT=*`
	`//STDOUT DD SYSOUT=*`
	`//STDENV DD *`
	`//STDERR DD SYSOUT=*`
	
	Note
	
	Para obtener más información sobre
		JCL, Mainframe, shell de Unix z/OS

Tarea	Descripción	Habilidades requeridas
	cómo ejecutar un comando en el shell de z/OS Unix, consulte La utilidad BPXBATCH (documentación de IBM). Para obtener más información sobre cómo crear o editar trabajos de JCL en z/OS, consulte What is ISPF? (¿Qué es el ISPF?) y The ISPF editor (El editor ISPF) (documentación de IBM).	

Tarea	Descripción	Habilidades requeridas
Ejecute el cliente SFTP de JCL.	1. En el editor ISPF, escriba SUB y, a continuación, pulse la tecla INTRO, una vez creada la tarea JCL. 2. Supervise la actividad de los trabajos por lotes de transferencia de archivos del mainframe en SDSF. **Note** Para obtener más información sobre cómo comprobar la actividad de los trabajos por lotes, consulte la z/OS SDSF User's Guide (documentación de IBM).	Mainframe, JCL, ISPF

Tarea	Descripción	Habilidades requeridas
Valide la transferencia de archivos.	1. Inicie sesión en la consola de administración de AWS, abra la consola de Amazon S3 y, a continuación, seleccione Buckets en el panel de navegación. 2. Seleccione el bucket que está asociado a su Transfer Family. 3. En la sección Objects de la pestaña Objects, busque el archivo que ha transferido desde el mainframe.	AWS general
Automatice el cliente SFTP de JCL.	Utilice el programador de tareas para activar automáticamente el cliente SFTP de JCL. **Note** Puede utilizar programadores de trabajos de mainframe, como BMC Control-M o CA Workload Automation, para automatizar los trabajos por lotes para la transferencia de archivos en función del tiempo y otras dependencias de los trabajos por lotes.	Programador de trabajos

Recursos relacionados

- How AWS Transfer Family works (Cómo funciona AWS Transfer Family)

Optimice el rendimiento de su aplicación modernizada AWS Blu Age

Vishal Jaswani, Manish Roy y Himanshu Sah, Amazon Web Services

Resumen

Las aplicaciones de mainframe que se modernizan con AWS Blu Age requieren pruebas de equivalencia funcional y de rendimiento antes de implementarlas en producción. En las pruebas de rendimiento, las aplicaciones modernizadas pueden funcionar más lentamente que los sistemas heredados, especialmente en trabajos por lotes complejos. Esta disparidad se debe a que las aplicaciones de mainframe son monolíticas, mientras que las aplicaciones modernas utilizan arquitecturas de varios niveles. Este patrón presenta técnicas de optimización para abordar estas brechas de rendimiento en las aplicaciones que se modernizan mediante la refactorización automatizada con Blu Age. AWS

El patrón utiliza el marco de modernización de AWS Blu Age con capacidades nativas de Java y ajuste de bases de datos para identificar y resolver los cuellos de botella en el rendimiento. El patrón describe cómo puede utilizar la creación de perfiles y la supervisión para identificar los problemas de rendimiento con métricas como los tiempos de ejecución de SQL, el uso de la memoria y los patrones. I/O A continuación, se explica cómo aplicar optimizaciones específicas, como la reestructuración de las consultas de la base de datos, el almacenamiento en caché y el perfeccionamiento de la lógica empresarial.

Las mejoras en los tiempos de procesamiento por lotes y en el uso de los recursos del sistema lo ayudan a igualar los niveles de rendimiento del mainframe en los sistemas modernizados. Este enfoque mantiene la equivalencia funcional durante la transición a arquitecturas modernas basadas en la nube.

Para utilizar este patrón, configure el sistema e identifique hotspots de rendimiento siguiendo las instrucciones de la sección Epics y aplique las técnicas de optimización que se describen en detalle en la sección Arquitectura.

Requisitos previos y limitaciones

Requisitos previos

- Una aplicación modernizada de AWS Blu Age
- ¿Una licencia JProfiler

- Privilegios administrativos para instalar herramientas de creación de perfiles y clientes de bases de datos
- AWS Certificación Blu Age Level 3
- Comprensión de nivel intermedio del marco AWS Blu Age, la estructura del código generado y la programación en Java

Limitaciones

Las siguientes funciones y características de optimización quedan fuera del alcance de este patrón:

- Optimización de la latencia de la red entre los niveles de aplicación
- Optimizaciones a nivel de infraestructura mediante tipos de instancias de Amazon Elastic Compute Cloud (Amazon EC2) y optimización del almacenamiento
- Pruebas simultáneas de carga de usuarios y pruebas de estrés

Versiones de producto

- JProfiler versión 13.0 o posterior (recomendamos la versión más reciente)
- Versión 8.14 o posterior de pgAdmin

Arquitectura

Este patrón configura un entorno de creación de perfiles para una aplicación de AWS Blu Age mediante herramientas como JProfiler pgAdmin. Es compatible con la optimización mediante el SQLExecution generador DAOManager y el generador APIs proporcionado por AWS Blu Age.

El resto de esta sección proporciona información detallada y ejemplos para identificar los hotspots de rendimiento y las estrategias de optimización para sus aplicaciones modernizadas. Los pasos de la sección Epics se refieren a esta información para brindar más pautas.

Identificación de los hotspots de rendimiento en las aplicaciones de mainframe modernizadas

En las aplicaciones de mainframe modernizadas, los hotspots de rendimiento son áreas específicas del código que provocan ralentizaciones o ineficiencias significativas. Estos hotspots suelen deberse a las diferencias de arquitectura entre el mainframe y las aplicaciones modernizadas. Para identificar estos obstáculos en el rendimiento y optimizar el rendimiento de su aplicación modernizada, puede utilizar tres técnicas: el registro de SQL, un `EXPLAIN` plan de consultas y el análisis. JProfiler

Técnica de identificación de hotspots: registro de SQL

Las aplicaciones Java modernas, incluidas las que se han modernizado con AWS Blu Age, tienen funciones integradas para registrar consultas SQL. Puede habilitar registradores específicos en los proyectos de AWS Blu Age para rastrear y analizar las sentencias SQL ejecutadas por su aplicación. Esta técnica es particularmente útil para identificar patrones ineficientes de acceso a las bases de datos, como el exceso de consultas individuales o las llamadas a las bases de datos mal estructuradas, que podrían optimizarse mediante el procesamiento por lotes o el refinamiento de las consultas.

Para implementar el registro SQL en su aplicación modernizada de AWS Blu Age, establezca el nivel de registro en las sentencias SQL del `application.properties` archivo a fin `DEBUG` de capturar los detalles de la ejecución de las consultas:

```
level.org.springframework.beans.factory.support.DefaultListableBeanFactory : WARN
level.com.netfective.bluage.gapwalk.runtime.sort.internal: WARN
level.org.springframework.jdbc.core.StatementCreatorUtils: DEBUG
level.com.netfective.bluage.gapwalk.rt.blu4iv.dao: DEBUG
level.com.fiserv.signature: DEBUG
level.com.netfective.bluage.gapwalk.database.support.central: DEBUG
level.com.netfective.bluage.gapwalk.rt.db.configuration.DatabaseConfiguration: DEBUG
level.com.netfective.bluage.gapwalk.rt.db.DatabaseInteractionLoggerUtils: DEBUG
level.com.netfective.bluage.gapwalk.database.support.AbstractDatabaseSupport: DEBUG
level.com.netfective.bluage.gapwalk.rt: DEBUG
```

Supervise las consultas de alta frecuencia y de bajo rendimiento utilizando los datos registrados para identificar los objetivos de optimización. Céntrese en las consultas dentro de los procesos por lotes, ya que suelen tener el mayor impacto en el rendimiento.

Técnica de identificación de hotspots: plan EXPLAIN de las consultas

Este método utiliza las capacidades de planificación de consultas de los sistemas de administración de bases de datos relacionales. Puede utilizar comandos como `EXPLAIN` en PostgreSQL o MySQL o `EXPLAIN PLAN` en Oracle para examinar cómo la base de datos pretender ejecutar una consulta determinada. El resultado de estos comandos proporciona información valiosa sobre la estrategia de ejecución de la consulta; por ejemplo, si se utilizarán índices o si se realizarán exámenes de tablas completas. Esta información es fundamental para optimizar el rendimiento de las consultas, especialmente en los casos en que una indexación adecuada puede reducir considerablemente el tiempo de ejecución.

Extraiga las consultas SQL más repetitivas de los registros de la aplicación y analice la ruta de ejecución de las consultas con un rendimiento lento mediante el comando `EXPLAIN` específico de la base de datos. A continuación, se muestra un ejemplo de base de datos de PostgreSQL.

Consulta:

```
SELECT * FROM tenk1 WHERE unique1 < 100;
```

Comando de `EXPLAIN`:

```
EXPLAIN SELECT * FROM tenk1 where unique1 < 100;
```

Salida:

```
Bitmap Heap Scan on tenk1 (cost=5.06..224.98 rows=100 width=244)
Recheck Cond: (unique1 < 100)
-> Bitmap Index Scan on tenk1_unique1 (cost=0.00..5.04 rows=100 width=0)
Index Cond: (unique1 < 100)
```

Puede interpretar la salida de `EXPLAIN` de la siguiente forma:

- Lea el plan `EXPLAIN` desde las operaciones más internas hasta las más externas (de abajo hacia arriba).
- Busque los términos clave. Por ejemplo, `Seq Scan` indica un examen completo de la tabla y `Index Scan` muestra el uso del índice.
- Compruebe los valores de costo: el primer número es el costo inicial y el segundo es el costo total.
- Consulte el valor `rows` del número estimado de filas de salida.

En este ejemplo, el motor de consultas utiliza un examen del índice para buscar las filas coincidentes y, a continuación, prepara solo esas filas (`Bitmap Heap Scan`). Este método es más eficiente que examinar toda la tabla, a pesar del mayor costo del acceso a las filas individuales.

Las operaciones de examen de las tablas incluidas en la salida de un plan `EXPLAIN` indican que falta un índice. La optimización requiere la creación de un índice adecuado.

Técnica de identificación de puntos calientes: análisis JProfiler

JProfiler es una completa herramienta de creación de perfiles de Java que le ayuda a resolver los cuellos de botella en el rendimiento al identificar las llamadas lentas a las bases de datos y las

llamadas que requieren un uso intensivo de la CPU. Esta herramienta es particularmente eficaz para identificar las consultas SQL lentas y el uso ineficiente de la memoria.

Ejemplo de análisis para la consulta:

```
select evt.
 com.netfective.bluage.gapwalk.rt.blu4iv.dao.Blu4ivTableManager.queryNonTrasactional
```

La vista JProfiler Hot Spots proporciona la siguiente información:

- Columna Tiempo
  - Muestra la duración total de la ejecución (por ejemplo, 329 segundos)
  - Muestra el porcentaje del tiempo total de la aplicación (por ejemplo, 58,7 %)
  - Ayuda a identificar las operaciones que más tiempo consumen
- Columna Tiempo medio
  - Muestra la duración de cada ejecución (por ejemplo, 2692 microsegundos)
  - Indica el rendimiento de cada operación
  - Ayuda a detectar operaciones lentas
- Columna Eventos
  - Muestra el recuento de ejecuciones (por ejemplo, 122 387 veces)
  - Indica la frecuencia de la operación
  - Ayuda a identificar los métodos a los que se llama con frecuencia

Para ver los resultados del ejemplo:

- Frecuencia alta: 122 387 ejecuciones indican un potencial de optimización
- Problema de rendimiento: 2692 microsegundos durante un tiempo medio sugieren poca eficiencia
- Impacto crítico: el 58,7 % del tiempo total indica un cuello de botella importante

JProfiler puede analizar el comportamiento de la aplicación en tiempo de ejecución para revelar puntos críticos que podrían no ser evidentes mediante el análisis de código estático o el registro de SQL. Estas métricas lo ayudan a identificar las operaciones que necesitan optimizarse y a determinar la estrategia de optimización que sería más eficaz. Para obtener más información sobre JProfiler las funciones, consulte la JProfiler documentación.

Si utiliza estas tres técnicas (registro de SQL, `EXPLAIN` plan de consultas y JProfiler) en combinación, puede obtener una visión holística de las características de rendimiento de la aplicación. Al identificar y abordar los hotspots de rendimiento más críticos, puede cerrar la brecha de rendimiento entre la aplicación de mainframe original y el sistema modernizado basado en la nube.

Tras identificar los hotspots de rendimiento de la aplicación, puede aplicar estrategias de optimización, que se explican en la siguiente sección.

Estrategias de optimización para la modernización del mainframe

En esta sección se describen las estrategias clave para optimizar las aplicaciones que se han modernizado a partir de sistemas de mainframe. Se centra en tres estrategias: utilizar las existentes APIs, implementar un almacenamiento en caché eficaz y optimizar la lógica empresarial.

Estrategia de optimización: utilizar la existente APIs

AWS Blu Age proporciona varias interfaces DAO potentes APIs que puede utilizar para optimizar el rendimiento. Dos interfaces principales, DAOManager y SQLExecution Builder, ofrecen capacidades para mejorar el rendimiento de las aplicaciones.

DAOManager

DAOManager sirve como interfaz principal para las operaciones de bases de datos en aplicaciones modernizadas. Ofrece varios métodos para mejorar las operaciones de las bases de datos y mejorar el rendimiento de las aplicaciones, especialmente para las operaciones sencillas de creación, lectura, actualización y eliminación (CRUD, por sus siglas en inglés) y procesamiento por lotes.

- Uso SetMaxResults. En la DAOManager API, puede usar el SetMaxResultsmétodo para especificar el número máximo de registros que se van a recuperar en una sola operación de base de datos. De forma predeterminada, DAOManager recupera solo 10 registros a la vez, lo que puede provocar varias llamadas a la base de datos al procesar conjuntos de datos de gran tamaño. Utilice esta optimización cuando la aplicación tenga que procesar una gran cantidad de registros y actualmente esté realizando varias llamadas a bases de datos para recuperarlos. Esto resulta particularmente útil en situaciones de procesamiento por lotes en las que se realiza una iteración a través de un conjunto de datos de gran tamaño. En el siguiente ejemplo, el código de la izquierda (antes de la optimización) usa el valor de recuperación de datos predeterminado de 10 registros. El código de la derecha (después de la optimización) se configura setMaxResultspara recuperar 100 000 registros a la vez.

> **Note**
>
> Elija lotes de mayor tamaño con cuidado y compruebe el tamaño del objeto, ya que esta optimización aumenta el consumo de memoria.

- Sustituir SetOnGreatorOrEqual por SetOnEqual. Esta optimización implica cambiar el método que se utiliza para establecer la condición de recuperación de registros. El SetOnGreatorOrEqualmétodo recupera los registros que son mayores o iguales a un valor especificado, mientras que solo SetOnEqualrecupera los registros que coinciden exactamente con el valor especificado.

  SetOnEqualUtilícelo como se ilustra en el siguiente ejemplo de código, cuando sepa que necesita coincidencias exactas y esté utilizando actualmente el SetOnGreatorOrEqualmétodo seguido de readNextEqual(). Esta optimización reduce la recuperación innecesaria de datos.

- Utilice operaciones de escritura y actualización por lotes. Puede utilizar las operaciones por lotes para agrupar varias operaciones de escritura o actualización en una sola transacción de la base de datos. Esto reduce el número de llamadas a la base de datos y puede mejorar considerablemente el rendimiento de las operaciones que implican varios registros.

  En el siguiente ejemplo, el código de la izquierda realiza operaciones de escritura en bucle, lo que ralentiza el rendimiento de la aplicación. Puede optimizar este código mediante una operación de escritura por lotes: durante cada iteración del bucle `WHILE`, se agregan registros a un lote hasta que el tamaño del lote alcance un tamaño predeterminado de 100. A continuación, puede vaciar el lote cuando alcance el tamaño de lote predeterminado y, a continuación, vaciar los registros restantes en la base de datos. Esto resulta especialmente útil en las situaciones en las que se procesan conjuntos de datos de gran tamaño que requieren actualizaciones.

- Agregue índices. Agregar índices es una optimización a nivel de base de datos que puede mejorar considerablemente el rendimiento de las consultas. Los índices permiten que la base de datos localice rápidamente las filas con un valor de columna específico sin tener que examinar toda la tabla. Utilice la indexación en las columnas que se utilizan con frecuencia en las cláusulas `WHERE`, las condiciones `JOIN` o las instrucciones `ORDER BY`. Esto es particularmente importante para las tablas de gran tamaño o cuando la recuperación rápida de datos es fundamental.

SQLExecutionConstructor

SQLExecutionBuilder es una API flexible que puede utilizar para controlar las consultas SQL que se ejecutarán, recuperar solo determinadas columnas mediante `SELECT` el uso de nombres de tablas dinámicas y utilizar nombres de tablas dinámicas. `INSERT` En el siguiente ejemplo, SQLExecutor Builder usa una consulta personalizada que usted defina.

Elegir entre DAOManager y SQLExecution Builder

La elección entre estas opciones APIs depende de su caso de uso específico:

- Úselo DAOManager cuando desee que AWS Blu Age Runtime genere las consultas SQL en lugar de escribirlas usted mismo.
- Elija SQLExecution Builder cuando necesite escribir consultas SQL para aprovechar las funciones específicas de la base de datos o escribir consultas SQL óptimas.

Estrategia de optimización: almacenamiento en caché

En las aplicaciones modernizadas, la implementación de estrategias de almacenamiento en caché eficaces puede reducir significativamente las llamadas a las bases de datos y mejorar los tiempos de respuesta. Esto ayuda a cerrar la brecha de rendimiento entre los entornos de mainframe y en la nube.

En las aplicaciones de AWS Blu Age, las implementaciones de almacenamiento en caché sencillas utilizan estructuras de datos internas, como mapas hash o listas de matrices, por lo que no es necesario configurar una solución de almacenamiento en caché externa que requiera una reestructuración de costes y código. Este enfoque es particularmente eficaz para los datos a los que se accede con frecuencia, pero que no cambian a menudo. Al implementar el almacenamiento en caché, tenga en cuenta las limitaciones de memoria y los patrones de actualización para mantener el rendimiento y las ventajas de rendimiento reales de los datos almacenados en caché.

La clave para un almacenamiento en caché exitoso es identificar los datos correctos que se van a almacenar en caché. En el siguiente ejemplo, el código de la izquierda siempre lee los datos de la tabla, mientras que el código de la derecha lee los datos de la tabla cuando el mapa hash local no tiene un valor para una clave determinada. `cacheMap` es un objeto de mapa hash que se crea en el contexto del programa y se borra con el método de limpieza del contexto del programa.

Almacenamiento en caché con: DAOManager

Almacenamiento en caché con Builder: SQLExecution

Estrategia de optimización: optimización de la lógica empresarial

La optimización de la lógica empresarial se centra en reestructurar el código generado automáticamente por AWS Blu Age para alinearlo mejor con las capacidades de la arquitectura moderna. Esto se hace necesario cuando el código generado mantiene la misma estructura lógica que el código de mainframe heredado, lo que puede no ser óptimo para los sistemas modernos. El objetivo es mejorar el rendimiento y, al mismo tiempo, mantener la equivalencia funcional de la aplicación original.

Este enfoque de optimización no se centra solo en los simples ajustes de la API y las estrategias de almacenamiento en caché. Implica cambios en la forma en que la aplicación procesa los datos e interactúa con la base de datos. Algunas de las optimizaciones más comunes son evitar operaciones de lectura innecesarias para las actualizaciones sencillas, eliminar las llamadas redundantes a las bases de datos y reestructurar los patrones de acceso a los datos para adaptarlos mejor a la arquitectura moderna de la aplicación. A continuación se muestran algunos ejemplos:

- Actualizar los datos directamente en la base de datos.Reestructure su lógica empresarial mediante actualizaciones directas de SQL en lugar de DAOManager realizar múltiples operaciones con bucles. Por ejemplo, el siguiente código (lado izquierdo) realiza varias llamadas a la base de datos y utiliza memoria excesiva. En concreto, utiliza varias operaciones de lectura y escritura en bases de datos dentro de bucles, actualizaciones específicas en lugar de hacer procesamientos por lotes y crear objetos innecesarios para cada iteración.

  El siguiente código optimizado (en la derecha) utiliza una sola operación de actualización de Direct SQL. En concreto, utiliza una sola llamada a la base de datos en lugar de realizar varias llamadas y no requiere bucles, ya que todas las actualizaciones se gestionan en una sola instrucción. Esta optimización proporciona un mejor rendimiento y una mejor utilización de los recursos y reduce la complejidad. Evita la inyección de código SQL, proporciona un mejor almacenamiento en caché del plan de consultas y ayuda a mejorar la seguridad.

> **Note**
>
> Utilice siempre consultas parametrizadas para evitar la inyección de código SQL y garantizar una administración adecuada de las transacciones.

- Reducción de las llamadas redundantes a las bases de datos. Las llamadas redundantes a las bases de datos pueden afectar significativamente al rendimiento de las aplicaciones, especialmente cuando se producen dentro de bucles. Una técnica de optimización sencilla pero eficaz consiste en evitar repetir la misma consulta a la base de datos varias veces. En la siguiente comparación de código se demuestra cómo al mover la llamada a la base de datos `retrieve()` fuera del bucle se evita la ejecución redundante de consultas idénticas, lo que mejora la eficiencia.

- Reducción de las llamadas a la base de datos mediante la cláusula SQL `JOIN`. Implemente SQLExecution Builder para minimizar las llamadas a la base de datos. SQLExecutionBuilder proporciona un mayor control sobre la generación de SQL y es particularmente útil para consultas complejas que DAOManager no se pueden gestionar de manera eficiente. Por ejemplo, el código siguiente utiliza varias DAOManager llamadas:

```
List<Employee> employees = daoManager.readAll();
for(Employee emp : employees) {
    Department dept = deptManager.readById(emp.getDeptId());  // Additional call for
 each employee
    Project proj = projManager.readById(emp.getProjId());     // Another call for
 each employee
    processEmployeeData(emp, dept, proj);
}
```

  El código optimizado usa una sola llamada a la base de datos en SQLExecution Builder:

```
SQLExecutionBuilder builder = new SQLExecutionBuilder();
builder.append("SELECT e.*, d.name as dept_name, p.name as proj_name");
builder.append("FROM employee e");
builder.append("JOIN department d ON e.dept_id = d.id");
builder.append("JOIN project p ON e.proj_id = p.id");
builder.append("WHERE e.status = ?", "ACTIVE");

List<Map<String, Object>> results = builder.execute();  // Single database call
for(Map<String, Object> result : results) {
    processComplexData(result);
}
```

Uso conjunto de estrategias de optimización

Estas tres estrategias funcionan de forma sinérgica: APIs proporcionan las herramientas para un acceso eficiente a los datos, el almacenamiento en caché reduce la necesidad de recuperar datos de forma repetida y la optimización de la lógica empresarial garantiza que APIs se utilicen de la manera más eficaz posible. La supervisión y el ajuste periódicos de estas optimizaciones garantizan una mejora continua del rendimiento y, al mismo tiempo, mantienen la fiabilidad y la funcionalidad de la aplicación modernizada. La clave del éxito reside en comprender cuándo y cómo aplicar cada estrategia en función de las características y los objetivos de rendimiento de la aplicación.

Tools (Herramientas)

- JProfileres una herramienta de creación de perfiles de Java diseñada para desarrolladores e ingenieros de rendimiento. Analiza las aplicaciones Java y ayuda a identificar los cuellos de botella en el rendimiento, las pérdidas de memoria y los problemas de subprocesos. JProfiler ofrece perfiles de CPU, memoria y subprocesos, así como supervisión de bases de datos y máquinas virtuales Java (JVM) para proporcionar información sobre el comportamiento de las aplicaciones.

  > **Note**
  >
  > Como alternativa JProfiler, puede utilizar Java VisualVM. Se trata de una herramienta gratuita de código abierto de creación de perfiles de rendimiento y supervisión para aplicaciones de Java que permite supervisar en tiempo real el uso de la CPU, el consumo de memoria, la administración de subprocesos y las estadísticas de recopilación de elementos no utilizados. Dado que Java VisualVM es una herramienta JDK integrada, resulta más JProfiler rentable que para las necesidades básicas de creación de perfiles.

- pgAdmin es una plataforma de administración y desarrollo de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos. Puede usar pgAdmin para realizar una amplia gama de tareas, desde escribir consultas SQL sencillas hasta desarrollar bases de datos complejas. Algunas de sus características son un editor de código SQL que resalta la sintaxis, un editor de código en el servidor, un agente de programación para SQL, un intérprete de comandos y tareas por lotes, y compatibilidad con todas las características de PostgreSQL tanto para usuarios sin experiencia como con experiencia de PostgreSQL.

Prácticas recomendadas

Identificación de hotspots de rendimiento:

- Documente las métricas de rendimiento de referencia antes de iniciar las optimizaciones.
- Establezca objetivos claros de mejora del rendimiento en función de los requisitos empresariales.
- Al realizar evaluaciones comparativas, desactive la creación de registros detallados, ya que esto puede afectar al rendimiento.
- Configure un conjunto de pruebas de rendimiento y ejecútelo periódicamente.
- Utilice la versión más reciente de pgAdmin. (Las versiones más antiguas no admiten el plan `EXPLAIN` de consultas).
- Para realizar una evaluación comparativa, desconéctese una vez que se hayan JProfiler completado las optimizaciones, ya que esto aumenta la latencia.
- Para realizar evaluaciones comparativas, asegúrese de ejecutar el servidor en modo de inicio en lugar de en modo de depuración, ya que el modo de depuración aumenta la latencia.

Estrategias de optimización:

- Configure SetMaxResultslos valores en el `application.yaml` archivo para especificar lotes del tamaño correcto de acuerdo con las especificaciones de su sistema.
- Configure SetMaxResultslos valores en función del volumen de datos y las restricciones de memoria.
- Cambie SetOnGreatorOrEquala SetOnEqualsolo cuando se realicen llamadas posteriores`.readNextEqual()`.
- En las operaciones de escritura o actualización por lotes, gestione el último lote por separado, ya que podría ser más pequeño que el tamaño del lote configurado y la operación de escritura o actualización podría pasarlo por alto.

Almacenamiento en caché:

- Los campos que se introducen para el almacenamiento en caché en `processImpl`, que cambian con cada ejecución, siempre deben definirse en el contexto de ese `processImpl`. Los campos también deben borrarse mediante el método `doReset()` o `cleanUp()`.
- Cuando implemente el almacenamiento en caché en memoria, ajuste el tamaño de la caché. Las cachés muy grandes que se almacenan en la memoria pueden ocupar todos los recursos, lo que podría afectar al rendimiento general de la aplicación.

SQLExecutionConstructor:

- Para las consultas que planea usar en SQLExecution Builder, utilice nombres clave como`PROGRAMNAME_STATEMENTNUMBER`.
- Cuando utilice SQLExecution Builder, compruebe siempre el `Sqlcod` campo. Este campo contiene un valor que especifica si la consulta se ejecutó correctamente o si encontró algún error.
- Utilice consultas parametrizadas para evitar la inyección de código SQL.

Optimización de la lógica empresarial:

- Mantenga la equivalencia funcional al reestructurar el código y ejecute pruebas de regresión y comparaciones de bases de datos para el subconjunto de programas correspondiente.
- Mantenga instantáneas de la creación de perfiles para poder compararlas.

Epics

Instalación JProfiler y pgAdmin

Tarea	Descripción	Habilidades requeridas
Instalar y configurar. JProfiler	1. En la página de JProfiler descargas, descárguelo JProfiler para su sistema operativo (Windows, macOS o Linux). 2. Complete el proceso de instalación siguiendo las instrucciones de la JProfiler documentación. 3. Realice la configuración inicial: a. Inicie la JProfiler aplicación. b. Active la clave de la licencia. c. Ajuste la configuración predeterminada de JVM.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	4. Verificar la instalación: a. Lanza JProfiler. b. Realice una sesión de prueba de creación de perfiles. Para obtener instrucciones, consulte Conexión a servicios locales en la sección Creación de perfiles de una JVM de la documentación. JProfiler	

Tarea	Descripción	Habilidades requeridas
Instale y configure pgAdmin.	En este paso, debe instalar y configurar un cliente de base de datos para que realice consultas en la base de datos. Este patrón utiliza una base de datos PostgreSQL y pgAdmin como cliente de base de datos. Si utiliza otro motor de base de datos, siga la documentación del cliente de base de datos correspon diente. 1. Descargue e instale pgAdmin para su sistema operativo desde la página de descargas de pgAdmin. Establezca la contraseña maestra durante la instalaci ón. 2. Conéctese al servidor de la base de datos. Para obtener instrucciones, consulte la documentación de pgAdmin. 3. Compruebe la instalación mediante la herramienta Query Tool de pgAdmin para ejecutar consultas SQL básicas.	Desarrollador de aplicaciones

Identificación de hotspots

Tarea	Descripción	Habilidades requeridas
Habilite el registro de consultas SQL en su aplicación AWS Blu Age.	Habilite los registradores para el registro de consultas SQL en el `application.properties` archivo de su aplicación AWS Blu Age, tal y como se explica en la sección de Arquitectura.	Desarrollador de aplicaciones
Genere y analice los planes `EXPLAIN` de consultas para identificar los hotspots de rendimiento de las bases de datos.	Para obtener información detallada, consulte la sección Arquitectura.	Desarrollador de aplicaciones
Cree una JProfiler instantánea para analizar un caso de prueba de rendimiento lento.	1. Lanzamiento: JProfiler a. Abre la JProfiler aplicación. b. En Start Center, seleccione la pestaña Quick Attach. c. Seleccione el proceso de Tomcat en la lista. d. Elija Iniciar. 2. Ajuste la configuración de creación de perfiles: a. Seleccione Recommended Sampling Option. b. En la pantalla de configuración, mantenga las opciones predeterminadas y seleccione OK.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	c. Espere a que aparezca el estado Connected en la barra de estado. 3. Registre los datos de rendimiento: a. En la barra de herramien tas, seleccione Start Recording. b. Ejecute su caso de prueba y espere a que se complete. c. Seleccione Stop Recording. 4. Guarde y visualice la instantánea: a. Seleccione Save Snapshot. b. Elija la ubicación en la que desee guardar la instantánea y, a continuación, seleccione Save.	

Tarea	Descripción	Habilidades requeridas
Analice la JProfiler instantán ea para identificar los cuellos de botella en el rendimiento.	Siga estos pasos para analizar la instantánea. JProfiler 1. Abra la instantánea: a. Seleccione Archivo, Open Snapshot. b. Navegue hasta la ubicación de la instantán ea guardada. c. Seleccione Open a new window para iniciar el análisis. 2. Analice las operaciones de la base de datos: a. Vaya a la sección JDBC/ Database y seleccione la pestaña JPA/Hibernate. b. Revise las consultas por hora (que es la opción de ordenación predeterm inada). c. Elija la consulta de más arriba para optimizarla. 3. Revise el uso de la CPU: a. En la sección de CPU, seleccione la vista Hot Spots. b. Identifique el código con mayor porcentaje de tiempo para optimizarlo. c. Fíjese en cualquier patrón recurrente.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	4. Tras identificar los hotspots, establezca una línea de base y, a continuación, implemente las estrategias de optimización adecuadas , tal y como se explica en los siguientes resúmenes . Céntrese en estas optimizaciones: • Para consultas lentas, usa SQLExecution Builder o DAOManager la optimización. • En caso de que acceda a los datos con frecuencia, implemente mecanismo s de almacenamiento en caché. • En caso de tener una lógica empresarial compleja, simplifique la lógica, evite realizar demasiadas llamadas a la base de datos y determine si se puede simplificar el código ejecutando una consulta sencilla. Por ejemplo, si el código inserta datos de la tabla A en la tabla B, vuelva a escribir este código para ejecutar un comando SQL similar al siguiente:	

Tarea	Descripción	Habilidades requeridas
	`INSERT INTO TABLE A SELECT * FROM TABLE B` 5. Siga analizando y optimizando el código en orden de impacto (de mayor a menor) hasta que la aplicación cumpla con los requisitos de rendimiento. Para obtener más información sobre su uso JProfiler, consulte la sección Arquitectura y la JProfiler documentación.	

Establecimiento de una línea de base

Tarea	Descripción	Habilidades requeridas
Establezca una línea de base de rendimiento antes de implementar las optimizaciones.	1. Como medida inicial del rendimiento, ejecute el caso de prueba sin ninguna optimización. Cree una JProfiler instantánea del estado actual y documente las siguientes métricas: • Tiempo total de ejecución • Número de llamadas a la base de datos • Porcentaje de utilización de la CPU	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	• Patrón de uso de la memoria 2. Cree una línea de base de documento: a. Guarde todas las métricas con una marca de tiempo y condiciones de prueba. b. Tenga en cuenta cualquier factor externo que pueda afectar al rendimiento. c. Guarde la JProfiler instantánea para compararla después de la optimización. 3. Planifique los cambios de optimización que se describen en el siguiente resumen: a. Revise las métricas de la línea de base. b. Identifique la operación que desea optimizar. c. Cree una copia de seguridad del código actual. d. Documente las mejoras esperadas. 4. Mida cada cambio antes de la implementación:	

Tarea	Descripción	Habilidades requeridas
	a. Ejecute un caso de prueba utilizando las condiciones de la línea de base. b. Registre el tiempo de ejecución. c. Documente el comportamiento actual.	

Aplicación de estrategias de optimización

Tarea	Descripción	Habilidades requeridas
Optimice las llamadas de lectura.	Optimice la recuperac ión de datos mediante el DAOManager SetMaxRes ultsmétodo. Para obtener más información sobre este enfoque, consulte la sección Arquitectura.	Desarrollador de aplicaciones, DAOManager
Refactorice la lógica empresarial para evitar varias llamadas a la base de datos.	Reduzca las llamadas a la base de datos mediante una cláusula `JOIN` en SQL. Para obtener detalles y ejemplos, consulte Optimización de la lógica empresarial en la sección Arquitectura.	Desarrollador de aplicaciones, SQLExecution constructor
Refactorice el código para usar el almacenamiento en caché para reducir la latencia de las llamadas de lectura.	Para obtener información sobre esta técnica, consulte Almacenamiento en caché en la sección Arquitectura.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Reescriba el código ineficiente que utiliza varias DAOManager operaciones para realizar operaciones de actualización sencillas.	Para obtener más información sobre cómo actualizar los datos directamente en la base de datos, consulte Optimización de la lógica empresarial en la sección Arquitectura.	Desarrollador de aplicaciones

Estrategias de optimización de pruebas

Tarea	Descripción	Habilidades requeridas
Valide cada cambio de optimización de forma iterativa y, al mismo tiempo, mantenga la equivalencia funcional.	1. Después de implementar las optimizaciones: a. Ejecute los mismos casos de prueba a partir de la línea de base que estableció. b. Registre el nuevo tiempo de ejecución. c. Compruebe que los resultados coincidan con la salida de la línea de base. 2. Si la optimización se traduce en una mejora, documente las ganancias reales y, a continuación, pase a la siguiente optimización. Si encuentra problemas, revierta los cambios,	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	revise su enfoque y pruebe soluciones alternativas. 3. Realice un seguimiento del progreso de cada cambio: a. Compare las métricas nuevas con las métricas de la línea de base. b. Calcule el porcentaje de mejora. c. Mantenga un total acumulado de ganancias . **Note** El uso de métricas de línea de base como referencia garantiza una medición precisa del impacto de cada optimización y, al mismo tiempo, mantiene la fiabilidad del sistema.	

Resolución de problemas

Problema	Solución
Al ejecutar la aplicación moderna, verá una excepción con el error `Query_ID not found`.	Para resolver este problema, siga estos pasos: 1. Compruebe si existe un archivo con el nombre `query.sql` en la carpeta `sql`

Problema	Solución
	del directorio de trabajo del servidor de la aplicación. 2. Compruebe que el nombre del archivo `.sql` coincida con el nombre del programa. Por ejemplo, en el caso de un programa denominado `ABC`, el nombre del archivo debe ser `ABC.sql`.
Ha agregado índices, pero no ve ninguna mejora de rendimiento.	Siga estos pasos para asegurarse de que el motor de consultas utilice el índice: 1. Si utiliza PostgreSQL, ejecute el comando `EXPLAIN <sql query>`. 2. Compruebe el resultado del comando para `Seq Scan` o `Index Scan`. `Seq Scan` significa que el conjunto de índices no está disponible en las columnas que utiliza la cláusula `where` de la consulta SQL. 3. Cree un índice en el conjunto correcto de columnas e intente formar consultas que utilicen el índice creado.
Te encuentras con una excepción out-of-me mory.	Compruebe que el código libere la memoria almacenada en la estructura de datos.
Las operaciones de escritura por lotes hacen que falten registros en la tabla	Revise el código para asegurarse de que se realice una operación de escritura adicional cuando el recuento de lotes no es cero.

Problema	Solución
El registro de SQL no aparece en los registros de la aplicación.	1. Compruebe la ubicación y la sintaxis del archivo de configuración de registro. 2. Asegúrese de que el nivel de registro esté establecido en `DEBUG` para los paquetes especificados. Por ejemplo: `level.com.netfective.bluage .gapwalk.rt.blu4iv.dao: DEBUG level.org.springframework.jdbc .core: DEBUG` 3. Compruebe los permisos del archivo de registro del servidor de la aplicación. 4. Reinicie el servidor de la aplicación después de realizar cambios en la configuración.

Recursos relacionados

- Refactorización automática de aplicaciones con AWS Blu Age (Guía AWS Mainframe Modernization del usuario)
- Documentación de pgAdmin
- JProfiler documentación

Proteja y optimice el acceso de los usuarios a una base de datos de federación DB2 en AWS mediante contextos de confianza

Sai Parthasaradhi, Amazon Web Services

Resumen

Muchas empresas están migrando sus cargas de trabajo de la unidad central antigua a Amazon Web Services (AWS). Esta migración incluye el cambio de IBM Db2 para z/OS bases de datos a Db2 para Linux, Unix y Windows (LUW) en Amazon Elastic Compute Cloud (Amazon). EC2 Durante una migración gradual de las instalaciones a AWS, es posible que los usuarios necesiten acceder a los datos de IBM Db2 z/OS y Db2 LUW en EC2 Amazon hasta que todas las aplicaciones y bases de datos se hayan migrado por completo a Db2 LUW. En estos escenarios de acceso remoto a los datos, la autenticación de los usuarios puede resultar difícil porque las diferentes plataformas utilizan diferentes mecanismos de autenticación.

Este patrón explica cómo configurar un servidor de federación en Db2 para LUW con Db2 como base de datos remota. z/OS El patrón utiliza un contexto confiable para propagar la identidad de un usuario de Db2 LUW a Db2 sin volver a autenticarse en la base de datos z/OS remota. Para obtener más información sobre los contextos de confianza, consulte la sección Información adicional.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una instancia de Db2 que se ejecuta en una instancia de Amazon EC2
- Un Db2 remoto para una z/OS base de datos que se ejecuta en las instalaciones
- La red local conectada a AWS a través de AWS Site-to-Site VPN o AWS Direct Connect

Arquitectura

Arquitectura de destino

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- La Site-to-SiteVPN de AWS le ayuda a transferir el tráfico entre las instancias que lanza en AWS y su propia red remota.

Otras herramientas

- db2cli es el comando de la interfaz de la línea de comandos (CLI) interactiva de Db2.

Epics

Habilite la federación en la base de datos Db2 LUW que se ejecuta en AWS

Tarea	Descripción	Habilidades requeridas
Habilite la federación en la base de datos DB2 LUW.	Para habilitar la federación en DB2 LUW, ejecute el siguiente comando. `update dbm cfg using federated YES`	Administrador de base de datos
Reinicie la base de datos.	Para reiniciar la base de datos, ejecute el comando siguiente: `db2stop force; db2start;`	Administrador de base de datos

Cataloga la base de datos remota

Tarea	Descripción	Habilidades requeridas
Cataloga el subsistema Db2 z/OS remoto.	Para catalogar la z/OS base de datos Db2 remota en Db2	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	LUW que se ejecuta en AWS, utilice el siguiente comando de ejemplo. `catalog TCPIP NODE tcpnode REMOTE mainframehost SERVER mainframeport`	
Catalogue la base de datos remota.	Para catalogar la base de datos remota, utilice el siguiente comando de ejemplo. `catalog db dbnam1 as ndbnam1 at node tcpnode`	Administrador de base de datos

Cree la definición de servidor remoto

Tarea	Descripción	Habilidades requeridas
Recopile las credenciales de usuario para la base de datos remota de Db2. z/OS	Antes de continuar con los siguientes pasos, recopile la siguiente información: • Nombre z/OS del subsistema de Db2: el nombre de Db2 z/OS catalogado en LUW del paso anterior (por ejemplo,) `ndbnam1` • Versión Db2: z/OS la versión del subsistema Db2 z/OS (por ejemplo,) 12 • ID de z/OS usuario de Db2: el usuario con el privilegi	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	o BIND, que se necesita para crear únicamente la definición de servidor (por ejemplo,) `dbuser1` • z/OS Contraseña de Db2: la contraseña de `dbuser1` (por ejemplo,) `dbpasswd` • Usuario z/OS proxy de Db2: el ID del usuario proxy, que se utilizará para establecer una conexión de confianza (por ejemplo,) `zproxy` • Contraseña del z/OS proxy de Db2: la contraseña del `zproxy` usuario (por ejemplo,) `zproxy`	
Cree la capa DRDA.	Ejecute el siguiente comando para crear una capa DRDA. `CREATE WRAPPER DRDA;`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree la definición del servidor.	Para crear la definición del servidor, ejecute el siguiente comando de ejemplo. `CREATE SERVER ndbserver TYPE DB2/ZOS VERSION 12 WRAPPER DRDA AUTHORIZATION "dbuser1" PASSWORD "dbpasswd " OPTIONS ( DBNAME 'ndbnam1',FED_PROX Y_USER 'ZPROXY' );` En esta definición, `FED_PROXY_USER` especifica el usuario proxy que se utilizará para establecer conexiones de confianza a la base de datos de Db2 z/OS . El ID de usuario y la contraseña de autorización solo son necesarios para crear el objeto de servidor remoto en la base de datos de Db2 LUW. No se utilizarán más adelante durante el tiempo de ejecución.	Administrador de base de datos

Creación de asignaciones de usuarios

Tarea	Descripción	Habilidades requeridas
Cree un asignación de usuarios para el usuario proxy.	Para crear un asignación de usuarios para el usuario proxy, ejecute el siguiente comando.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`CREATE USER MAPPING FOR ZPROXY SERVER ndbserver OPTIONS (REMOTE_AUTHID 'ZPROXY', REMOTE_PASSWORD 'zproxy');`	

Tarea	Descripción	Habilidades requeridas
Cree asignaciones de usuarios para cada usuario en Db2 LUW.	Cree asignaciones de usuarios para todos los usuarios de la base de datos de Db2 LUW en AWS que necesiten acceder a datos remotos a través del usuario proxy. Ejecute el siguiente comando para crear las asignaciones de usuario. `CREATE USER MAPPING FOR PERSON1 SERVER ndbserver OPTIONS (REMOTE_AUTHID 'USERZID', USE_TRUSTED_CONTEXT 'Y');` La declaración especifica que un usuario de Db2 LUW (PERSON1) puede establecer una conexión de confianza con la base de datos remota de Db2 z/OS (). `USE_TRUSTED_CONTEXT 'Y'` Una vez establecida la conexión a través del usuario proxy, el usuario puede acceder a los datos mediante el ID de z/OS usuario de Db2 (). `REMOTE_AUTHID 'USERZID'`	Administrador de base de datos

Cree el objeto de contexto de confianza

Tarea	Descripción	Habilidades requeridas
Cree el objeto de contexto de confianza.	Para crear el objeto de contexto de confianza en la z/OS base de datos remota de Db2, utilice el siguiente comando de ejemplo. `CREATE TRUSTED CONTEXT CTX_LUW_ZOS BASED UPON CONNECTIO N USING SYSTEM AUTHID ZPROXY ATTRIBUTES ( ADDRESS '10.10.10.10' ) NO DEFAULT ROLE ENABLE WITH USE FOR PUBLIC WITHOUT AUTHENTIC ATION;` En esta definición, `CTX_LUW_ZOS` es un nombre arbitrario para el objeto de contexto de confianza. El objeto contiene el ID del usuario proxy y la dirección IP del servidor desde el que debe originarse la conexión de confianza. En este ejemplo, el servidor de la base de datos Db2 LUW en AWS. También puede utilizar el nombre de dominio en lugar de la dirección IP. La cláusula `WITH USE FOR PUBLIC WITHOUT`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`AUTHENTICATION` indica que se permite cambiar el ID de usuario en una conexión de confianza para cada ID de usuario. No es necesario proporcionar una contraseña.	

Recursos relacionados

- Instalación de control de acceso a los recursos de IBM (RACF)
- Federación IBM Db2 LUW
- Contextos de confianza

Información adicional

Contextos de confianza de Db2

Un contexto de confianza es un objeto de base de datos de Db2 que define una relación de confianza entre un servidor federado y un servidor de base de datos remoto. Para definir una relación de confianza, el contexto de confianza especifica los atributos de confianza. Existen tres tipos de atributos de confianza:

- El ID de autorización del sistema que realiza la solicitud de conexión inicial a la base de datos
- La dirección IP o el nombre de dominio desde los que se realiza la conexión
- La configuración de cifrado para las comunicaciones de datos entre el servidor de la base de datos y el cliente de la base de datos

Se establece una conexión de confianza cuando todos los atributos de una solicitud de conexión coinciden con los atributos especificados en cualquier objeto de contexto de confianza definido en el servidor. Existen dos tipos diferentes de conexiones de confianza: implícitas y explícitas. Una vez establecida una conexión de confianza implícita, el usuario hereda un rol que no está disponible para él fuera del ámbito de esa definición de conexión de confianza. Una vez establecida una conexión de confianza explícita, los usuarios pueden conectarse a la misma conexión física, con o sin autenticación. Además, a los usuarios de Db2 se les pueden asignar roles que especifiquen

privilegios que solo se utilizarán dentro de la conexión de confianza. Este patrón utiliza una conexión de confianza explícita.

Contexto de confianza en este patrón

Una vez completado el patrón, PERSON1 en Db2, LUW accede a los datos remotos de Db2 z/OS mediante un contexto de confianza federado. La conexión para PERSON1 se establece a través de un usuario proxy si la conexión se origina en la dirección IP o el nombre de dominio que se especifica en la definición del contexto de confianza. Una vez establecida la conexión, el ID PERSON1 de z/OS usuario de Db2 correspondiente se cambia sin necesidad de volver a autenticarse, y el usuario puede acceder a los datos u objetos en función de los privilegios de Db2 configurados para ese usuario.

Ventajas de los contextos de confianza federados

- Este enfoque mantiene el principio del privilegio mínimo al eliminar el uso de un ID de usuario o de aplicación común, que requeriría un conjunto de todos los privilegios que requieren todos los usuarios.
- La identidad real del usuario que realiza la transacción tanto en la base de datos federada como en la remota siempre se conoce y se puede auditar.
- El rendimiento mejora porque la conexión física se reutiliza entre los usuarios sin necesidad de que el servidor federado vuelva a autenticarse.

Transfiera z/OS datos de Db2 a gran escala a Amazon S3 en archivos CSV

Bruno Sahinoglu, Abhijit Kshirsagar e Ivan Schuster, Amazon Web Services

Resumen

Un mainframe sigue siendo el sistema de registro de muchas empresas que conservan una enorme cantidad de datos, incluidas entidades de datos maestros con registros de las transacciones comerciales actuales e históricas. A menudo está aislado, y los sistemas distribuidos de la misma empresa no pueden acceder fácilmente a él. Con la aparición de la tecnología en la nube y la democratización de los macrodatos, las empresas tratan de usar la información oculta en los datos del mainframe para desarrollar nuevas capacidades empresariales.

Con ese objetivo, las empresas buscan abrir sus datos Db2 de mainframe a su entorno de nube de Amazon Web Services (AWS). Los motivos empresariales son varios, y los métodos de transferencia varían de un caso a otro. Es posible que prefiera conectar la aplicación directamente al mainframe, o que prefiera replicar los datos prácticamente en tiempo real. Si el caso de uso es alimentar un almacén de datos o un lago de datos, disponer de una up-to-date copia ya no es un problema y el procedimiento descrito en este patrón puede ser suficiente, especialmente si se quiere evitar los costes de licencia de productos de terceros. Otro caso de uso podría ser la transferencia de datos de un mainframe para un proyecto de migración. En un escenario de migración, es necesario contar con datos para realizar las pruebas de equivalencia funcional. El enfoque descrito en esta publicación es una forma rentable de transferir los datos de Db2 al entorno de nube de AWS.

Dado que Amazon Simple Storage Service (Amazon S3) es uno de los servicios de AWS más integrados, puede acceder a los datos desde allí y recopilar información directamente mediante otros servicios de AWS, como Amazon Athena, AWS Lambda Functions o Amazon. QuickSight También puede cargar los datos en Amazon Aurora o Amazon DynamoDB mediante AWS Glue o AWS Database Migration Service (AWS DMS). Con ese objetivo en mente, este patrón describe cómo descargar datos de Db2 en archivos CSV en formato ASCII en el mainframe y transferir los archivos a Amazon S3.

Para ello, se han desarrollado scripts de mainframe para ayudar a generar lenguajes de control de tareas (JCLs) para descargar y transferir tantas tablas de Db2 como necesite.

Requisitos previos y limitaciones

Requisitos previos

- Usuario del sistema z/OS operativo IBM con autorización para ejecutar scripts JCL y Restructured Extended Executor (REXX).
- Acceso a los servicios del sistema z/OS Unix (USS) para generar claves públicas y privadas de SSH (Secure Shell).
- Un bucket de S3 con permisos de escritura. Para obtener más información, consulte la sección Cree su primer bucket de S3 en la documentación de Amazon S3.
- Un servidor habilitado para el protocolo SSH File Transfer (SFTP) de AWS Transfer Family con Service Managed como proveedor de identidad y Amazon S3 como servicio de almacenamiento de AWS. Para obtener más información, consulte Crear un servidor habilitado para SFTP en la documentación de AWS Transfer Family.

Limitaciones

- Este enfoque no es adecuado para la sincronización de datos prácticamente en tiempo real o en tiempo real.
- Los datos solo se pueden mover de Db2 z/OS a Amazon S3, y no al revés.

Arquitectura

Pila de tecnología de origen

- Mainframe que ejecuta Db2 en z/OS

Pila de tecnología de destino

- AWS Transfer Family
- Amazon S3
- Amazon Athena
- Amazon QuickSight
- AWS Glue
- Amazon Relational Database Service (Amazon RDS)
- Amazon Aurora
- Amazon Redshift

Arquitectura de origen y destino

El siguiente diagrama muestra el proceso de generación, extracción y transferencia de z/OS datos de Db2 en formato CSV ASCII a un bucket de S3.

1. Se selecciona una lista de tablas para la migración de datos del catálogo de Db2.
2. La lista se usa para impulsar la generación de trabajos de descarga con las columnas numéricas y de datos en formato externo.
3. A continuación, los datos se transfieren a Amazon S3 mediante AWS Transfer Family.
4. Un trabajo de extracción, transformación y carga (ETL) de AWS Glue puede transformar los datos y cargarlos en un bucket procesado en el formato especificado, o bien AWS Glue puede introducir los datos directamente en la base de datos.
5. Amazon Athena y Amazon se QuickSight pueden usar para consultar y renderizar los datos para impulsar el análisis.

En el siguiente diagrama se muestra un flujo lógico de todo el proceso.

1. El primer JCL, denominado TABNAME, usará la utilidad DSNTIAUL de Db2 para extraer y generar la lista de tablas que planea descargar de Db2. Para elegir las tablas, debe adaptar manualmente la entrada SQL para seleccionar y añadir criterios de filtro que incluyan uno o más esquemas de Db2.
2. El segundo JCL, denominado REXXEXEC, usará un esqueleto de JCL y el programa REXX proporcionado para procesar la lista de tablas creada por el JCL TABNAME y generar un JCL por nombre de tabla. Cada JCL incluirá un paso para descargar la tabla y otro paso para enviar el archivo al bucket de S3 mediante el protocolo SFTP.
3. El último paso consiste en ejecutar el JCL para descargar la tabla y transferir el archivo a AWS. Todo el proceso se puede automatizar con AWS o mediante un programador en las instalaciones.

Tools (Herramientas)

Servicios de AWS

- Amazon Athena es un servicio interactivo de consultas que le permite analizar datos directamente en Amazon Simple Storage Service (Amazon S3) usando SQL estándar.

- Amazon Aurora es un motor de base de datos relacional completamente administrado diseñado para la nube y compatible con MySQL y PostgreSQL.
- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.
- Amazon QuickSight es un servicio de inteligencia empresarial (BI) a escala de nube que le ayuda a visualizar, analizar y elaborar informes sobre sus datos en un único panel de control.
- Amazon Redshift es un servicio de almacenamiento de datos administrado de varios petabytes en la nube de AWS.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Transfer Family es un servicio de transferencia segura que le permite transferir archivos dentro y fuera de los servicios de almacenamiento de AWS.

Herramientas de mainframe

- El Protocolo SSH File Transfer (SFTP) es un protocolo seguro de transferencia de archivos que permite el inicio de sesión remoto y la transferencia de archivos entre servidores. SSH proporciona seguridad al cifrar todo el tráfico.
- DSNTIAUL es un programa de muestra proporcionado por IBM para descargar datos.
- DSNUTILB es un programa de utilidades por lotes proporcionado por IBM para descargar datos con diferentes opciones de DSNTIAUL.
- z/OS OpenSSH es un puerto SSH de software de código abierto que se ejecuta en el Servicio de Sistema Unix bajo la red del sistema operativo IBM. z/OS. SSH is a secure, encrypted connection program between two computers running on a TCP/IP Proporciona múltiples utilidades, como ssh-keygen.
- El script REXX (Restructured Extended Executor) se usa para automatizar la generación de JCL con los pasos Db2 Unload y SFTP.

Código

El código de este patrón está disponible en el repositorio unloaddb2. GitHub

Prácticas recomendadas

Para la primera descarga, lo generado JCLs debería descargar todos los datos de la tabla.

Tras la primera descarga completa, realice descargas graduales para mejorar el rendimiento y ahorrar costos. Actualice la consulta SQL de la plantilla JCL para adaptarla a cualquier cambio en el proceso de descarga.

Puede convertir el esquema manualmente o mediante un script de Lambda con SYSPUNCH de Db2 como entrada. Para un proceso industrial, la herramienta de conversión de esquemas (SCT) de AWS es la opción recomendada.

Por último, use un programador basado en mainframe o un programador en AWS con un agente en el mainframe para ayudar a gestionar y automatizar todo el proceso.

Epics

Configuración del bucket de S3

Tarea	Descripción	Habilidades requeridas
Cree el bucket de S3.	Para obtener instrucciones, consulte Crear su primer bucket de S3.	AWS general

Configure el servidor Transfer Family

Tarea	Descripción	Habilidades requeridas
Cree un servidor compatible con SFTP.	Para abrir y crear un servidor SFTP en la consola de AWS Transfer Family, haga lo siguiente: 1. En la página Elegir protocolos, active la casilla SFTP (Protocolo SSH File Transfer): transferencia de	AWS general

Tarea	Descripción	Habilidades requeridas
	archivos a través de Secure Shell. 2. Para el proveedor de identidad, seleccione Service managed (Administrado por el servicio). 3. En el punto de conexión, seleccione Acceso público. 4. En el dominio, seleccione Amazon S3. 5. En la página Configurar detalles adicionales, mantenga la configuración predeterminada. 6. Cree el servidor.	
Cree un rol de IAM para Transfer Family.	Para crear un rol de AWS Identity and Access Management (IAM) que permita a Transfer Family obtener acceso a Amazon S3, siga las instrucciones de Crear una política y rol de IAM.	Administrador de AWS
Añada un usuario gestionado por el servicio Amazon S3.	Para añadir el usuario gestionado por el servicio Amazon S3, siga las instrucciones de la documentación de AWS y use su ID de usuario de mainframe.	AWS general

Proteja el protocolo de comunicación

Tarea	Descripción	Habilidades requeridas
Cree la clave de SSH.	En el entorno de USS de su servidor principal, ejecute el siguiente comando. `ssh-keygen -t rsa` **Note** Cuando se le pida una contraseña, deje el campo vacío.	Desarrollador de Mainframe

Proporcione los niveles de autorización correctos a la carpeta SSH y a los archivos de clave.	De forma predeterminada, las claves públicas y privadas se almacenarán en el directorio de usuario `/u/home/username/.ssh` .
	Debe conceder autorización 644 a los archivos de clave, y 700 a la carpeta.
	`chmod 644 .ssh/id_rsa`
	`chmod 700 .ssh`
		Desarrollador de Mainframe

Copie el contenido de la clave pública a su usuario gestionado por el servicio Amazon S3.	Para copiar el contenido de clave pública generado por USS abra la consola de AWS Transfer Family. 1. En el panel de navegación, seleccione Servers (Servidores).	Desarrollador de Mainframe

Tarea	Descripción	Habilidades requeridas
	2. Seleccione el identificador en la columna Server ID (ID de servidor) para ver los Server details (Detalles del servidor) 3. En Usuarios, seleccione un nombre de usuario para ver la página de Detalles del usuario 4. En SSH public keys, seleccione Add SSH public key (Añadir clave pública de SSH) para añadir una nueva clave SSH pública a un usuario. En la clave pública de SSH, introduzca su clave pública. El servicio valida su clave antes de que añada al nuevo usuario. 5. Elija Agregar clave.	

Genera el JCLs

Tarea	Descripción	Habilidades requeridas
Genere la lista de tablas Db2 incluidas.	Proporcione el código SQL de entrada para crear una lista de las tablas destinadas a la migración de datos. Este paso requiere que especifique los criterios de selección consultando la tabla SYSIBM.SYSTABLES del	Desarrollador de Mainframe

Tarea	Descripción	Habilidades requeridas
	catálogo de Db2 mediante una cláusula where de SQL. Los filtros se pueden personalizar para incluir un esquema específico, o bien nombres de tablas que comiencen con un prefijo concreto o en función de una marca de tiempo para la descarga gradual. El resultado se captura en un conjunto de datos secuencial físico (PS) en el mainframe. Este conjunto de datos servirá de entrada para la siguiente fase de generación de JCL. Antes de usar JCL TABNAME (puede renombrarlo si es necesario), realice los siguientes cambios: 1. Sustituya <Jobcard> por una clase de trabajo y un usuario autorizado a ejecutar las utilidades de Db2. 2. Sustituya < HLQ1 > o personalice los nombres de los conjuntos de datos de salida para que cumplan con los estándares de su sitio. 3. Actualice la pila STEPLIB de PDSEs (conjunto de datos particionado	

Tarea	Descripción	Habilidades requeridas

	ampliado) de acuerdo con los estándares de su sitio. El ejemplo de este patrón emplea los valores predeterminados de IBM.
	4. Sustituya el nombre de PLAN y el LIB por los valores específicos de su instalación.
	5. Sustituya <Schema> y <Prefix> por sus criterios de selección del catálogo de Db2.
	6. Guarde el JCL resultant e en una biblioteca PDS (conjunto de datos particion ado).
	7. Envíe el JCL.
	
	Trabajo de extracción de lista de tablas de Db2
	
	`<Jobcard>`
	`//*`
	`//* UNLOAD ALL THE TABLE`
	`NAMES FOR A PARTICULAR`
	`SCHEMA`
	`//*`
	`//STEP01 EXEC PGM=IEFBR`
	`14`
	`//*`
	`//DD1 DD DISP=(MOD`
	`,DELETE,DELETE),`
	`// UNIT=SYSDA,`
	`// SPACE=(1000,`
	`(1,1)),`	

Tarea	Descripción	Habilidades requeridas

	`//  DSN=<HLQ1 >.DSN81210.TABLIST`
	`//*`
	`//DD2  DD  DISP=(MOD ,DELETE,DELETE),`
	`//  UNIT=SYSDA,`
	`//  SPACE=(1000, (1,1)),`
	`//  DSN=<HLQ1 >.DSN81210.SYSPUNCH`
	`//*`
	`//UNLOAD  EXEC PGM=IKJEF T01,DYNAMNBR=20`
	`//SYSTSPRT DD`
	` SYSOUT=*`
	`//STEPLIB  DD`
	` DISP=SHR,DSN=DSNC1 0.DBCG.SDSNEXIT`
	`//  DD  DISP=SHR, DSN=DSNC10.SDSNLOAD`
	`//  DD  DISP=SHR, DSN=CEE.SCEERUN`
	`//  DD  DISP=SHR, DSN=DSNC10.DBCG.RU NLIB.LOAD`
	`//SYSTSIN  DD  *`
	`  DSN SYSTEM(DBCG)`
	`  RUN  PROGRAM(D SNTIAUL) PLAN(DSNT IB12) PARMS('SQL') -`
	`  LIB('DSNC 10.DBCG.RUNLIB.LOAD')`
	`  END`
	`//SYSPRINT DD SYSOUT=*`
	`//*`
	`//SYSUDUMP DD SYSOUT=*`
	`//*`
	`//SYSREC00 DD DISP=(NEW ,CATLG,DELETE),`
	`//  UNIT=SYSD A,SPACE=(32760,(10 00,500)),`	

Tarea	Descripción	Habilidades requeridas

	`//  DSN=<HLQ1>.DSN81210.TABLIST`
	`//*`
	`//SYSPUNCH DD DISP=(NEW,CATLG,DELETE),`
	`//  UNIT=SYSDA,SPACE=(32760,(1000,500)),`
	`//  VOL=SER=SCR03,RECFM=FB,LRECL=120,BLKSIZE=12`
	`//  DSN=<HLQ1>.DSN81210.SYSPUNCH`
	`//*`
	`//SYSIN  DD *`
	`  SELECT CHAR(CREATOR), CHAR(NAME)`
	`  FROM SYSIBM.SYSTABLES`
	`  WHERE OWNER = '<Schema>'`
	`  AND NAME LIKE '<Prefix>%'`
	`  AND TYPE = 'T';`
	`/*`	

Tarea	Descripción	Habilidades requeridas
Modifique las plantillas de JCL.	Las plantillas JCL proporcionadas con este patrón contienen una tarjeta de trabajo y nombres de bibliotecas genéricas. Sin embargo, la mayoría de los sitios de mainframe tendrán sus propios estándares de nomenclatura para los nombres de conjuntos de datos, bibliotecas y tarjetas de trabajo. Por ejemplo, es posible que necesite una clase de trabajo específica para ejecutar trabajos de Db2. El subsistema Job Entry implementa JES2 y JES3 puede imponer cambios adicionales. Las bibliotecas de carga estándar pueden tener un primer calificador diferente a SYS1, que es el predeterminado de IBM. Por lo tanto, personalice las plantillas para adecuarlas a los estándares específicos de su sitio antes de ejecutarlas. Realice los siguientes cambios en el esqueleto de JCL UNLDSKEL: 1. Sustituya la tarjeta de trabajo por una clase de trabajo y un usuario	Desarrollador de Mainframe

Tarea	Descripción	Habilidades requeridas
	autorizado a ejecutar las utilidades de Db2. 2. Personalice los nombres de los conjuntos de datos de salida para adecuarlos los estándares de su sitio. 3. Actualice la pila STEPLIB de PDSEs acuerdo con los estándares de su sitio. El ejemplo de este patrón emplea los valores predeterminados de IBM. 4. Sustituya <DSN> por el nombre y la ID de correlaci ón del subsistema Db2. 5. Guarde el JCL resultante en una biblioteca de PDS que forme parte de su pila de ISPSLIB, biblioteca básica de plantillas estándar para ISPF. Descargue el esqueleto de JCL mediante SFTP `//&USRPFX.U JOB (DB2UNLOAD),'JOB', CLASS=A,MSGCLASS=A, //  TIME=1440 ,NOTIFY=&USRPFX //* DELETE DATASETS //STEP01  EXEC PGM=IEFBR14 //DD01  DD DISP=(MOD ,DELETE,DELETE),`	

Tarea	Descripción	Habilidades requeridas

	`//  UNIT=SYSD`
	`A,`
	`//  SPACE=(TR`
	`K,(1,1)),`
	`// DSN=&USRPFX..DB2.P`
	`UNCH.&JOBNAME`
	`//DD02  DD DISP=(MOD`
	`,DELETE,DELETE),`
	`//  UNIT=SYSD`
	`A,`
	`//  SPACE=(TR`
	`K,(1,1)),`
	`// DSN=&USRPFX..DB2.U`
	`NLOAD.&JOBNAME`
	`//*`
	`//* RUNNING DB2`
	` EXTRACTION BATCH JOB`
	` FOR AWS DEMO`
	`//*`
	`//UNLD01  EXEC`
	` PGM=DSNUTILB,REGIO`
	`N=0M,`
	`// PARM='<DSN>,UNLOAD'`
	`//STEPLIB  DD`
	` DISP=SHR,DSN=DSNC1`
	`0.DBCG.SDSNEXIT`
	`//  DD  DISP=SHR,`
	`DSN=DSNC10.SDSNLOAD`
	`//SYSPRINT DD  SYSOUT=*`
	`//UTPRINT  DD  SYSOUT=*`
	`//SYSOUT  DD  SYSOUT=*`
	`//SYSPUN01 DD`
	` DISP=(NEW,CATLG,DE`
	`LETE),`
	`//  SPACE=(CY`
	`L,(1,1),RLSE),`
	`// DSN=&USRPFX..DB2.P`
	`UNCH.&JOBNAME`
	`//SYSREC01 DD`
	` DISP=(NEW,CATLG,DE`
	`LETE),`	

Tarea	Descripción	Habilidades requeridas

	`//  SPACE=(CYL,(10,50),RLSE),`
	`// DSN=&USRPFX..DB2.UNLOAD.&JOBNAME`
	`//SYSPRINT DD SYSOUT=*`
	`//SYSIN  DD *`
	`  UNLOAD`
	`  DELIMITED COLDEL ','`
	`  FROM TABLE &TABNAME`
	`  UNLDDN SYSREC01`
	`  PUNCHDDN SYSPUN01`
	`  SHRLEVEL CHANGE`
	`  ISOLATION UR;`
	`  /*`
	`//*`
	`//* FTP TO AMAZON S3`
	`  BACKED FTP SERVER IF`
	`  UNLOAD WAS SUCCESSFUL`
	`//*`
	`//SFTP EXEC PGM=BPXBATCH,COND=(4,LE),REGION=0M`
	`//STDPARM DD *`
	`  SH cp "//'&USRPFX..DB2.UNLOAD.&JOBNAME'"`
	`  &TABNAME..csv;`
	`  echo "ascii`
	`  " >> uplcmd;`
	`  echo "PUT &TABNAME..csv " >>>> uplcmd;`
	`  sftp -b uplcmd -i .ssh/id_rsa &FTPUSER.@&FTPSITE;`
	`  rm &TABNAME..csv;`
	`  //SYSPRINT DD SYSOUT=*`
	`  //STDOUT DD SYSOUT=*`
	`  //STDENV DD *`
	`  //STDERR DD SYSOUT=*`	

Tarea	Descripción	Habilidades requeridas

Tarea	Descripción	Habilidades requeridas
Genere el JCL de descarga masiva.	Este paso implica ejecutar un script REXX en un entorno ISPF mediante JCL. Proporcione la lista de tablas incluidas en el primer paso como entrada para la generación masiva de JCL con el nombre `TABLIST DD`. El JCL generará un nuevo JCL por nombre de tabla en un conjunto de datos particionado definido por el usuario y especificado con el nombre `ISPFILE DD`. Asigne esta biblioteca de antemano. Cada nuevo JCL tendrá dos pasos: uno para descargar la tabla de Db2 en un archivo y otro para enviar el archivo al bucket de S3. Realice los siguientes cambios en el JCL REXXEXEC (puede cambiar el nombre): 1. Sustituya `Job card user ID` por una ID de usuario de mainframe con autoridad de descarga de las tablas. Sustituya `SYSPROC`, `ISPPLIB`, `ISPSLIB`, `ISPMLIB` y los valores `ISPTLIB` y `<HLQ1>`, o personalice `DSN` según los estándares de	Desarrollador de Mainframe

Tarea	Descripción	Habilidades requeridas
	su sitio. Para averiguar los valores específicos de su instalación, ejecute el comando `TSO ISRDDN`. 2. Sustituya `<MFUSER>` por un ID de usuario con privilegios de ejecución de tareas en la instalación. 3. Sustituya `<FTPUSER>` por un ID de usuario con privilegios de USS y FTP en la instalación. Se presupone que esta ID de usuario y sus claves de seguridad SSH se encuentran en el directorio de Unix Systems Services correspondiente de la computadora central. 4. Sustituya `<AWS TransferFamily IP>` por la dirección IP o el nombre de dominio de AWS Transfer Family. Esta dirección se utilizará para el paso de SFTP. 5. Envíe el JCL después de solicitar el alojamiento estándar del sitio y actualizar el programa REXX como se describe a continuación.	

Tarea	Descripción	Habilidades requeridas

	Generación masiva de trabajos JCL
	
	`//RUNREXX JOB (CREATEJCL),'RUNS ISPF TABLIST', CLASS=A,MSGCLASS=A,`
	
	`//  TIME=1440 ,NOTIFY=&SYSUID`
	`//* Most of the values required can be updated to your site specific`
	`//* values using the command 'TSO ISRDDN' in your ISPF session.`
	`//* Update all the lines tagged with //update marker to desired`
	`//* site specific values.`
	`//ISPF EXEC PGM=IKJEFT01,REGION=2048K,DYNAMNBR=25`
	`//SYSPROC DD DISP=SHR,DSN=USER.Z23D.CLIST`
	`//SYSEXEC DD DISP=SHR,DSN=<HLQ1>.TEST.REXXLIB`
	`//ISPPLIB DD DISP=SHR,DSN=ISP.SISPPENU`
	`//ISPSLIB DD DISP=SHR,DSN=ISP.SISPSENU`
	`//  DD DISP=SHR,DSN=<HLQ1>.TEST.ISPSLIB`
	`//ISPMLIB DD DSN=ISP.SISPMENU,DISP=SHR`	

Tarea	Descripción	Habilidades requeridas

	`//ISPTLIB DD`
	`DDNAME=ISPTABL`
	`// DD DSN=ISP.S`
	`ISPTENU,DISP=SHR`
	`//ISPTABL DD`
	`LIKE=ISP.SISPTENU,`
	`UNIT=VIO`
	`//ISPPROF DD`
	`LIKE=ISP.SISPTENU,`
	`UNIT=VIO`
	`//ISPLOG DD`
	`SYSOUT=*,RECFM=VA,`
	`LRECL=125`
	`//SYSPRINT DD SYSOUT=*`
	`//SYSTSPRT DD`
	`SYSOUT=*`
	`//SYSUDUMP DD`
	`SYSOUT=*`
	`//SYSDBOUT DD`
	`SYSOUT=*`
	`//SYSTSPRT DD`
	`SYSOUT=*`
	`//SYSUDUMP DD`
	`SYSOUT=*`
	`//SYSDBOUT DD`
	`SYSOUT=*`
	`//SYSHELP DD`
	`DSN=SYS1.HELP,DISP`
	`=SHR`
	`//SYSOUT DD SYSOUT=*`
	`//* Input list of`
	`tablenames`
	`//TABLIST DD`
	`DISP=SHR,DSN=<HLQ1`
	`>.DSN81210.TABLIST`
	`//* Output pds`
	`//ISPFILE DD`
	`DISP=SHR,DSN=<HLQ1`
	`>.TEST.JOBGEN`
	`//SYSTSIN DD *`	

Tarea	Descripción	Habilidades requeridas
	``` ISPSTART CMD(ZSTEPS <MFUSER> <FTPUSER> <AWS TransferFamily IP>) /* ``` Antes de ejecutar el script REXX, realice los siguientes cambios: 1. Guarde el script REXX en una biblioteca PDS definida en la pila `SYSEXEC` del JCL REXXEXEC, editada en el paso anterior con el nombre de miembro ZSTEPS. Si desea renombrarlo, actualice el JCL según sus necesidades. 2. Este script usa la opción de rastreo para imprimir información adicional en caso de que se produzcan errores. En su lugar, puede añadir un código de gestión de errores después de las instrucciones `EXECIO`, `ISPEXEC` y `TSO`, y eliminar la línea de rastreo. 3. Este script genera nombres de miembro con la convención de nomenclatura `L0Dnnnnn`, con capacidad para hasta 100 000 miembros. Si tiene más de 100 000 tablas, use un	

Tarea	Descripción	Habilidades requeridas
	prefijo más corto y ajuste los números de la instrucción `tempjob`. Script ZSTEPS REXX `/*REXX - - -

Tarea	Descripción	Habilidades requeridas

	<pre> ADDRESS ISPEXEC
	 "FTINCL UNLDSKEL"
	     /* member will be
	 saved in ISPDSN library
	 allocated in JCL */
	     ADDRESS ISPEXEC
	 "FTCLOSE NAME("tem
	pjob")"
	    END
	
	    ADDRESS TSO "FREE
	 F(TABLIST) "
	    ADDRESS TSO "FREE
	 F(ISPFILE) "
	
	exit 0</pre>	

Ejecute el JCLs

Tarea	Descripción	Habilidades requeridas
Realice el paso de descarga de Db2.	Tras la generación del JCL, tendrá tantas tablas JCLs como desee descargar. Esta historia emplea un ejemplo generado por el JCL para explicar la estructura y los pasos más importantes. No tiene que hacer nada. La siguiente información es solo para referencia. Si su intención es enviar las JCLs que ha generado en el paso anterior, vaya a Enviar la LODnnnnn JCLs tarea.	Desarrollador de mainframe, ingeniero de sistemas

Tarea	Descripción	Habilidades requeridas

	Al descargar datos de Db2 usando un JCL con la utilidad DSNUTILB Db2 proporcionada por IBM, debe asegurarse de que los datos descargados no contengan datos numéricos comprimidos. Para ello, utilice el parámetro de DSNUTILB `DELIMITED` .
	
	El parámetro `DELIMITED` permite descargar los datos en formato CSV añadiendo un carácter como delimitador y comillas dobles para el campo de texto, eliminando el relleno de la columna VARCHAR y convirtiendo todos los campos numéricos a FORMATO EXTERNO, incluidos los campos de FECHA.
	
	El siguiente ejemplo muestra el aspecto del paso de descarga en el JCL generado, usando el carácter de coma como delimitador.
	
	`UNLOAD`
	`DELIMITED COLDEL ','`
	`FROM TABLE SCHEMA_NAME.TBNAME`
	`UNLDDN SYSREC01`
	`PUNCHDDN SYSPUN01`	

Tarea	Descripción	Habilidades requeridas
	`SHRLEVEL CHANGE ISOLATION UR;`	
Realice el paso de SFTP.	Para usar el protocolo SFTP de un JCL, emplee la utilidad BPXBATCH. La utilidad SFTP no puede acceder directamente a los conjuntos de datos de MVS. Puede usar el comando de copia (`cp`) para copiar el archivo secuencial `&USRPFX..DB2.UNLOAD.&JOBNAME` al directorio USS, donde se convierte en `&TABNAME..csv` . Ejecute el comando `sftp` con la clave privada (`id_rsa`) y la ID de usuario de RACF como nombre de usuario para conectarse a la dirección IP de AWS Transfer Family. `SH cp "//'&USRPFX..DB2.UNLOAD.&JOBNAME'" &TABNAME..csv; echo "ascii " >> uplcmd; echo "PUT &TABNAME..csv " >>>> uplcmd; sftp -b uplcmd -i .ssh/id_rsa &FTPUSER.@&FTP_TF_SITE; rm &TABNAME..csv;`	Desarrollador de mainframe, ingeniero de sistemas

Tarea	Descripción	Habilidades requeridas
Envíe el LODnnnnn JCLs.	El JCL anterior generaba todas las tablas de LODnnnnn JCL que debían descargar se, transformarse en CSV y transferirse al bucket de S3. Ejecute el `submit` comando en todas las JCLs que se hayan generado.	Desarrollador de mainframe, ingeniero de sistemas

Recursos relacionados

Para obtener más información sobre las diferentes herramientas y soluciones usadas en este documento, consulte lo siguiente:

- Guía del usuario de z/OS OpenSSH
- Db2 z/OS — Ejemplos de sentencias de control UNLOAD
- Db2 z/OS — Descarga de archivos delimitados
- Transfer Family: cree un servidor habilitado para SFTP
- Transfer Family: trabajar con usuarios gestionados por servicios

Información adicional

Una vez que tenga sus datos de Db2 en Amazon S3, podrá obtener información de múltiples maneras. Como Amazon S3 se integra con los servicios de análisis de datos de AWS, puede consumir o exponer libremente estos datos de forma distribuida. Por ejemplo, puede hacer lo siguiente:

- Cree un lago de datos en Amazon S3 y extraiga información valiosa mediante query-in-place el uso de herramientas de análisis y aprendizaje automático sin mover los datos.
- Iniciar una función de Lambda configurando un flujo de trabajo de procesamiento posterior a la carga integrado con AWS Transfer Family.
- Desarrollar nuevos microservicios para acceder a los datos en Amazon S3 o en una base de datos totalmente administrada con AWS Glue, un servicio de integración de datos sin servidor que

facilita la detección, preparación y combinación de datos para el análisis, el machine learning y el desarrollo de aplicaciones.

En un caso de uso de migración, dado que puede transferir cualquier dato del mainframe a S3, puede hacer lo siguiente:

- Retirar la infraestructura física y crear una estrategia de archivado de datos rentable con Amazon S3 Glacier y S3 Glacier Deep Archive.
- Crear soluciones de copia de seguridad y restauración escalables, duraderas y seguras con Amazon S3 y otros servicios de AWS, como S3 Glacier y Amazon Elastic File System (Amazon EFS), para mejorar o reemplazar las capacidades existentes en las instalaciones.

Transforma Easytrieve a lenguajes modernos usando AWS Transform personalizado

Shubham Roy, Subramanyam Malisetty y Harshitha Shashidhar, de Amazon Web Services

Resumen

Este patrón proporciona una guía prescriptiva para una transformación más rápida y con menor riesgo de las cargas de trabajo del generador de informes Broadcom Easytrieve (EZT) de mainframe mediante una transformación personalizada de idioma a idioma.AWS Transform Aborda los desafíos de modernizar las cargas de trabajo EZT exclusivas y exclusivas de mainframe que se utilizan habitualmente para el procesamiento de datos por lotes y la generación de informes. Este patrón reemplaza los enfoques de migración costosos, prolongados y propensos a errores, que se basan en herramientas patentadas y una experiencia poco común en mainframe, por una solución automatizada de inteligencia artificial basada en agentes que usted crea. AWS Transform

Este patrón proporciona una definición de transformación personalizada y lista para usar para la transformación EZT. La definición utiliza varias entradas de transformación:

- Reglas de negocio de EZT extraídas mediante métodos personalizados AWS Transform
- Documentación de referencia sobre la programación de EZT
- Código fuente de EZT
- Conjuntos de datos de entrada y salida de mainframe

AWS Transform custom utiliza estas entradas para generar aplicaciones funcionalmente equivalentes en los lenguajes de destino modernos, como Java o Python.

El proceso de transformación utiliza funciones inteligentes de ejecución de pruebas, depuración automática y corrección iterativa para validar la equivalencia funcional con los resultados esperados. También es compatible con el aprendizaje continuo, lo que permite la definición de transformación personalizada para mejorar la precisión y la coherencia en las transformaciones sucesivas. Con este patrón, las organizaciones pueden reducir el esfuerzo y el riesgo de migración, hacer frente a la deuda técnica especializada en mainframes y modernizar las cargas de trabajo de EZT AWS para mejorar la agilidad, la fiabilidad, la seguridad y la innovación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta activa AWS
- Una carga de trabajo EZT para mainframe con datos de entrada y salida

Limitaciones

Limitaciones de alcance

- Compatibilidad con el idioma: solo se admite la EZT-to-Java transformación para este patrón de transformación específico. Este patrón APG se prueba en código EZT en línea en. JCL/Proc
- Fuera de alcance: para la transformación de otros lenguajes de programación de mainframe y uso para mainframe. AWS Transform Obtenga más información en la guía del usuario sobre los tipos de archivos compatibles para la transformación de aplicaciones de mainframe. AWS Transform

Limitaciones del proceso

- Dependencia de la validación: sin los datos de salida de referencia, la transformación no se puede validar.
- Lógica patentada: las utilidades altamente específicas y desarrolladas a medida requieren documentación de usuario adicional y materiales de referencia para que el agente de IA las interprete correctamente.

Limitaciones técnicas

- Límites de servicio: para ver los límites y las cuotas de servicio AWS Transform personalizados, consulte la Guía AWS Transform del usuario (Cuotas) y la referencia AWS general (Transformar cuotas).

Versiones de producto

- AWS Transform CLI — Última versión
- Node.js — versión 2.0 o posterior
- Git — Última versión
- Entorno de destino
  - Java: versión 17 o posterior
  - Spring Boot: la versión 3.x es el objetivo principal de las aplicaciones refactorizadas

- Maven: versión 3.6 o posterior

Arquitectura

Pila de tecnología de origen

- Sistema operativo: IBM z/OS
- Lenguaje de programación — Easytrieve, lenguaje de control de tareas (JCL)
- Base de datos: IBM DB2 para archivos planos de z/OS mainframe, método de acceso al almacenamiento virtual (VSAM)

Pila de tecnología de destino

- Sistema operativo — Amazon Linux
- Computación: Amazon Elastic Compute Cloud (Amazon EC2)
- Lenguaje de programación: Java
- Base de datos Amazon Relational Database Service (Amazon RDS)

Arquitectura de destino

Flujo de trabajo

Esta solución utiliza definiciones de transformación AWS Transform personalizadas y predefinidas para modernizar las aplicaciones Easytrieve (EZT) de mainframe a Java mediante un flujo de trabajo automatizado de tres pasos. AWS Transform custom gestiona todo el proceso (la extracción de reglas empresariales (BRE), la transformación del código y la validación de la equivalencia funcional, basándose en las definiciones de transformación que se proporcionan como parte de esta solución. Se requiere la validación humana para validar el BRE generado y el informe de validación de la equivalencia funcional.

Paso 1: Preparar la carpeta de entradas

1. código fuente/: código fuente EZT (archivos.ezt), flujos de trabajos JCL (archivos.jcl/.jcl), programas COBOL, cuadernos y tarjetas de control
2. bre-doc/: documento de extracción de reglas de negocio generado
3. input-data/: conjuntos de datos de entrada de referencia del ordenador central para su validación

4. output-data/: conjuntos de datos de salida de la computadora central de referencia para su validación
5. document_references/ — Definiciones de transformación y documentación de referencia proporcionada por:

   - `bre_transformation_definition.md` — Define el proceso de extracción de reglas de negocio en 5 fases

   - `transformation_definition.md` — Define cómo Easytrieve construye un mapa para Java

   - `summaries.md` — Reglas y patrones de transformación

   - `ca-easytrieve-report-generator-11-6.txt` — Manual de referencia de Easytrieve

Paso 2: Extraiga reglas empresariales con AWS Transform Custom

1. Interactúe con la AWS Transform CLI mediante un lenguaje natural para revisar las definiciones de transformación (TD) disponibles y personalizar la TD de BRE para que se ajuste a sus criterios y reglas específicos

2. Utilice el TD finalizado para generar el documento BRE: analiza de forma AWS Transform personalizada los artefactos fuente del mainframe (Easytrieve, JCL, COBOL, cuadernos, tarjetas de control) y crea un BRE estructurado con un catálogo de reglas empresariales, diseños de archivos, linaje de datos y mapeos de tipos de datos

3. Mueva el documento BRE generado a la carpeta para usarlo en el paso 3 `bre-doc/`

Paso 3: Generar código modernizado funcional equivalente

1. Interactúe con la AWS Transform CLI mediante un lenguaje natural para revisar las definiciones de transformación base (TD) disponibles y personalizar la TD base para que se ajuste a sus criterios y reglas específicos.
2. A continuación, invoque la AWS Transform CLI con el código fuente del proyecto. AWS Transform custom crea planes de transformación, convierte EZT a Java tras su aprobación, genera archivos auxiliares, crea el JAR ejecutable y valida los criterios de salida.
3. Utilice el agente de validación para probar la equivalencia funcional con la salida del mainframe. El Self-Debugger agente corrige los problemas de forma autónoma. Los resultados finales incluyen informes de validación de código Java y HTML validados.

Automatización y escala

- La arquitectura de ejecución multimodo de Agentic AI (AWS Transform personalizada) aprovecha la IA de Agentic con 3 modos de ejecución (conversacional, interactivo y totalmente automatizado) para automatizar tareas de transformación complejas, como el análisis de código, la refactorización, la planificación de la transformación y las pruebas.
- Sistema de comentarios sobre el aprendizaje adaptativo: la plataforma implementa mecanismos de aprendizaje continuo mediante el análisis de muestras de código, el análisis de la documentación y la integración de los comentarios de los desarrolladores con las definiciones de transformación versionadas.
- Arquitectura de procesamiento simultáneo de aplicaciones: el sistema permite la ejecución paralela distribuida de múltiples operaciones de transformación de aplicaciones simultáneamente en una infraestructura escalable.

Tools (Herramientas)

Servicios de AWS

- AWS Transform custom es un servicio de IA de agencia que se utiliza para transformar las aplicaciones EZT heredadas en lenguajes de programación modernos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos. Amazon S3 sirve como el servicio de almacenamiento principal de AWS Transform Custom para almacenar definiciones de transformaciones, repositorios de código y resultados de procesamiento.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos. La IAM proporciona un marco de seguridad AWS Transform personalizado, gestionando los permisos y el control de acceso para las operaciones de transformación.

Otras herramientas

- AWS Transform CLI es la interfaz de línea de comandos AWS Transform personalizada, que permite a los desarrolladores definir, ejecutar y administrar transformaciones de código personalizadas a través de conversaciones en lenguaje natural y modos de ejecución

automatizados. AWS Transform custom admite sesiones interactivas (atx custom def exec) y transformaciones autónomas para una modernización escalable de las bases de código.

- El sistema de control de versiones de Git se utiliza para la protección de sucursales, el seguimiento de cambios y las capacidades de reversión durante la aplicación de correcciones automatizadas.
- Java es el lenguaje de programación y el entorno de desarrollo utilizados en este patrón.

Repositorio de código

El código de este patrón está disponible en Easytrieve to Modern Languages Transformation with AWS Transform Custom on. GitHub

Prácticas recomendadas

- Establezca una estructura de proyecto estandarizada: cree una estructura de cuatro carpetas (código fuente, bre-doc, datos de entrada y datos de salida), valide la integridad y documente el contenido antes de la transformación.
- Utilice archivos de referencia para la validación: utilice archivos de entrada de referencia de producción, realice una comparación byte a byte con la salida de referencia y acepte la tolerancia cero ante las desviaciones.
- Utilice todos los documentos de referencia disponibles: para aumentar la precisión de la transformación, proporcione todos los documentos de referencia disponibles, como los requisitos empresariales y las listas de verificación de codificación.
- Proporcione información para mejorar la calidad: AWS Transform Custom extrae automáticamente lo aprendido de las ejecuciones de transformación (comentarios de los desarrolladores, problemas de código) y crea elementos de conocimiento para ellos. Después de cada transformación exitosa, revise los elementos de conocimiento y apruebe el que le gustaría utilizar en futuras ejecuciones. Esto mejora la calidad de las futuras transformaciones.

Epics

Configuración AWS Transform personalizado

Tarea	Descripción	Habilidades requeridas
Aprovisione la infraestructura de AWS Transform forma personalizada.	Implemente la infraestr uctura lista para la producció n necesaria para alojar un entorno de transformación seguro. Esto incluye una instancia privada de Amazon EC2 configurada con las herramientas, los permisos de IAM y la configuración de red necesarios para convertir el código de Easytrieve. Para aprovisionar el entorno mediante la infraestructura como código (IaC), siga las instrucciones de implement ación que se encuentran en el repositorio Personalizado con Transformación a Lenguajes Modernos de Easytrieve. AWS Transform GitHub	Desarrollador de aplicaciones, administrador de AWS
Prepare los materiales de entrada para la transform ación.	1. Introduzca este comando para crear la estructura de carpetas: `mkdir -p /root/tra nsform-workspace/m ainframe-source/{s ource-code,bre-doc ,input-data,output- data}`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	Esto crea las siguientes carpetas:
	• `source-code` — Almacenamiento para el código fuente de EZT
	• `bre-doc`— Almacenamiento para el documento BRE
	• `input-data` — Almacenamiento de los datos de entrada para la ejecución por lotes del mainframe (Sequential/Text/DB2 archivos en formato EBCDIC)
	• `output-data` — Almacenamiento de los datos de salida en el mainframe tras la ejecución por lotes (Sequential/Text/DB2 archivos en formato EBCDIC)
	2. Introduce estos comandos para inicializar el repositorio de Git:
	`cd /root/transform-workspace/mainframe-source/source-code`
	`git init`
	`git add .`	

Tarea	Descripción	Habilidades requeridas
	`git commit -m "Initial commit"`	

Crea una definición de transformación personalizada

Tarea	Descripción	Habilidades requeridas
Cree una definición de transformación BRE	Siga estos pasos para crear la definición de transform ación personalizada para BRE (Business Rule Extraction) a partir del código fuente de Easytrieve. 1. Ve al repositorio de códigos de este patrón y copia bre_transformation _definition.md de la carpeta de documentos junto con la carpeta document_reference s de la guía de codificación de EZT. 2. Cargue ese contenido en la carga de la AWS Transform CLI en la ubicación que elija y anote la ubicación de la ruta que se utilizará en los siguientes pasos. 3. Invoque AWS Transform desde la CLI con el comando atx.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	4. Proporcione este mensaje en la CLI: Cree una transformación personalizada utilizando mi archivo de definición de transformación disponible en la ruta <path to content from step #2 > AWS Transform crea una nueva definición de transform ación personalizada para la generación de BRE. 5. Revise la definición de transformación y realice los cambios necesarios.	
Publique la definición de transformación de BRE	Tras revisar y validar la definición de transformación de BRE, puede publicarla en el registro AWS Transform personalizado con un mensaje en lenguaje natural, proporcio nando un nombre de definició n, por ejemplo Easytrieve-Business-Rule-Extract.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Cree una definición de transformación.	Siga estos pasos para crear la definición de transform ación personalizada para la transformación de EZT a Java con validación funcional. 1. Ve al repositorio de código de este patrón y copia el contenido de la `documents` carpeta. Esto debería incluir transformation_def inition.md, summaries .md y la carpeta con la guía de codificación EZT. `document_reference s` 2. Cargue ese contenido en la carga de la AWS Transform CLI en la ubicación que elija y anote la ubicación de la ruta que se utilizará en los siguientes pasos. 3. Invoque AWS Transform desde la CLI con el `atx` comando. 4. Proporcione este mensaje en la CLI: Crear una transformación personali zada con mi archivo de definición de transform ación disponible en la ruta AWS Transform <path to content from step #2 > crea una nueva definición de	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	transformación personali zada para la transformación de EZT a Java. 5. Revise la definición de transformación y realice los cambios necesarios.	
Publique la definición de transformación.	Tras revisar y validar la definición de transformación, puede publicarla en el registro AWS Transform personalizado con un mensaje en lenguaje natural, proporcionando un nombre de definición, por ejemplo Easytrieve-to-Java-Migration.	Desarrollador de aplicaciones

Genere un extracto de reglas de negocio (BRE)

Tarea	Descripción	Habilidades requeridas
Ejecute el trabajo de generación de BRE.	Ejecute el comando AWS Transform CLI y elija la opción interactiva o no interactiva: Non-interactive ejecución (totalmente autónoma): `atx custom def exec -- transformation-name "Easytrieve-Business-Rule-Extract" --code-repository-path ~/root/transform-workspace/mainframe-source/source-code --non-int`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	`eractive --trust-all-tools`
	
	Ejecución interactiva (con supervisión humana):
	
	`atx custom def exec -n "Easytrieve-Business-Rule-Extract" -p ~/root/transform-workspace/mainframe-source/source-code`
	
	Reanudar la ejecución interrumpida:
	
	`atx --resume`
	
	OR
	
	`atx --conversation-id <conversation-id>`
	
	Mueva el documento BRE generado a la carpeta bre-doc/ para usarlo como entrada durante el Easytrieve-to-Java paso de transformación.	

Prepare los datos de referencia para su validación.

Tarea	Descripción	Habilidades requeridas
Revise el resumen de validación de la transformación.	Antes de ejecutar la transformación AWS Transform personalizada, compruebe	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	que la `input-data` carpeta contiene los archivos de datos necesarios capturados antes de ejecutar el trabajo por lotes del mainframe. Tras ejecutar el trabajo por lotes en el ordenador central, asegúrese de que la `output-data` carpeta capture los archivos resultantes. Todos los archivos tienen un Sequential/Text/DB2 formato que utiliza la codificación EBCDIC según los requisitos de ejecución. • Coloque los datos de entrada en la carpeta `input-data/` • Coloque la salida de referencia en `output-data/` la carpeta	

Tarea	Descripción	Habilidades requeridas

Ejecute el trabajo de transform ación personalizado.	Ejecute el comando AWS Transform CLI y elija la opción interactiva o no interactiva:
	
	:# Non-interactive
	 execution (fully
	 autonomous):
	atx custom def exec \
	  --transformation-n
	ame "Easytrieve-to-Jav
	a-Migration" \
	  --code-repository-
	path ~/root/transform-
	workspace/mainframe-
	source/source-code \
	  --build-command "mvn
	 clean install" \
	  --non-interactive \
	  --trust-all-tools \
	
	# Interactive execution
	 (with human oversight
	):
	atx custom def exec \
	  -n "Easytrieve-to-Jav
	a-Migration" \
	  -p ~/root/transform-
	workspace/mainframe-
	source/source-code \
	  -c "mvn clean install"
	
	# Resume interrupted
	 execution:
	atx -resume
	# OR
	atx --conversation-id
	 <conversation-id>
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	AWS Transform se valida automáticamente mediante build/test comandos durante la ejecución de la transform ación.	

Valide y entregue el código probado

Tarea	Descripción	Habilidades requeridas

Revise el resumen de validación de la transform ación.	1. Espere AWS Transform a que el código se valide automáticamente mediante los comandos de compilaci ón y prueba.
	2. Ingresa este comando para buscar la última sesión:
	`LATEST_SESSION=$(l s -t ~/.aws/atx/ custom/ | head -1`
	3. Introduzca este comando para ver el resumen de la validación:
	`cat ~/.aws/atx/ custom/$LATEST_S ESSION/artifacts/v alidation_summary. md`
	4. Introduzca este comando para comprobar el estado general:
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`grep "OVERALL STATUS" ~/.aws/atx/custom/$LATEST_SESSION/artifacts/validation_summary.md`	

Acceda a los informes de validación.	Introduzca estos comandos para revisar los artefactos de validación detallados:
	`# Full validation report`
	`cat ~/.aws/atx/custom/$LATEST_SESSION/artifacts/validation_report.html`
	`# Generated code location`
	`ls ~/.aws/atx/custom/$LATEST_SESSION/generated/`
	`# Execution logs`
	`cat ~/.aws/atx/custom/$LATEST_SESSION/logs/execution.log`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Habilite los elementos de conocimiento para un aprendizaje continuo.	Mejore la precisión de la transformación futura al incluir los elementos de conocimiento sugeridos en su configuración persistente. Tras una transformación, el agente almacena los patrones identificados y las reglas de mapeo en el directorio de sesión local. Para revisar y aplicar estos elementos aprendidos, ejecute estos comandos en su instancia de Amazon EC2:
	
	`# List all knowledge items for a specific transformation definition`
	`atx custom def list-ki -n <transformation-name>`
	
	`# Retrieve the details of a specific knowledge item`
	`atx custom def get-ki -n <transformation-name> --id <id>`
	
	`# Update the status of a knowledge item (ENABLED or DISABLED)`
	`atx custom def update-ki-status -n <transformation-name> --id <id> --status ENABLED`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`# Update the knowledge item configuration to enable auto-approval` `atx custom def update-ki-config -n <transformation-name> --auto-enabled TRUE`	

Resolución de problemas

Problema	Solución
Configuración de las rutas de entrada y salida Los archivos de entrada no se leen o los archivos de salida no se escriben correctamente.	Especifique la ruta completa del directorio donde se almacenan los archivos de entrada e indique claramente la ubicación en la que debe escribirse la salida. Asegúrese de que los permisos de acceso adecuados estén configurados para estos directorios. Las mejores prácticas incluyen el uso de rutas absolutas en lugar de rutas relativas para evitar la ambigüedad y la verificación de que todas las rutas especificadas existan con los permisos adecuados read/write .
Reanudar las ejecuciones interrumpidas La ejecución se interrumpió o debe continuar desde donde se detuvo	Puede reanudar la ejecución desde donde la dejó proporcionando el ID de conversación en el comando CLI. Busque el ID de la conversación en los registros del intento de ejecución anterior.
Resolver las restricciones de memoria Se produce un error de memoria insuficiente durante la ejecución.	Puede solicitar AWS Transform compartir el tamaño actual de la JVM en memoria y, a continuación, aumentar la asignación de memoria en función de esta información. Este

Problema	Solución
	ajuste ayuda a adaptarse a mayores requisitos de procesamiento. Considere la posibilidad de dividir los trabajos grandes en lotes más pequeños si persisten las limitaciones de memoria después de los ajustes.
Abordar las discrepancias en los archivos de salida Los archivos de salida no coinciden con las expectativas e AWS Transform indican que no es posible realizar más cambios.	Proporcione comentarios específicos y razones técnicas que expliquen por qué la salida actual es incorrecta. Incluya documentación técnica o empresarial adicional para respaldar sus requisitos. Este contexto detallado ayuda a AWS Transform corregir el código para generar los archivos de salida adecuados. • Ejemplos específicos que comparan el resultado esperado con el real • Referencias a la documentación o las normas pertinentes • Explicación clara del impacto de la discrepancia en el negocio

Recursos relacionados

- AWS Transform documentación personalizada
- Generador de informes Easytrieve 11.6

Más patrones

- Implemente las automatizaciones de seguridad para la AWS WAF solución mediante Terraform
- Replicar bases de datos de unidades centrales en AWS mediante Precisely Connect

Administración

Temas

- Administración de costos
- Informática para usuarios finales
- Computación de alto rendimiento
- Nube híbrida
- Gestión y gobernanza
- Mensajería y comunicaciones
- Estrategia de varias cuentas

Administración de costos

Temas

- Crear informes detallados de costos y uso para los trabajos de AWS Glue con el explorador de costos de AWS
- Crear informes detallados de costos y uso para los clústeres de Amazon EMR mediante el explorador de costos de AWS.
- Más patrones

Crear informes detallados de costos y uso para los trabajos de AWS Glue con el explorador de costos de AWS

Parijat Bhide y Aromal Raj Jayarajan, Amazon Web Services

Resumen

Este patrón muestra cómo realizar un seguimiento de los costos de uso de los trabajos de integración de datos de AWS Glue mediante la configuración de etiquetas de asignación de costos definidas por el usuario. Puede usar estas etiquetas para crear informes detallados de costos y uso en el explorador de costos de AWS para trabajos en varias dimensiones. Por ejemplo, puede realizar un seguimiento de los costos de uso a nivel de equipo, proyecto o centro de costos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Uno o más Trabajos de AWS Glue que tienen activadas las etiquetas definidas por el usuario

Arquitectura

Pila de tecnología de destino

- AWS Glue
- Explorador de costos de AWS

En el siguiente diagrama se muestra cómo aplicar etiquetas para realizar un seguimiento de los costos de uso de los trabajos de AWS Glue.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un ingeniero de datos o un administrador de AWS crea etiquetas de asignación de costos definidas por el usuario para los trabajos de AWS Glue.
2. Un administrador de AWS activa las etiquetas.
3. Las etiquetas envían los metadatos al explorador de costos de AWS.

Tools (Herramientas)

- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.
- El Explorador de costos de AWS permite ver y analizar los costos y el uso.

Epics

Crear y activar etiquetas para sus trabajos de AWS Glue

Tarea	Descripción	Habilidades requeridas
Cree etiquetas de asignación de costos definidas por el usuario para los trabajos de AWS Glue.	Para añadir etiquetas a un trabajo de AWS Glue existente 1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la consola de AWS Glue. 2. En el panel de navegación izquierdo, en ETL, elija Trabajos. 3. En la sección Sus trabajos, seleccione el nombre del trabajo que va a etiquetar. 4. Elija la pestaña Detalles del trabajo. A continuación, expanda la sección de Propiedades avanzadas. 5. En Etiquetas, elija Agregar etiqueta nueva. 6. En Nombre, escriba un nombre para su etiqueta.	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	7. (Opcional) En Valor, introduzca un valor que desee asociar a la clave. 8. (Opcional) Repita los pasos del 5 al 7 para cada etiqueta que quiera crear para la tarea. 9. Seleccione Save. Para añadir etiquetas a un nuevo trabajo de AWS Glue 1. Cree un nuevo trabajo de AWS Glue en función de los requisitos del caso de uso. Para obtener instrucciones, consulte Trabajar con trabajos en la consola de AWS Glue en la Guía para desarrolladores de AWS Glue. 2. Cuando configure los ajustes de Detalles del trabajo, siga los pasos del 4 al 9 de la sección Cómo añadir etiquetas a un trabajo de AWS Glue existente de esta tarea. **Note** Para obtener más información, consulte Etiquetas de AWS en	

Tarea	Descripción	Habilidades requeridas
	AWS Glue en la Guía para desarrolladores de AWS Glue.	
Active las etiquetas de asignación de costos definidas por el usuario.	Siga las instrucciones de Activación de etiquetas de asignación de costos definidas por el usuario en la Guía del usuario de facturación de AWS.	Administrador de AWS

Crear informes de costos y uso para sus trabajos de AWS Glue

Tarea	Descripción	Habilidades requeridas
Cree informes de costos y uso para sus trabajos de AWS Glue mediante filtros de etiquetas en el explorador de costos de AWS.	1. Inicie sesión en la consola de administración de AWS y abra la consola de administración de AWS. 2. En el panel de navegación izquierdo, elija Informes. 3. Elija Crear nuevo informe. 4. En Seleccione un tipo de informe, seleccione Costo y uso (recomendado). A continuación, elija Crear informe. 5. En Filtros, seleccione Servicio. Se muestra el menú desplegable del Servicio. 6. Seleccione la casilla situada junto a Glue. A continuac	AWS general, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	ión, seleccione Aplicar filtros. 7. Para los Filtros, seleccione Etiqueta. Se muestra el menú desplegable de Etiqueta. 8. Seleccione Equipo. A continuación, seleccione las casillas de verificación situadas junto a los equipos a los que haya asignado etiquetas. Excluya a los equipos a los que no haya asignado etiquetas. A continuación, seleccione Aplicar filtros. 9. En la parte superior del gráfico, seleccione Etiqueta. A continuación, seleccione las etiquetas de los trabajos de AWS Glue para los que desee crear un informe. 10. En la parte superior del gráfico, seleccione el menú desplegable de los Últimos 3 meses y seleccione el período que desea que abarque el informe. A continuación, seleccione el menú desplegable Mensual y seleccione cómo quiere que se agreguen las partidas del informe	

Tarea	Descripción	Habilidades requeridas
	en función del período de tiempo. 11. Elija Save as (Guardar como). A continuación, introduzca un título para su informe. 12. Elija Save report. Para obtener más información, consulte Exploración de sus datos con Cost Explorer en la Guía del usuario de administración de costos de AWS.	

Crear informes detallados de costos y uso para los clústeres de Amazon EMR mediante el explorador de costos de AWS.

Parijat Bhide y Aromal Raj Jayarajan, Amazon Web Services

Resumen

Este patrón muestra cómo realizar un seguimiento de los costos de uso de los clústeres de Amazon EMR mediante la configuración de etiquetas de asignación de costos definidas por el usuario. Puede usar estas etiquetas para crear informes detallados de costos y uso en el explorador de costos de AWS para clústeres en varias dimensiones. Por ejemplo, puede realizar un seguimiento de los costos de uso a nivel de equipo, proyecto o centro de costos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Uno o más clústeres de EMR que tienen activadas las etiquetas definidas por el usuario

Arquitectura

Pila de tecnología de destino

- Amazon EMR
- Explorador de costos de AWS

Arquitectura de destino

El siguiente diagrama muestra cómo puede aplicar etiquetas para realizar un seguimiento de los costos de uso de clústeres de Amazon EMR específicos.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un ingeniero de datos o un administrador de AWS crea etiquetas de asignación de costos definidas por el usuario para los clústeres de Amazon EMR.
2. Un administrador de AWS activa las etiquetas.
3. Las etiquetas envían los metadatos al explorador de costos de AWS.

Tools (Herramientas)

Herramientas

- Amazon EMR es una plataforma de clúster administrada que simplifica la ejecución de marcos de macrodatos en AWS para procesar y analizar grandes cantidades de datos.
- El Explorador de costos de AWS permite ver y analizar los costos y el uso.

Epics

Crear y activar etiquetas para sus clústeres de Amazon EMR

Tarea	Descripción	Habilidades requeridas
Cree etiquetas de asignación de costos definidas por el usuario para los clústeres de Amazon EMR.	Para añadir etiquetas a un clúster de Amazon EMR existente Siga las instrucciones en Cómo añadir etiquetas a un clúster existente en la Guía de administración de Amazon EMR. Para añadir etiquetas a un nuevo clúster de Amazon EMR Siga las instrucciones en Cómo añadir etiquetas a un nuevo clúster en la Guía de administración de Amazon EMR. Para obtener más información sobre cómo configurar un clúster de Amazon EMR, consulte Planificar y configura	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	r clústeres en la Guía de administración de Amazon EMR.	
Active las etiquetas de asignación de costos definidas por el usuario.	Siga las instrucciones de Activación de etiquetas de asignación de costos definidas por el usuario en la Guía del usuario de facturación de AWS.	Administrador de AWS

Crear informes de costos y uso para sus clústeres de Amazon EMR

Tarea	Descripción	Habilidades requeridas
Cree informes de costo y uso para sus clústeres de Amazon EMR mediante filtros de etiquetas en al explorador de costos de AWS.	1. Inicie sesión en la consola de administración de AWS y abra la consola de administración de AWS. 2. En el panel de navegación izquierdo, elija Informes. 3. Elija Crear nuevo informe. 4. En Seleccione un tipo de informe, seleccione Costo y uso (recomendado). A continuación, elija Crear informe. 5. En Filtros, seleccione Servicio. Se muestra el menú desplegable del Servicio. 6. Seleccione las casillas de verificación situadas junto a EMR (Elastic	AWS general, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	MapReduce) y EC2-Instances (Elastic Compute Cloud — Compute). A continuación, seleccione Aplicar filtros. 7. Para los Filtros, seleccione Etiqueta. Se muestra el menú desplegable de Etiqueta. 8. Seleccione Equipo. A continuación, seleccione las casillas de verificación situadas junto a los equipos a los que haya asignado etiquetas. Excluya a los equipos a los que no haya asignado etiquetas. A continuación, seleccione Aplicar filtros. 9. En la parte superior del gráfico, seleccione Etiqueta. A continuación, seleccione las etiquetas de los clústeres de Amazon EMR para los que desee crear un informe. 10. En la parte superior del gráfico, seleccione el menú desplegable de los Últimos 3 meses y seleccione el período que desea que abarque el informe. A continuación, seleccione el menú desplegable	

Tarea	Descripción	Habilidades requeridas
	Mensual y seleccione cómo quiere que se agreguen las partidas del informe en función del período de tiempo. 11. Elija Save as (Guardar como). A continuación, introduzca un título para su informe. 12. Elija Save report. Para obtener más información, consulte Exploración de sus datos con Cost Explorer en la Guía del usuario de administración de costos de AWS.	

Más patrones

- Automatice las operaciones de AWS infraestructura con Amazon Bedrock
- Inventario automático de AWS los recursos en varias cuentas y regiones
- Automatice la creación de recursos de Amazon WorkSpaces Applications mediante AWS CloudFormation
- Archivar automáticamente los elementos en Amazon S3 con DynamoDB TTL
- Detener e iniciar automáticamente una instancia de base de datos de Amazon RDS mediante AWS Systems Manager Maintenance Windows
- Crear informes detallados de costos y uso para Amazon RDS y Amazon Aurora
- Costos de almacenamiento estimados para una tabla de Amazon DynamoDB
- Estime el costo de una tabla de DynamoDB para la capacidad bajo demanda
- Configuración del escalado automático basado en eventos en Amazon EKS mediante Amazon EKS Pod Identity y KEDA
- Coordine la dependencia de los recursos y la ejecución de tareas mediante la construcción AWS Fargate WaitCondition hook

Informática para usuarios finales

Temas

- Implemente la autenticación SAML 2.0 para Amazon WorkSpaces mediante Auth0 y AWS Managed Microsoft AD
- Más patrones

Implemente la autenticación SAML 2.0 para Amazon WorkSpaces mediante Auth0 y AWS Managed Microsoft AD

Siva Vinnakota y Shantanu Padhye, Amazon Web Services

Resumen

Este patrón explora cómo puede integrar Auth0 AWS Directory Service for Microsoft Active Directory para crear una solución de autenticación SAML 2.0 sólida para su entorno de Amazon WorkSpaces . En él se explica cómo establecer una federación entre ellos Servicios de AWS para habilitar funciones avanzadas, como la autenticación multifactor (MFA) y los flujos de inicio de sesión personalizados, a la vez que se preserva el acceso ininterrumpido al escritorio. AWS Managed Microsoft AD Ya sea que administre solo unos pocos usuarios o miles, esta integración ayuda a proporcionar flexibilidad y seguridad a su organización. Este patrón proporciona los pasos del proceso de configuración para que pueda implementar esta solución en su propio entorno.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- AWS Managed Microsoft AD
- Un escritorio aprovisionado en Amazon WorkSpaces Personal que esté asociado a AWS Managed Microsoft AD
- Una instancia de Amazon Elastic Compute Cloud (Amazon EC2)
- Una cuenta de Auth0

Limitaciones

Algunas Servicios de AWS no están disponibles en todas Regiones de AWS. Para conocer la disponibilidad de las regiones, consulte Servicios de AWS by Region. Para los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

El proceso de autenticación con SAML 2.0 para una aplicación WorkSpaces cliente consta de cinco pasos que se ilustran en el siguiente diagrama. Estos pasos representan un flujo de trabajo típico para iniciar sesión. Puede usar este enfoque distribuido de autenticación después de seguir las

instrucciones de este patrón para ayudar a proporcionar un método estructurado y seguro para el acceso de los usuarios.

Flujo de trabajo:

1. Registro. El usuario inicia la aplicación cliente WorkSpaces e introduce el código de WorkSpaces registro para su directorio compatible con SAML WorkSpaces . WorkSpaces devuelve la URL del proveedor de identidad (IdP) de Auth0 a la aplicación cliente.
2. Inicio de sesión.El WorkSpaces cliente redirige al navegador web del usuario mediante la URL Auth0. El usuario se autentica con su nombre de usuario y contraseña. Auth0 devuelve una aserción de SAML al navegador del cliente. La aserción de SAML es un token cifrado que afirma la identidad del usuario.
3. Autenticar. El navegador del cliente publica la afirmación SAML en el AWS Sign-In punto final para validarla. AWS Sign-In permite a la persona que llama asumir una función AWS Identity and Access Management (IAM). Esto devuelve un token que contiene credenciales temporales para el rol de IAM.
4. WorkSpaces iniciar sesión. El WorkSpaces cliente presenta el token al punto final del WorkSpaces servicio. WorkSpaces intercambia el token por un token de sesión y devuelve el token de sesión al WorkSpaces cliente con una URL de inicio de sesión. Cuando el WorkSpaces cliente carga la página de inicio de sesión, el valor del nombre de usuario se rellena con el `NameId` valor introducido en la respuesta de SAML.
5. Streaming. El usuario introduce su contraseña y se autentica en el WorkSpaces directorio. Tras la autenticación, WorkSpaces devuelve un token al cliente. El cliente redirige de nuevo al WorkSpaces servicio y presenta el token. Esto gestiona una sesión de streaming entre el WorkSpaces cliente y el WorkSpace.

> **Note**
>
> Para configurar una experiencia de inicio de sesión único sin necesidad de solicitar una contraseña, consulta la sección sobre autenticación basada en certificados y WorkSpaces datos personales en la documentación. WorkSpaces

Tools (Herramientas)

Servicios de AWS

- Amazon WorkSpaces es un servicio de infraestructura de escritorios virtuales (VDI) totalmente gestionado que proporciona a los usuarios escritorios basados en la nube sin tener que adquirir e implementar hardware ni instalar software complejo.
- AWS Directory Service for Microsoft Active Directorypermite que sus cargas de trabajo y AWS recursos compatibles con directorios utilicen Microsoft Active Directory en. Nube de AWS

Otras herramientas

- Auth0 es una plataforma de autenticación y autorización que lo ayuda a administrar el acceso a sus aplicaciones.

Epics

Configuración de conector LDAP de Active Directory en Auth0

Tarea	Descripción	Habilidades requeridas
Instale el conector LDAP de Active Directory en Auth0 con. AWS Managed Microsoft AD	1. Inicie sesión en el panel de Auth0 y elija Autenticación, Empresa, Active Directory / LDAP. Elija Crear una conexión. 2. Proporcione el nombre de la conexión de Active Directory y, a continuación, elija Crear. 3. En la pestaña Configura ción, descargue el agente para su sistema operativo. Cuando se complete la instalación, su navegador predeterminado mostrará una petición de la URL del ticket.	Administrador de la nube, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	4. Ingrese la URL del ticket de aprovisionamiento, que debe ser única para su cadena de conexión y, a continuación, elija Continuar. 5. En el cuadro de diálogo Configuración de LDAP de AD, en Nombre de usuario y Contraseña, ingrese sus credenciales de administrador y, a continuación, elija Guardar. Cuando se haya establecido la conexión con Auth0, se mostrará el registro de configuración con el estado de notificación Correcto para todas las comprobaciones.	

Tarea	Descripción	Habilidades requeridas
Crear una aplicación en Auth0 para generar el archivo de manifiesto de metadatos de SAML.	1. Inicie sesión en el panel de Auth0 y cree una nueva aplicación siguiendo las instrucciones de la documentación de Auth0. 2. En el panel de Auth0, elija el nombre de la aplicación para acceder a los ajustes de configuración. En la AddOnspestaña, elija SAML2 Web App. 3. En la pestaña Configuración del complemento, en Application Callback URL, introduce https://signin.aws.amazon.com/saml. Aquí es a donde el token de SAML enviará la solicitud POST. 4. En la pestaña Configuración, en el cuadro Configuración, pegue el siguiente código de configuración de SAML en formato JSON: `{ "audience": "https://signin.aws.amazon.com/saml", "mappings": { "email": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/sAMAccountName", "name": "http://schemas.xmlsoap.org/`	Administrador de la nube, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas

	<pre>ws/2005/05/identity/
	claims/name"
	  },
	  "createUpnClaim":
	 false,
	  "passthroughClaims
	WithNoMapping":
	 false,
	  "mapUnknownClaimsA
	sIs": false,
	  "mapIdentities":
	 false,
	  "nameIdentifierFor
	mat": "urn:oasi
	s:names:tc:SAML:2.
	0:nameid-format:pe
	rsistent",
	  "nameIdentifierPro
	bes": [
	  "http://s
	chemas.auth0.com/s
	AMAccountName"
	  ]
	}</pre> 5. Guarde y, a continuación, elija Habilitar.
	6. Elija la pestaña Uso y descargue el archivo de manifiesto de metadatos del proveedor de identidad es. Esta información se necesita para los siguientes pasos.
	7. Cierre la ventana de la aplicación SAML2 web.
	8. En la pantalla de aplicacio nes, elija Conexiones. En Enterprise, seleccione el	

Tarea	Descripción	Habilidades requeridas
	Directory/LDAP conector activo correcto y actívelo.	

Configuración del IdP, el rol y la política para SAML 2.0 en IAM

Tarea	Descripción	Habilidades requeridas
Crear un IdP de SAML 2.0 en IAM.	Para configurar SAML 2.0 como IdP, siga los pasos que se describen en Crear un proveedor de identidades de SAML en IAM en la documentación de IAM.	Administrador de la nube
Crear un rol de IAM y una política para la federación de SAML 2.0.	1. Cree un rol de IAM para la federación de SAML 2.0. Para obtener instrucciones, consulta el paso 2 de las instrucciones para configurar SAML 2.0 for WorkSpaces Personal de la WorkSpaces documentación. 2. Cree una política de IAM y asóciela al rol que creó en el paso anterior. Para obtener instrucciones, consulta el paso 3 de las instrucciones para configurar SAML 2.0 for WorkSpaces Personal de la WorkSpaces documentación.	Administrador de la nube

Configuración de las aserciones en Auth0

Tarea	Descripción	Habilidades requeridas
Configurar Auth0 y las aserciones de SAML.	Puede usar las acciones de Auth0 para configurar las aserciones en las respuestas de SAML 2.0. Una aserción de SAML es un token cifrado que afirma la identidad del usuario. 1. Inicie sesión en el panel de Auth0. Elija Acciones, Biblioteca, Crear acción, Crear desde cero. 2. Proporcione los valores siguientes y, a continuac ión, elija Crear. Nombre: especifique un nombre para la acción Activador: selecciona Iniciar sesión Login/Post Tiempo de ejecución: elija el nodo 18 3. En la siguiente pantalla, ingrese el siguiente código: `exports.onExecuteP ostLogin = async (event, api) => { if (event.cl ient.name === "Workspace_Saml") { const awsRole = 'arn:aws:iam::0307 84294031:role/Work`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas

	space_Auth0,arn:aws:iam::030784294031:saml-provider/Auth0';
	const awsRoleSession = event.user.sAMAccountName;
	const email = event.user.emails[0];
	api.samlResponse.setDestination('https://signin.aws.amazon.com/saml');
	api.samlResponse.setAttribute('https://aws.amazon.com/SAML/Attributes/Role', awsRole)
	api.samlResponse.setAttribute('https://aws.amazon.com/SAML/Attributes/RoleSessionName', awsRoleSession)
	api.samlResponse.setAttribute('https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email', email)
	} return;
	};
	4. Elija Implementar.
	
	Esto completa la configuración de la autenticación SAML 2.0	

Tarea	Descripción	Habilidades requeridas
	para escritorios WorkSpace s personales. En la sección Arquitectura se ilustra el proceso de autenticación tras la configuración.	

Resolución de problemas

Problema	Solución
Problemas de autenticación con SAML 2.0 en WorkSpaces	Si tienes algún problema al implementar la autenticación SAML 2.0 para WorkSpaces Personal, sigue los pasos y enlaces que se describen en el artículo de AWS Re:post sobre la solución de problemas de la autenticación SAML 2.0. Para obtener información adicional sobre cómo investigar los errores de SAML 2.0 al acceder, consulta: WorkSpaces • ¿Cómo creo un archivo HAR y los registros de la consola desde mi navegador en AWS Support caso de que se trate? (AWS Re:POST) • Ver una respuesta SAML en su navegador (documentación de IAM)

Recursos relacionados

- Configuración de SAML 2.0 para WorkSpaces uso personal (documentación) WorkSpaces
- Documentación de Auth0

Más patrones

- Automatice la creación de recursos de Amazon WorkSpaces Applications mediante AWS CloudFormation
- Mejorar la calidad de las llamadas en las estaciones de trabajo de los agentes en los centros de contacto de Amazon Connect
- Puesta en marcha de las tareas de Automatización de AWS Systems Manager de forma sincrónica desde AWS Step Functions

Computación de alto rendimiento

Temas

- Implementación de un sistema de archivos de Lustre para un procesamiento de datos de alto rendimiento mediante Terraform y DRA
- Configurar un panel de monitoreo de Grafana para AWS ParallelCluster
- Más patrones

Implementación de un sistema de archivos de Lustre para un procesamiento de datos de alto rendimiento mediante Terraform y DRA

Arun Bagal e Ishwar Chauthaiwale, Amazon Web Services

Resumen

Este patrón despliega automáticamente un sistema de archivos Lustre AWS y lo integra con Amazon Elastic Compute Cloud (Amazon EC2) y Amazon Simple Storage Service (Amazon S3).

Esta solución lo ayuda a configurar rápidamente un entorno de computación de alto rendimiento (HPC) con almacenamiento integrado, recursos de computación y acceso a los datos de Amazon S3. Combina las capacidades de almacenamiento de Lustre con las opciones informáticas flexibles que ofrece Amazon EC2 y el almacenamiento de objetos escalable de Amazon S3, para que pueda abordar cargas de trabajo con uso intensivo de datos en el aprendizaje automático, la HPC y el análisis de macrodatos.

El patrón utiliza un módulo HashiCorp Terraform y Amazon FSx for Lustre para agilizar el siguiente proceso:

- Aprovisionamiento de un sistema de archivos de Lustre
- Establecer una asociación de repositorios de datos (DRA) entre FSx for Lustre y un bucket de S3 para vincular el sistema de archivos de Lustre con los objetos de Amazon S3
- Crear una instancia EC2
- Montaje del sistema de archivos Lustre con el DRA vinculado a Amazon S3 en la instancia EC2

Las ventajas de esta solución incluyen:

- Diseño modular. Puede mantener y actualizar fácilmente los componentes individuales de esta solución.
- Escalabilidad. Puede implementar rápidamente entornos consistentes en todas Cuentas de AWS nuestras regiones.
- Flexibilidad. Puede personalizar la implementación para adaptarla a sus necesidades específicas.
- Prácticas recomendadas. Este patrón utiliza módulos preconfigurados que siguen las AWS mejores prácticas.

Para obtener más información sobre los sistemas de archivos de Lustre, consulte el sitio web de Lustre.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Una política de privilegios mínimos AWS Identity and Access Management (IAM) (consulte las instrucciones)

Limitaciones

FSx para Lustre limita el sistema de archivos de Lustre a una única zona de disponibilidad, lo que podría ser un problema si tiene requisitos de alta disponibilidad. Si la zona de disponibilidad que contiene el sistema de archivos falla, se pierde el acceso al sistema de archivos hasta la recuperación. Para lograr una alta disponibilidad, puede usar DRA para vincular el sistema de archivos de Lustre con Amazon S3 y transferir datos entre zonas de disponibilidad.

Versiones de producto

- Terraform, versión 1.9.3 o posterior
- HashiCorp AWS Provider versión 4.0.0 o posterior

Arquitectura

En el siguiente diagrama se muestra la arquitectura FSx de Lustre y la complementaria Servicios de AWS de. Nube de AWS

La arquitectura incluye lo siguiente:

- Un bucket de S3 se utiliza como una ubicación de almacenamiento de datos duradera, escalable y rentable. La integración entre FSx for Lustre y Amazon S3 proporciona un sistema de archivos de alto rendimiento que se vincula perfectamente con Amazon S3.
- FSx for Lustre ejecuta y administra el sistema de archivos Lustre.

- Amazon CloudWatch Logs recopila y supervisa los datos de registro del sistema de archivos. Estos registros proporcionan información sobre el rendimiento, el estado y la actividad de su sistema de archivos de Lustre.
- Amazon EC2 se utiliza para acceder a los sistemas de archivos de Lustre mediante el cliente Lustre de código abierto. EC2 las instancias pueden acceder a los sistemas de archivos desde otras zonas de disponibilidad dentro de la misma nube privada virtual (VPC). La configuración de la red permite el acceso a través de subredes dentro de la VPC. Una vez montado el sistema de archivos de Lustre en la instancia, puede trabajar con los archivos y directorios como haría con cualquier sistema de archivos local.
- AWS Key Management Service (AWS KMS) mejora la seguridad del sistema de archivos al proporcionar cifrado para los datos en reposo.

Automatización y escala

Terraform facilita la implementación, administración y escalado de sus sistemas de archivos de Lustre en múltiples entornos. En el FSx caso de Lustre, un único sistema de archivos tiene limitaciones de tamaño, por lo que es posible que necesite escalar horizontalmente creando varios sistemas de archivos. Puede usar Terraform para aprovisionar varios sistemas de archivos de Lustre en función de sus necesidades de carga de trabajo.

Tools (Herramientas)

Servicios de AWS

- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas y aplicaciones Servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática escalable en el Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon FSx for Lustre hace que sea fácil y rentable lanzar, ejecutar y escalar un sistema de archivos Lustre de alto rendimiento.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Repositorio de código

El código de este patrón está disponible en el sistema de archivos GitHub Provision FSx for Lustre, que utiliza el repositorio Terraform.

Prácticas recomendadas

- Las variables siguientes definen el sistema de archivos de Lustre. Asegúrese de configurarlas correctamente en función de su entorno, tal y como se indica en la sección Epics.
  - `storage_capacity`— La capacidad de almacenamiento del sistema de archivos Lustre, en. GiBs La configuración mínima y predeterminada es 1200 GiB.
  - `deployment_type`: el tipo de implementación del sistema de archivos de Lustre. Para obtener una explicación de las dos opciones, `PERSISTENT_1` y `PERSISTENT_2` (por defecto), consulte la documentación FSx de Lustre.
  - `per_unit_storage_throughput`— El rendimiento de lectura y escritura, en tiB MBs por segundo.
  - `subnet_id`— El ID de la subred privada en la que desea realizar el despliegue FSx para Lustre.
  - `vpc_id`— El ID de su nube privada virtual en la AWS que desea realizar la implementación FSx de Lustre.
  - `data_repository_path`: la ruta al bucket de S3 que se vinculará al sistema de archivos de Lustre.
  - `iam_instance_profile`— El perfil de la instancia de IAM que se utilizará para lanzar la EC2 instancia.
  - `kms_key_id`— El nombre del recurso de Amazon (ARN) de la AWS KMS clave que se utilizará para el cifrado de datos.
- Garantice el acceso y la ubicación adecuados a la red dentro de la VPC mediante las variables `security_group` y `vpc_id`.
- Ejecute el comando `terraform plan` tal y como se describe en la sección Epics para obtener una vista previa de los cambios y verificarlos antes de aplicarlos. Esto ayuda a atrapar posibles problemas y garantiza que esté al tanto de lo que se implementará.
- Utilice el comando `terraform validate` tal y como se describe en la sección Epics para comprobar si hay errores de sintaxis y confirmar que la configuración es correcta.

Epics

Configure su entorno

Tarea	Descripción	Habilidades requeridas
Instale Terraform.	Para instalar Terraform en su máquina local, siga las instrucciones de la documentación de Terraform.	AWS DevOps, DevOps ingeniero
Configure AWS las credenciales.	Para configurar el perfil AWS Command Line Interface (AWS CLI) de la cuenta, sigue las instrucciones de la AWS documentación.	AWS DevOps, DevOps ingeniero
Clona el GitHub repositorio.	Para clonar el GitHub repositorio, ejecute el comando: `git clone https://github.com/aws-samples/provision-fsx-lustre-with-terraform.git`	AWS DevOps, DevOps ingeniero

Configure e implemente FSx para Lustre

Tarea	Descripción	Habilidades requeridas
Actualice la configuración de implementación.	1. En el repositorio clonado de su máquina local, navegue hasta el directorio `fsx_deployment` : `cd fsx_deployment`	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	2. Abra el archivo `terraform.tfvars` y actualice los valores de las variables siguientes: • `vpc_id` • `subnet_id` • `data_repository_path` • `iam_instance_profile` • `kms_key_id` Para obtener descripciones de estas variables, consulte la sección de prácticas recomendadas. 3. En el mismo directorio, abra el archivo `locals.tf` y actualice los rangos de CIDR para las variables `fsx_inress` y `fsx_egress` del grupo de seguridad. 4. Si es necesario, abra el archivo `variables.tf` y actualice los valores predeterminados de estas variables: • `storage_capacity` • `deployment_type` • `per_unit_storage_throughput`	

Tarea	Descripción	Habilidades requeridas
	Para obtener descripciones de estas variables, consulte la sección de prácticas recomendadas.	
Inicialice el entorno de Terraform.	Para inicializar su entorno para ejecutar el módulo `fsx_deployment` de Terraform, ejecute: `terraform init`	AWS DevOps, DevOps ingeniero
Valide la sintaxis de Terraform .	Para comprobar si hay errores de sintaxis y confirmar que la configuración es correcta, ejecute: `terraform validate`	AWS DevOps, DevOps ingeniero
Valide la configuración de Terraform.	Para crear un plan de ejecución de Terraform y obtener una vista previa de la implementación, ejecute: `terraform plan -var-file terraform.tfvars`	AWS DevOps, DevOps ingeniero
Implemente el módulo de Terraform.	Para implementar los recursos FSx de for Lustre, ejecute: `terraform apply -var-file terraform.tfvars`	AWS DevOps, DevOps ingeniero

Limpie AWS los recursos

Tarea	Descripción	Habilidades requeridas

Eliminar AWS recursos.	Cuando termines de usar tu entorno de FSx For Lustre, podrás eliminar los AWS recursos desplegados por Terraform para evitar incurrir en cargos innecesarios. El módulo de Terraform incluido en el repositorio de código automatiza esta limpieza.
	1. En el repositorio local, navegue hasta el directorio `fsx_deployment` :
	`cd fsx_deployment`
	2. Ejecute el comando:
	`terraform destroy -var-file terraform.tfvars`
		AWS DevOps, DevOps ingeniero

Resolución de problemas

Problema	Solución
FSx for Lustre devuelve errores.	Para obtener ayuda con FSx los problemas de Lustre, consulte Solución de problemas de Amazon FSx for Lustre en la documentación de FSx for Lustre.

Recursos relacionados

- Creación de Amazon FSx for Lustre mediante Terraform (referencia del AWS proveedor en la documentación de Terraform)
- Introducción a Amazon FSx for Lustre (FSx para ver la documentación de Lustre)
- AWS entradas de blog sobre Amazon FSx for Lustre

Configurar un panel de monitoreo de Grafana para AWS ParallelCluster

Dario La Porta y William Lu, Amazon Web Services

Resumen

AWS le ParallelCluster ayuda a implementar y administrar clústeres de computación de alto rendimiento (HPC). Es compatible con los programadores de trabajos de código abierto AWS Batch y Slurm. Aunque AWS ParallelCluster está integrado con Amazon CloudWatch para el registro y las métricas, no proporciona un panel de supervisión de la carga de trabajo.

El panel de control de Grafana para AWS ParallelCluster (GitHub) es un panel de supervisión para AWS. ParallelCluster Proporciona información sobre el programador de tareas y métricas de supervisión detalladas a nivel del sistema operativo (SO). Para obtener más información sobre los paneles incluidos en esta solución, consulte Ejemplos de paneles en el repositorio. GitHub Estas métricas le ayudan a comprender mejor la carga de trabajo de HPC y su rendimiento. Sin embargo, el código del panel de control no se actualiza para las versiones más recientes de AWS ParallelCluster ni para los paquetes de código abierto que se utilizan en la solución. Este patrón mejora la solución para proporcionar los siguientes beneficios:

- Compatible con AWS ParallelCluster v3
- Usa la última versión de los paquetes de código abierto, incluidos Prometheus, Grafana, Prometheus Slurm Exporter y NVIDIA DCGM-Exporter
- Aumenta la cantidad de núcleos de CPU GPUs que utilizan los trabajos de Slurm
- Añade un panel de supervisión de trabajos
- Mejora el panel de monitoreo de nodos de la GPU para nodos con 4 u 8 unidades de procesamiento gráfico () GPUs

Esta versión de la solución mejorada se ha implementado y verificado en el entorno de producción de HPC de un cliente de AWS.

Requisitos previos y limitaciones

Requisitos previos

- AWS ParallelCluster CLI, instalada y configurada.

- Una configuración de red compatible con AWS ParallelCluster. Este patrón usa la configuración de AWS ParallelCluster con dos subredes, que requiere una subred pública, una subred privada, una puerta de enlace a Internet y una puerta de enlace NAT.
- Todos los nodos ParallelCluster del clúster de AWS deben tener acceso a Internet. Esto es necesario para que los scripts de instalación puedan descargar el software de código abierto y las imágenes de Docker.
- Un key pair en Amazon Elastic Compute Cloud (Amazon EC2). Los recursos con este par de claves tienen acceso Secure Shell (SSH) al nodo principal.

Limitaciones

- Este patrón está diseñado para Ubuntu 20.04 LTS. Si usa una versión diferente de Ubuntu, o si usa Amazon Linux o CentOS, tendrá que modificar los scripts que se proporcionan con esta solución. Dichas modificaciones no se incluyen en este patrón.

Versiones de producto

- Ubuntu 20.04 LTS
- ParallelCluster 3.X

Consideraciones de costos y facturación

- La solución implementada en este patrón no está cubierta por el nivel gratuito. Se aplican cargos a Amazon EC2, Amazon FSx for Lustre, la puerta de enlace NAT en Amazon VPC y Amazon Route 53.

Arquitectura

Arquitectura de destino

En el siguiente diagrama, se muestra cómo un usuario puede acceder al panel de supervisión de AWS ParallelCluster en el nodo principal. El nodo principal ejecuta NICE DCV, Prometheus, Grafana, Prometheus Slurm Exporter, Prometheus Node Exporter y NGINX Open Source. Los nodos de cómputo ejecutan Prometheus Node Exporter y también ejecutan NVIDIA DCGM-Exporter si el nodo lo contiene. GPUs El nodo principal recupera información de los nodos de cómputo y muestra esos datos en el panel de control de Grafana.

En la mayoría de los casos, el nodo principal no está muy cargado, ya que el programador de tareas no requiere una cantidad significativa de CPU o memoria. Los usuarios acceden al panel de control del nodo principal mediante SSL en el puerto 443.

Todos los usuarios con acceso de lectura autorizado pueden ver los paneles de supervisión de forma anónima. Solo el administrador de Grafana puede modificar los paneles. Debe configurar una contraseña para el administrador de Grafana en el archivo `aws-parallelcluster-monitoring/docker-compose/docker-compose.head.yml`.

Tools (Herramientas)

Servicios de AWS

- NICE DCV es un protocolo de visualización remota de alto rendimiento que le permite ofrecer escritorios remotos y streaming de aplicaciones desde cualquier nube o centro de datos a cualquier dispositivo, en condiciones de red variables.
- AWS le ParallelCluster ayuda a implementar y administrar clústeres de computación de alto rendimiento (HPC). Es compatible con los programadores de trabajos de código abierto AWS Batch y Slurm.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido.

Otras herramientas

- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización a nivel del sistema operativo para entregar software en contenedores.
- Grafana es un software de código abierto que le permite consultar, visualizar, alertar y explorar métricas, registros y trazas.
- NGINX Open Source es un servidor web de código abierto y proxy inverso.
- NVIDIA Data Center GPU Manager (DCGM) es un conjunto de herramientas para administrar y monitorear las unidades de procesamiento gráfico (GPUs) de los centros de datos de NVIDIA en entornos de clústeres. Este patrón usa DCGM-Exporter, que le ayuda a exportar las métricas de GPU de Prometheus.

- Prometheus es un conjunto de herramientas de supervisión de sistemas de código abierto que recopila y almacena sus métricas como datos de serie temporal con pares clave-valor asociados, denominados etiquetas. Este patrón también usa Prometheus Slurm Exporter para recopilar y exportar métricas, y Prometheus Node Exporter para exportar métricas de los nodos de cómputo.
- Ubuntu es un sistema operativo de código abierto basado en Linux y diseñado para servidores empresariales, escritorios, entornos de nube e IoT.

Repositorio de código

El código de este patrón está disponible en el GitHub pcluster-monitoring-dashboardrepositorio.

Epics

Cree los recursos necesarios

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Crear un bucket de Amazon S3. Este bucket se usa para almacenar los scripts de configuración. Para obtener instrucciones, consulte Crear un bucket en la documentación de Amazon S3.	AWS general
Clonar el repositorio.	Clona el GitHub pcluster-monitoring-dashboardrepositorio ejecutando el siguiente comando. `git clone https://github.com/aws-samples/parallelcluster-monitoring-dashboard.git`	DevOps ingeniero
Cree una contraseña de administrador.	1. Seleccione la carpeta `aws-parallelcluster-`	Scripts Linux Shell

Tarea	Descripción	Habilidades requeridas
	`monitoring` , seleccione la carpeta `docker-compose` y abra el archivo docker-compose.head.yml. 2. En la variable `GF_SECURITY_ADMIN_PASSWORD` , sustituya `Grafana4PC!` por una contraseña de su elección. Esta es la contraseña administrativa que usará para gestionar la cuenta de Grafana. 3. Guarde y cierre el archivo docker-compose.head.yml.	
Copie los archivos necesarios en el bucket de S3.	Copie el script post_install.sh y la aws-parallelcluster-monitoringcarpeta en el depósito de S3 que creó. Para más instrucciones, consulte Cargar objetos en la documentación de Amazon S3.	AWS general

Tarea	Descripción	Habilidades requeridas
Configure un grupo de seguridad adicional para el nodo principal.	1. Cree un grupo de seguridad para el nodo principal. Este grupo de seguridad permitirá que el tráfico entrante llegue a los paneles de supervisión del nodo principal. Para más instrucciones, consulte Crear un grupo de seguridad en la documentación de Amazon VPC. 2. Agregar una regla de entrada al grupo de seguridad Para obtener más instrucciones, consulte Cómo añadir reglas a un grupo de seguridad en la documentación de Amazon VPC. Utilice los siguientes parámetros para la regla: • Tipo: HTTPS • Protocolo: TCP • Intervalo de puertos: 443 • Origen: introduzca su dirección IP • Descripción: permitir a los usuarios acceder al panel de supervisión	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure una política de IAM para el nodo principal.	Cree una política basada en identidades para el nodo principal. Esta política permite al nodo recuperar datos métricos de Amazon CloudWatch. El GitHub repositorio contiene un ejemplo de política. Para obtener más instrucciones, consulte Creación de políticas de IAM en la documentación de AWS Identity and Access Management (IAM).	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure una política de IAM para los nodos de cómputo.	Cree una política basada en identidades para los nodos de computación. Esta política permite al nodo crear las etiquetas que contienen la ID y el propietario del trabajo. El GitHub repositorio contiene un ejemplo de política. Para obtener más información, consulte Creación de políticas de IAM en la documentación de IAM. Si usa el archivo de ejemplo proporcionado, sustituya los siguientes valores: • <REGION>: la región de AWS donde se aloja el clúster. • <ACCOUNT_ID>: ID de la cuenta de AWS.	Administrador de AWS

Cree el clúster

Tarea	Descripción	Habilidades requeridas
Modifique el archivo de plantilla de clúster proporcio nado.	Cree el ParallelCluster clúster de AWS. Utilice el archivo de plantilla de CloudFormation AWS cluster.yaml proporcio nado como punto de partida para crear el clúster. Sustituya	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	los siguientes valores en la plantilla proporcionada: • <REGION>: la región de AWS donde se aloja el clúster. • <HEADNODE_SUBNET> – La subred pública de la VPC. • <ADDITIONAL_HEAD_NODE_SG> – El nombre del grupo de seguridad que ha creado para el nodo principal. • <KEY_NAME>— Introduce el nombre de un par de EC2 claves de Amazon existente. Los recursos con este par de claves tienen acceso Secure Shell (SSH) al nodo principal. • <ALLOWED_IPS> -– Introduzca el rango de direcciones IP con formato CIDR que puede realizar conexiones SSH en el nodo principal. • <ADDITIONAL_HEAD_NODE_POLICY> – Introduzca el nombre de la política de IAM que ha creado para el nodo principal.	

Tarea	Descripción	Habilidades requeridas
	• <BUCKET_NAME>: escriba el nombre del bucket de S3·que creó. • <COMPUTE_SUBNET> – Introduzca el nombre de la subred privada en la VPC. • <ADDITIONAL_HEAD_NODE_POLICY> – Introduzca el nombre de la política de IAM que ha creado para el nodo de computación.	
Cree el clúster.	En la AWS ParallelCluster CLI, introduzca el siguiente comando. Esto despliega la CloudFormation plantilla y crea el clúster. Para obtener más información sobre este comando, consulte pcluster create-cluster en la documentación de AWS. ParallelCluster `pcluster create-cluster -n <cluster_name> -c cluster.yaml`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Supervise la creación del clúster.	Introduzca el siguiente comando para supervisar la creación del cluster. Para obtener más información sobre este comando, consulte pcluster describe-cluster en la documentación de AWS. ParallelCluster `pcluster describe-cluster -n <cluster_name>`	Administrador de AWS

Use los paneles de Grafana

Tarea	Descripción	Habilidades requeridas
Acceda al portal de Grafana.	1. Introduzca el siguiente comando para obtener la dirección IP pública del nodo principal. `pcluster describe-cluster -n <cluster_name> --query headNode.publicIpAddress` 2. En un navegador web, acceda a la siguiente URL para entrar en el panel de control de Grafana. https://<head_node_public_ip_address>	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	3. En la página de inicio de Grafana, elija el icono de cuatro cuadrados Panel de control, en el menú de la izquierda, y seleccione General. Se mostrará una lista de paneles configura dos. Grafana ofrece los siguientes paneles: • Costo del clúster: contiene información sobre el costo del clúster • Registros del clúster: contiene información sobre los registros del clúster • Detalles del nodo de cómputo: contiene información sobre las estadísticas de uso de los nodos de cómputo • Lista de nodos de cómputo: contiene una lista de los nodos de cómputo del clúster • Nodos de GPU: contiene información sobre las estadísticas de uso de los nodos de GPU • Detalles de los trabajos: contiene información sobre la utilización de los recursos del trabajo	

Tarea	Descripción	Habilidades requeridas
	• Detalles del nodo principal: contiene información sobre las estadísticas de uso del nodo principal • ParallelCluster Resumen: contiene información sobre el uso del clúster	

Limpie la solución para dejar de incurrir en costos asociados

Tarea	Descripción	Habilidades requeridas
Elimine el clúster.	Para eliminar el clúster, escriba siguiente comando. Para obtener más información sobre este comando, consulte pcluster delete-cluster en la documentación de AWS. ParallelCluster `pcluster delete-cluster -n <cluster_name>`	Administrador de AWS
Elimine las políticas de IAM.	Elimine las políticas que creó para el nodo principal y el nodo de cómputo. Para más información acerca de la eliminación de políticas , consulte Eliminación de políticas de IAM en la documentación de IAM.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Eliminar la regla y el grupo de seguridad.	Elimine el grupo de seguridad que creó para el nodo principal. Para obtener más información, consulte Eliminar reglas de grupo de seguridad y Eliminar un grupo de seguridad en la documentación de Amazon VPC.	Administrador de AWS
Elimine el bucket de S3.	Elimine el bucket de S3 que creó para almacenar los scripts de configuración. Para obtener más información, consulte Eliminación de un bucket en la documentación de Amazon S3.	AWS general

Resolución de problemas

Problema	Solución
No se puede acceder al nodo principal en el navegador.	Compruebe el grupo de seguridad y confirme que el puerto de entrada 443 esté abierto.
Grafana no se abre.	En el nodo principal, busque `docker logs Grafana` en el registro del contenedor.
Algunas métricas no tienen datos.	En el nodo principal, compruebe los registros de todos los contenedores.

Recursos relacionados

Documentación de AWS

- Políticas de IAM para Amazon EC2

Otros recursos de AWS

- AWS ParallelCluster
- Panel de monitoreo para AWS ParallelCluster (entrada del blog de AWS)

Otros recursos

- Sistema de monitorización Prometheus
- Grafana

Más patrones

- Implementación de diagnósticos y solución de problemas de Kubernetes con tecnología de IA con la integración de K8sGPT y Amazon Bedrock

Nube híbrida

Temas

- Configure una CI/CD canalización para cargas de trabajo híbridas en Amazon ECS Anywhere mediante AWS CDK y GitLab
- Más patrones

Configure una CI/CD canalización para cargas de trabajo híbridas en Amazon ECS Anywhere mediante AWS CDK y GitLab

Rafael Ortiz, Amazon Web Services

Resumen

Amazon ECS Anywhere es una extensión de Amazon Elastic Container Service (Amazon ECS). Permite registrar una instancia externa, como un servidor en las instalaciones o una máquina virtual (VM), en su clúster de Amazon ECS. Esta característica ayuda a reducir los costos y mitigar la compleja operativa y orquestación de los contenedores locales. Puede usar ECS Anywhere para implementar y ejecutar aplicaciones de contenedor tanto en entornos en las instalaciones como en la nube. Evita que su equipo tenga que aprender varios dominios y conjuntos de habilidades, o administrar software complejo por su cuenta.

Este patrón describe un step-by-step enfoque para aprovisionar un clúster de Amazon ECS con instancias de Amazon ECS Anywhere mediante pilas del Cloud Development Kit (AWS CDK) de Amazon Web Services (AWS). A continuación, utiliza AWS CodePipeline para configurar una canalización de integración e implementación continuas (CI/CD). A continuación, replica el repositorio de GitLab código en AWS CodeCommit e implementa la aplicación en contenedores en el clúster de Amazon ECS.

Este patrón está diseñado para ayudar a quienes utilizan la infraestructura local a ejecutar aplicaciones de contenedores y GitLab a administrar la base de código de la aplicación. Puede administrar esas cargas de trabajo con los servicios en la nube de AWS sin interrumpir su infraestructura existente en las instalaciones.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una aplicación en contenedor ejecutada en una infraestructura en las instalaciones.
- Un GitLab repositorio en el que puede administrar la base de código de su aplicación. Para obtener más información, consulte Repository (GitLab).
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada. Para obtener más información, consulte Instalar o actualizar la última versión de la CLI de AWS (documentación de la CLI de AWS).

- Kit de herramientas de AWS CDK, instalado y configurado globalmente. Para más información, consulte Instalar el CDK de AWS (documentación sobre el CDK de AWS).
- npm, instalado y configurado para la AWS CDK en. TypeScript Para obtener más información, consulte Descargar e instalar Node.js y npm (documentación de npm).

Limitaciones

- Para ver las limitaciones y consideraciones, consulte Instancias externas (Amazon ECS Anywhere) en la documentación de Amazon ECS.

Versiones de producto

- Kit de herramientas de AWS CDK, versión 2.27.0 o posterior
- npm versión 7.20.3 o posterior
- Node.js versión 16.6.1 o posterior

Arquitectura

Pila de tecnología de destino

- AWS CDK
- AWS CloudFormation
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- Amazon ECS Anywhere
- Amazon Elastic Container Registry (Amazon ECR)
- AWS Identity y Access Management (IAM)
- AWS Systems Manager
- GitLab repositorio

Arquitectura de destino

Este diagrama representa dos flujos de trabajo principales descritos en este patrón: el aprovisionamiento del clúster de Amazon ECS y la configuración de la CI/CD canalización que configura e implementa la CI/CD canalización, de la siguiente manera:

1. Aprovisionamiento del clúster de Amazon ECS
    a. Al implementar la primera pila de CDK de AWS, se crea una CloudFormation pila en AWS.
    b. Esta CloudFormation pila aprovisiona un clúster de Amazon ECS y los recursos de AWS relacionados.
    c. Para registrar una instancia externa en un clúster de Amazon ECS, debe instalar AWS Systems Manager Agent (SSM Agent) en su máquina virtual y registrar la máquina virtual como instancia gestionada por AWS Systems Manager.
    d. También debe instalar el agente de contenedores de Amazon ECS y Docker en su máquina virtual para registrarla como instancia externa en el clúster de Amazon ECS.
    e. Cuando la instancia externa está ya registrada y configurada con el clúster de Amazon ECS, puede ejecutar varios contenedores en su máquina virtual, registrada como instancia externa.
    f. El clúster de Amazon ECS está activo y puede ejecutar las cargas de trabajo de la aplicación a través de contenedores. La instancia de contenedor de Amazon ECS Anywhere se ejecuta en un entorno en las instalaciones, pero está asociada al clúster de Amazon ECS en la nube.
2. Configuración e implementación de la CI/CD canalización
    a. Al implementar la segunda pila de CDK de AWS, se crea otra CloudFormation pila en AWS.
    b. Esta CloudFormation pila proporciona una canalización CodePipeline y los recursos de AWS relacionados.
    c. Los cambios en el código de la aplicación se insertan y se combinan en un GitLab repositorio local.
    d. El GitLab repositorio se replica automáticamente en el CodeCommit repositorio.
    e. Las actualizaciones del CodeCommit repositorio se inician automáticamente. CodePipeline
    f. CodePipeline copia el código de la aplicación desplegable integrada CodeCommit y la crea. CodeBuild
    g. CodePipeline crea una imagen de Docker del entorno de CodeBuild compilación y la envía al repositorio de Amazon ECR.
    h. CodePipeline inicia CodeDeploy acciones que extraen la imagen del contenedor del repositorio de Amazon ECR.
    i. CodePipeline implementa la imagen del contenedor en el clúster de Amazon ECS.

Automatización y escala

Este patrón emplea AWS CDK como herramienta de infraestructura como código (IaC) para configurar e implementar esta arquitectura. AWS CDK le ayuda a organizar los recursos de AWS y a configurar Amazon ECS Anywhere y la CI/CD canalización.

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura en la nube de AWS en código.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS le CodePipeline ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores escalable y rápido que ayuda a ejecutar, detener y administrar contenedores en un clúster. Este patrón también emplea Amazon ECS Anywhere, que permite registrar un servidor en las instalaciones o una máquina virtual en el clúster de Amazon ECS.

Otras herramientas

- Node.js es un entorno de JavaScript ejecución basado en eventos diseñado para crear aplicaciones de red escalables.
- npm es un registro de software que se ejecuta en un entorno Node.js y se utiliza para compartir o tomar prestados paquetes y administrar la implementación de paquetes privados.
- Vagrant es una utilidad de código abierto para compilar y mantener entornos de desarrollo de software virtual portátiles. Este patrón usa Vagrant con fines de demostración para crear una máquina virtual en las instalaciones.

Repositorio de código

El código de este patrón está disponible en la canalización de GitHub CI/CD de Amazon ECS Anywhere mediante el repositorio CDK de AWS.

Prácticas recomendadas

Tenga en cuenta las siguientes prácticas recomendadas al implementar este patrón:

- Prácticas recomendadas para desarrollar e implementar una infraestructura de nube con AWS CDK
- Prácticas recomendadas para desarrollar aplicaciones en la nube con AWS CDK (publicación del blog de AWS)

Epics

Verificar la configuración de AWS CDK

Tarea	Descripción	Habilidades requeridas
Verifique la versión de AWS CDK.	Compruebe la versión del kit de herramientas de AWS CDK ejecutando el siguiente comando. `cdk --version` Este patrón requiere la versión 2.27.0 o posterior. Si tiene una versión anterior, siga las instrucciones de la documentación de AWS CDK para actualizarla.	DevOps ingeniero
Verifique la versión de npm.	Verifique la versión de npm introduciendo el siguiente comando.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`npm --version` Este patrón requiere la versión 7.20.3 o posterior. Si tiene una versión anterior, siga las instrucciones de la documentación de npm para actualizarla.	

Configure las credenciales de AWS.	Para configurar las credenciales de AWS, ejecute el comando `aws configure` y siga las instrucciones.
	
	`$aws configure`
	`AWS Access Key ID`
	`[None]: <your-access-key-ID>`
	`AWS Secret Access Key`
	`[None]: <your-secret-access-key>`
	`Default region name`
	`[None]: <your-Region-name>`
	`Default output format`
	`[None]:`
		DevOps ingeniero

Inicie el entorno de AWS CDK

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio de código de AWS CDK.	1. Clone el repositorio Proceso de CI/CD para Amazon ECS Anywhere mediante AWS CDK para usarlo en este patrón	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	ejecutando el siguiente comando.
	
	`git clone https://github.com/aws-samples/amazon-ecs-anywhere-cicd-pipeline-cdk-sample.git`
	
	2. Acceda al directorio clonado ejecutando el siguiente comando.
	
	`cd amazon-ecs-anywhere-cicd-pipeline-cdk-sample`	

Arranque el entorno de .	Implemente la CloudFormation plantilla en la cuenta y la región de AWS que desee utilizar introduciendo el siguiente comando. `cdk bootstrap <account-number>/<Region>` Para obtener más información, consulte Proceso de arranque en la documentación de AWS CDK.	DevOps ingeniero

Creación e implementación de la infraestructura para Amazon ECS Anywhere

Tarea	Descripción	Habilidades requeridas

Instale las dependencias del paquete y compile los TypeScript archivos.	Instale las dependenc ias del paquete y compile los TypeScript archivos introduciendo los siguientes comandos.
	`$cd EcsAnywhereCdk`
	`$npm install`
	`$npm fund`
	Estos comandos instalan todos los paquetes del repositorio de muestra. Para obtener más información, consulte npm ci y npm install en la documentación de npm. Si recibe algún error relacionado con la falta de paquetes al ejecutar estos comandos, consulte la sección de Solución de problemas de este patrón.
		DevOps ingeniero

Compilar el proyecto.	Para construir el código del proyecto, introduzca el siguiente comando. `npm run build` Para obtener más informaci ón sobre la compilaci ón e implementación del proyecto, consulte Su primera	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	aplicación de AWS CDK en la documentación de AWS CDK.	

Implemente la pila de infraestructura de Amazon ECS Anywhere.	1. Haga una lista de las pilas introduciendo el siguiente comando.
	`$cdk list`
	2. Confirme que el resultado devuelve las pilas `EcsAnywhereInfraStack` y `ECSAnywherePipelineStack` .
	3. Implementar la pila de `EcsAnywhereInfraStack` introduciendo el siguiente comando.
	`$cdk deploy EcsAnywhereInfraStack`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Verifique la creación y el resultado de la pila.	1. Inicie sesión en la consola de administración de AWS y abra la CloudFormation consola en https://console.aws.amazon.com/cloudformation/. 2. En la página Pilas, seleccione la pila `EcsAnywhereInfraStack` . 3. Confirme que el estado de la pila es `CREATE_IN_PROGRESS` o `CREATE_COMPLETE` . La configuración del clúster de Amazon ECS puede llevar algún tiempo. No proceda hasta que se haya completado la creación de la pila.	DevOps ingeniero

Configure una máquina virtual en las instalaciones

Tarea	Descripción	Habilidades requeridas
Configurar su VM.	Cree una máquina virtual de Vagrant ejecutando el comando `vagrant up` desde el directorio raíz donde se encuentra Vagrantfile. Para obtener más información,	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	consulte la documentación de Vagrant.	

Tarea	Descripción	Habilidades requeridas

Registre su máquina virtual como instancia externa.	1. Inicie sesión en la máquina virtual de Vagrant ejecutando el comando `vagrant ssh`. Para obtener más información, consulte la documentación de Vagrant.
	2. Instale la CLI de AWS en la máquina virtual siguiendo las instrucciones de instalación de la CLI de AWS y ejecute los siguientes comandos.
	`$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" \`
	`> -o "awscliv2.zip"`
	`$sudo apt install unzip`
	`$unzip awscliv2.zip`
	`$sudo ./aws/install`
	`$aws configure`
	`AWS Access Key ID [None]: <your-access-key-ID>`
	`AWS Secret Access Key [None]: <your-secret-access-key>`
	`Default region name [None]: <your-Region-name>`
	`Default output format [None]:`
	1. Cree un código de activación y una ID que usará para
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	registrar su máquina virtual en AWS Systems Manager y activar su instancia externa. El resultado de este comando incluye los valores de ID de activación y código de activación.
	
	`aws ssm create-activation \ > --iam-role EcsAnywhereInstanceRole \ > | tee ssm-activation.json`
	
	Si recibe un error al ejecutar este comando, consulte la sección Solución de problemas.
	2. Exporte los valores de ID de activación y código.
	
	`export ACTIVATION_ID=<activation-ID> export ACTIVATION_CODE=<activation-code>`
	
	3. Descargue el script de instalación en su máquina virtual.
	
	`curl --proto "https" -o "ecs-anywhere-install.sh" \`	

Tarea	Descripción	Habilidades requeridas

	`> "https://amazon-ecs-agent.s3.amazonaws.com/ecs-anywhere-install-latest.sh"`
	4. Ejecute el script de instalación en su VM.
	`sudo bash ecs-anywhere-install.sh \ --cluster EcsAnywhereCluster \ --activation-id $ACTIVATION_ID \ --activation-code $ACTIVATION_CODE \ --region <region-name>`
	Este paso configura la máquina virtual como una instancia externa de Amazon ECS Anywhere, y registra la instancia en el clúster de Amazon ECS. Para obtener más información, consulte Registrar una instancia externa en un clúster en la documentación de Amazon ECS. Si tiene algún problema, consulte la sección Solución de problemas.	

Tarea	Descripción	Habilidades requeridas

Compruebe el estado de Amazon ECS Anywhere y de la máquina virtual externa.	Para comprobar si su máquina virtual está conectada al plano de control de Amazon ECS y en funcionamiento, ejecute los siguientes comandos.
	`$aws ssm describe-instance-information`
	`$aws ecs list-container-instances --cluster $CLUSTER_NAME`
		DevOps ingeniero

Despliegue la CI/CD canalización

Tarea	Descripción	Habilidades requeridas
Crea una rama en el CodeCommit repositorio.	Crea una rama con un nombre `main` en el CodeCommit repositorio creando la primera confirmación para el repositorio. Puede seguir la documentación de AWS para crear una confirmación CodeCommit. El siguiente comando es un ejemplo. `aws codecommit put-file \ --repository-name EcsAnywhereRepo \ --branch-name main \ --file-path README.md \ --file-content "Test" \ --name "Dev Ops" \`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`--email "devops@example.com" \ --commit-message "Adding README."`	
Configure la replicación de repositorios.	Puede duplicar un GitLab repositorio desde y hacia fuentes externas. Puede seleccionar qué repositorio servirá como origen. Las ramificaciones, las etiquetas y las confirmaciones se sincronizan automáticamente. Configura una réplica automática entre el GitLab repositorio que aloja tu aplicación y el CodeCommit repositorio. Para obtener instrucciones, consulte Configurar una réplica push de GitLab a CodeCommit (GitLab documentación). **Note** De manera predeterminada, la replicación sincroniza automáticamente el repositorio. Si desea actualizar manualmente los repositorios, consulte Actualizar una réplica (GitLab documentación).	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Despliegue la pila de CI/CD canalizaciones.	Implementar la pila de `EcsAnywherePipelineStack` introduciendo el siguiente comando. `$cdk deploy EcsAnywherePipelineStack`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Pruebe la CI/CD tubería.	1. Realiza cambios en el código de la aplicación y envíalo al GitLab repositorio local de origen. Por ejemplo, edite el archivo `../application/index.html` para actualizar el valor de versión de la aplicación. 2. Cuando el código se replica en el CodeCommit repositorio, se inicia la canalización. CI/CD Realice una de las siguientes acciones: • Si utilizas la duplicación automática para sincronizar el repositorio con el GitLab repositorio, continúa con el siguiente CodeCommit paso. • Si utiliza la duplicación manual, inserte los cambios en el código de la aplicación en el CodeCommit repositorio siguiendo las instrucciones de Actualizar una réplica (documentación). GitLab 3. En su máquina local, abra un navegador web y acceda a http://localhost:80. Se abrirá la página web de NGINX, ya que el puerto	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	80 se reenvía a localhost en Vagrantfile. Confirme que puede ver el valor de la versión actualizada de la aplicación. Este paso valida la implementación del proceso y la imagen. 4. (Opcional) Si desea verificar la implementación en la consola de administración de AWS, haga lo siguiente: a. Abra la consola de Amazon ECS en https://console.aws.amazon.com/ecs/. b. En la barra de navegación, seleccione la región a utilizar. c. En el panel de navegación, seleccione Clusters (Clústeres). d. En la página Clústeres, seleccione el clúster EcsAnywhereCluster. e. Elija Definiciones de tareas. f. Confirme que el contenedor se está ejecutando.	

Limpieza

Tarea	Descripción	Habilidades requeridas

Limpie y elimine los recursos.	Después de seguir este patrón, debe eliminar los proof-of-concept recursos que ha creado. Para limpiar, introduzca los siguientes comandos.
	`$cdk destroy EcsAnywhe rePipelineStack`
	`$cdk destroy EcsAnywhe reInfraStack`
		DevOps ingeniero

Resolución de problemas

Problema	Solución

Errores relacionados con la falta de paquetes al instalar dependencias de paquetes.	Ejecute uno de los siguientes comandos para resolver los paquetes que faltan.
	`$npm ci`
	o
	`$npm install -g @aws-cdk/<package_ name>`

Al ejecutar el comando `aws ssm create-activation` en la máquina virtual, recibe el siguiente error. `An error occurred (Validati onException) when calling the CreateActivation operation:`	La pila `EcsAnywhereInfraStack` no se ha implementado por completo, y el rol de IAM necesario para ejecutar este comando no se ha creado todavía. Comprueba el estado de la pila en la CloudFormation consola. Vuelva a

Problema	Solución
`Nonexistent role or missing ssm service principal in trust policy: arn:aws:iam::000000000000:role/EcsAnywhereInstanceRole`	intentar el comando después de que el estado cambie a `CREATE_COMPLETE` .

La comprobación de estado de Amazon ECS devuelve el resultado `UNHEALTHY` , y aparece el siguiente error en la sección Servicios del clúster en la consola de Amazon ECS.
 	
`service EcsAnywhereService was unable to place a task because no container instance met all of its requirements. Reason: No Container Instances were found in your cluster.`
	Reinicie el agente de Amazon ECS en su máquina virtual de Vagrant ejecutando los siguientes comandos.
	
	`$vagrant ssh`
	`$sudo systemctl restart ecs`
	`$sudo systemctl status ecs`

Recursos relacionados

- Página de marketing de Amazon ECS Anywhere
- Documentación de Amazon ECS Anywhere
- Demostración de Amazon ECS Anywhere (video)
- Muestras de talleres de Amazon ECS Anywhere (GitHub)
- Duplicación de repositorios (documentación) GitLab

Más patrones

- Implemente aplicaciones en contenedores si se AWS IoT Greengrass V2 ejecutan como un contenedor Docker
- Gestión de las aplicaciones de contenedores en las instalaciones mediante la configuración de Amazon ECS Anywhere con AWS CDK
- Cómo modificar los encabezados HTTP al migrar de F5 a un equilibrador de carga de aplicación en AWS
- Vuelva a alojar las cargas de trabajo en las instalaciones en la nube de AWS: lista de verificación de migración
- Utilice las consultas de BMC Discovery para extraer datos de migración para planificar la migración

Gestión y gobernanza

Temas

- Identifique y avise cuando los recursos de Amazon Data Firehose no estén cifrados con una clave AWS KMS
- Automatice las asignaciones de CIDR, IPAM y IPv4 CIDR de Amazon VPC para nuevos mediante AFT Cuentas de AWS
- Automatice la adición o actualización de entradas de registro de Windows con AWS Systems Manager
- Crear automáticamente una RFC en AMS mediante Python
- Detener e iniciar automáticamente una instancia de base de datos de Amazon RDS mediante AWS Systems Manager Maintenance Windows
- Centralización de la distribución de paquetes de software en AWS Organizations mediante Terraform
- Configure el registro para las aplicaciones.NET en Amazon CloudWatch Logs mediante NLog
- Copiar los productos de AWS Service Catalog en diferentes cuentas y regiones de AWS
- Crear una matriz RACI o RASCI para un modelo operativo en la nube
- Cree alarmas para métricas personalizadas mediante la detección de CloudWatch anomalías de Amazon
- Crear un IDE de AWS Cloud9 que utilice volúmenes de Amazon EBS con cifrado predeterminado
- Crea automáticamente CloudWatch paneles de Amazon basados en etiquetas
- Documentación del diseño de su AWS Landing Zone
- Mejore el rendimiento operativo habilitando Amazon DevOps Guru en varias regiones y cuentas de AWS y OUs con la CDK de AWS
- Control de los conjuntos de permisos para varias cuentas mediante Account Factory for Terraform
- Implementación del Generador de cuentas para Terraform (AFT) mediante una canalización de arranque
- Administre los productos de AWS Service Catalog en varias cuentas y regiones de AWS
- Supervisión de los clústeres de SAP RHEL Pacemaker mediante los servicios de AWS
- Supervise la actividad de las aplicaciones mediante CloudWatch Logs Insights
- Supervise el uso de una imagen de máquina de Amazon compartida en múltiples Cuentas de AWS
- Vea los detalles de la instantánea de EBS de su cuenta u organización de AWS

- Más patrones

Identifique y avise cuando los recursos de Amazon Data Firehose no estén cifrados con una clave AWS KMS

Ram Kandaswamy, Amazon Web Services

Resumen

Para garantizar la conformidad, algunas organizaciones deben tener el cifrado activado en los recursos de entrega de datos, como Amazon Data Firehose. Este patrón muestra una forma de monitorear, detectar y notificar cuando los recursos no cumplen con las normas.

Para mantener el requisito de cifrado, este patrón se puede utilizar AWS para proporcionar supervisión y detección automatizadas de los recursos de entrega de Amazon Data Firehose que no están cifrados con una clave AWS Key Management Service (AWS KMS). La solución envía notificaciones de alerta y se puede ampliar para que se corrija automáticamente. Esta solución se puede aplicar a una cuenta individual o a un entorno de varias cuentas, como un entorno que utilice una AWS landing zone o. AWS Control Tower

Requisitos previos y limitaciones

Requisitos previos

- Flujo de entrega de Amazon Data Firehose
- Permisos suficientes y familiaridad con lo que CloudFormation se utiliza en esta automatización de infraestructuras

Limitaciones

- La solución no es en tiempo real porque utiliza AWS CloudTrail eventos para la detección y hay un retraso entre el momento en que se crea un recurso no cifrado y el momento en que se envía la notificación.

Arquitectura

Pila de tecnología de destino

La solución utiliza tecnología sin servidor y los siguientes servicios:

- AWS CloudTrail

- Amazon CloudWatch
- AWS Command Line Interface (AWS CLI)
- AWS Identity and Access Management (IAM)
- Amazon Data Firehose
- AWS Lambda
- Amazon Simple Notification Service (Amazon SNS)

Arquitectura de destino

En el siguiente diagrama se muestran estos pasos:

1. Un usuario crea o modifica Amazon Data Firehose.
2. Se detecta un CloudTrail evento y se hace coincidir.
3. Lambda es invocado.
4. Se identifican los recursos que no cumplen con las normas.
5. Se envía una notificación por correo electrónico.

Automatización y escala

Puede utilizarla CloudFormation StackSets para aplicar esta solución a varias cuentas Regiones de AWS o a cuentas con un solo comando.

Tools (Herramientas)

- AWS CloudTrailes una Servicio de AWS que le ayuda a habilitar la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de su empresa Cuenta de AWS. Las acciones realizadas por un usuario, un rol o una Servicio de AWS persona se registran como eventos en CloudTrail. Los eventos incluyen las acciones realizadas en las operaciones Consola de administración de AWS AWS CLI AWS SDKs,, y API.
- Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en AWS los recursos.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le permite interactuar con ella Servicios de AWS mediante comandos del shell de la línea de comandos.

- AWS Identity and Access Management (IAM) es un servicio web que le ayuda a controlar de forma segura el acceso a AWS los recursos. Utilice IAM para controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos.
- Amazon Data Firehose es un servicio totalmente administrado para enviar datos de streaming en tiempo real. Con Firehose, no es necesario escribir aplicaciones ni administrar recursos. Configure los productores de datos para que envíen datos a Firehose y este entrega inmediatamente los datos al destino que usted especificó.
- AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo paga el tiempo de computación que consume, sin ningún cargo mientras su código no se ejecuta.
- Amazon Simple Notification Service (Amazon SNS) es un servicio administrado con el que se ofrece la entrega de mensajes de los publicadores a los suscriptores (también conocidos como productores y consumidores).

Epics

Aplique el cifrado para garantizar el cumplimiento

Tarea	Descripción	Habilidades requeridas
Despliegue CloudFormation StackSets.	En AWS CLI, utilice la `firehose-encryption-checker.yaml` plantilla (adjunta) para crear el conjunto de pilas ejecutando el siguiente comando. Proporcione un Nombre de recurso de Amazon (ARN) de tema de Amazon SNS válido para el parámetro. La implementación debe crear correctamente las reglas de CloudWatch eventos, la función Lambda y un rol de IAM con los permisos	Arquitecto de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	necesarios, tal y como se describe en la plantilla. `aws cloudformation create-stack-set --stack-set-name my-stack-set --template-body file://firehose-encryption-checker.yaml`	
Cree instancias de pila.	Las pilas se pueden crear en la cuenta que Regiones de AWS prefieras, así como en una o más cuentas. Para crear instancias de pila, ejecute el siguiente comando. Sustituya el nombre de la pila, los números de cuenta y las regiones por sus propios valores. `aws cloudformation create-stack-instances --stack-set-name my-stack-set --accounts 123456789012 223456789012 --regions us-east-1 us-east-2 us-west-1 us-west-2 --operation-preferences FailureToleranceCount=1`	Arquitecto de la nube, administrador de sistemas

Recursos relacionados

- Trabajando con CloudFormation StackSets

- ¿Qué es Amazon CloudWatch Events?

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Automatice las asignaciones de CIDR, IPAM y IPv4 CIDR de Amazon VPC para nuevos mediante AFT Cuentas de AWS

Kien Pham y Alex Pazik, Amazon Web Services

Resumen

Este patrón muestra cómo automatizar las asignaciones de IPv4 CIDR de Amazon VPC IP Address Manager (IPAM) para las nuevas mediante Cuentas de AWS AWS Control Tower Account Factory for Terraform (AFT). Esto se hace mediante una personalización a nivel de cuenta que asigna un bloque IPv4 CIDR de IPAM a una nueva nube privada virtual (VPC) mediante el módulo. `aft-account-customizations`

Con IPAM, puede organizar, asignar, monitorear y auditar las direcciones IP a gran escala, lo que le permite planificar, rastrear y monitorear fácilmente las direcciones IP de sus cargas de trabajo. AWS Puede crear un grupo de IPAM e IPAM para asignar un bloque IPv4 CIDR a una nueva VPC durante el proceso de venta de cuentas.

Requisitos previos y limitaciones

Requisitos previos

- Una activa AWS Control Tower habilitada en una compatible Cuenta de AWS y una AFT implementada Región de AWS
- Un proveedor de sistemas de control de versiones (VCS) compatible BitBucket, como GitHub, y Enterprise GitHub
- Interfaz de la línea de comandos (CLI) de Terraform instalada
- Un entorno de tiempo de ejecución en el que pueda ejecutar el módulo Terraform que instala AFT.
- AWS Command Line Interface (AWS CLI) instalado y configurado

Limitaciones

- Algunas Servicios de AWS no están disponibles en todas Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Versiones de producto

- AWS Control Tower landing zone versión 3.0 o posterior, anterior a la versión 4.0
- Versión 1.13.0 o posterior de la AFT, anterior a la versión 2.0.0
- La versión 1.2.0 o posterior de Terraform OSS, anterior a la versión 2.0.0
- Terraform AWS Provider (`terraform-provider-aws`) versión 5.11.0 o posterior, anterior a la versión 6.0.0
- La versión 2.1.0 o posterior del módulo de Terraform para IPAM (`aws-ia/ipam/aws`)

Arquitectura

En el siguiente diagrama se muestran el flujo de trabajo y los componentes de este patrón.

El flujo de trabajo consta de las tareas principales siguientes:

1. Cambios desencadenantes: los cambios en la personalización de Terraform e IPAM se transfieren al repositorio y se publican. GitHub Esta tarea activa la AWS CodeBuild canalización automáticamente.
2. Automatice la construcción: en su interior CodeBuild, se activan varios proyectos de compilación AWS Step Functions.
3. Aplica la personalización: Step Functions se coordina con CodeBuild ella para planificar y aplicar los cambios de Terraform. Esta tarea utiliza el módulo AFT Terraform para coordinar la asignación de IP del grupo de IPAM a la AWS cuenta vendida.

Tools (Herramientas)

Servicios de AWS

- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- AWS CodePipeline permite diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software y automatizar los pasos necesarios para lanzar los cambios en el software de manera continua.

- AWS Control Towerorganiza las capacidades de varios otros Servicios de AWS, incluidos AWS Organizations, y. AWS Service Catalog AWS IAM Identity Center Puede ayudarlo a configurar y administrar un entorno de AWS múltiples cuentas, siguiendo las mejores prácticas prescriptivas.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS SDK para Python (Boto3)es un kit de desarrollo de software que le ayuda a integrar su aplicación, biblioteca o script de Python con Servicios de AWS.
- AWS Service Catalogle ayuda a gestionar de forma centralizada los catálogos de servicios de TI AWS aprobados. Los usuarios finales pueden implementar rápidamente solo los servicios de TI aprobados que necesitan, de acuerdo con las limitaciones establecidas por su organización.
- AWS Step Functionses un servicio de organización sin servidor que le ayuda a combinar AWS Lambda funciones y otras Servicios de AWS para crear aplicaciones esenciales para la empresa.
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS. El administrador de direcciones IP de Amazon VPC (IPAM) es una función de VPC que le facilita la planificación, el seguimiento y la supervisión de las direcciones IP de sus cargas de trabajo. AWS

Otras herramientas

- GitHubes una plataforma para desarrolladores que los desarrolladores pueden usar para crear, almacenar, administrar y compartir su código.
- HashiCorp Terraform es una herramienta de infraestructura como código (IaC) que le ayuda a crear y administrar recursos locales y en la nube. Esto incluye componentes de bajo nivel, como instancias de procesamiento, almacenamiento y redes, y componentes de alto nivel, como entradas de DNS y característica de software como servicio (SaaS).
- Python es un lenguaje de programación informático de uso general. Puede usar esta herramienta para crear aplicaciones, automatizar tareas y desarrollar servicios en Nube de AWS.

Repositorio de código

- El código de este patrón está disponible en el repositorio GitHub AWS Control Tower Account Factory for Terraform.

Prácticas recomendadas

Al implementar AFT, le recomendamos que siga las prácticas recomendadas para garantizar una implementación segura, eficiente y correcta. Las pautas y recomendaciones clave para implementar y operar la AFT incluyen los siguientes pasos:

- Revisión exhaustiva de las entradas: revise y comprenda cuidadosamente cada entrada. La configuración correcta de las entradas es crucial para la configuración y el funcionamiento de la AFT.
- Actualizaciones periódicas de las plantillas: mantenga las plantillas actualizadas con las últimas AWS funciones y versiones de Terraform. Las actualizaciones periódicas lo ayudarán a aprovechar las nuevas funciones y a mantener la seguridad.
- Control de versiones: fije la versión de su módulo de AFT y, si es posible, utilice una implementación de AFT independiente para realizar las pruebas.
- Alcance: utilice AFT únicamente para implementar barreras de protección y personalizaciones de infraestructura. No use AFT para implementar la aplicación.
- Lint y validación: la canalización de AFT requiere una configuración de Terraform de tipo Lint y que esté validada. Ejecute Lint, valide y pruebe todo antes de enviar la configuración a los repositorios de AFT.
- Módulos de Terraform: cree código de Terraform reutilizable como módulos y especifique siempre las versiones de Terraform y del AWS proveedor para que se ajusten a los requisitos de su organización.

Epics

Configure y configure su entorno AWS

Tarea	Descripción	Habilidades requeridas
Implemente AWS Control Tower.	Instálelo y AWS Control Tower configúrelo en su AWS entorno para garantizar la	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	administración y el gobierno centralizados de su Cuentas de AWS. Para obtener más información, consulte Primeros pasos AWS Control Tower en la AWS Control Tower documentación.	
Implemente AWS Control Tower Account Factory para Terraform (AFT).	Configure AFT en una nueva cuenta de administración de AFT dedicada. Para obtener más información, consulte Configurar e iniciar su AWS Control Tower Account Factory para Terraform en la AWS Control Tower documentación.	Administrador de la nube
Complete la AFT después de la implementación.	Una vez que se complete el despliegue de la infraestructura AFT, complete los pasos que se indican en la documentación sobre los pasos posteriores al despliegue. AWS Control Tower	Administrador de la nube

Creación de un IPAM

Tarea	Descripción	Habilidades requeridas
Delegue un administrador de IPAM	Para delegar una cuenta de administrador de IPAM en su AWS organización, siga los siguientes pasos:	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	1. Con la cuenta AWS Organizations de administración, abra la consola de IPAM en. https://console.aws.amazon.com/ipam/ 2. En Consola de administración de AWS, elija el lugar Región de AWS en el que desee trabajar con el IPAM. 3. En el panel de navegación, elija Configuración de la organización. 4. Elija Delegar. La opción Delegar solo está disponible si ha iniciado sesión en la consola como cuenta de AWS Organizations administración. 5. Introduzca el Cuenta de AWS ID de una cuenta de IPAM. El administrador de IPAM debe estar en una cuenta de AWS Organizations miembro. 6. Seleccione Save changes (Guardar cambios). Como alternativa, puede usar AWS CLI y ejecutar el siguiente comando: `aws ec2 enable-ipam-organization-admin-account \`	

Tarea	Descripción	Habilidades requeridas
	`--delegated-admin-account-id 012345678901` Para obtener más información, consulte Integrar el IPAM con las cuentas de una AWS organización en la documentación de Amazon VPC enable-ipam-organization-adminy-account en AWS CLI la Referencia de comandos. **Important** Para seguir utilizando IPAM, debe iniciar sesión en la cuenta de administrador delegado. El perfil de SSO o las variables de AWS entorno especificadas en el siguiente paso deben permitirle iniciar sesión en esa cuenta y conceder permisos para crear un grupo regional y de alto nivel de IPAM.	

Tarea	Descripción	Habilidades requeridas

Cree un grupo regional y de nivel superior de IPAM.	El GitHub repositorio de este patrón contiene una plantilla de Terraform que puede usar para crear su grupo de nivel superior y su grupo regional de IPAM. A continuación, puede compartir los grupos con una organizac ión, unidad organizativa (OU) u otro recurso mediante AWS Resource Access Manager (). Cuenta de AWSAWS RAM
	
	Utilice los siguientes pasos:
	
	1. Ejecute los siguientes comandos :
	
	`# Navigate to the IPAM module`
	`cd ipam/terraform`
	
	`# Initiate the IPAM module`
	`terraform init`
	
	2. Abra el archivo `main.tf`, modifique el código como se describe en los comentarios siguientes y guarde el archivo.
	
	`terraform { required_providers { aws = { source = "hashicorp/aws"`
		Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	<pre> version = ">= 5.11.0, < 6.0.0"
	    }
	  }
	}
	
	provider "aws" {
	  region = "us-east-1" # Replace with the region to create your top-level pool
	}
	
	module "ipam" {
	  source = "aws-ia/ipam/aws"
	  version = ">= 2.1.0"
	
	  top_name = "my-top-level-pool" # Replace with your desired top-level pool name
	  top_description = "top-level pool" # Replace with your desired top-level level pool description
	  top_cidr = ["10.0.0.0/16"] # Replace with your desired top-level pool CIDR
	
	  pool_configurations = {
	    my-regional-pool = { # (Optional) Replace with a different resource name
	      name = "my-regional-pool"</pre>	

Tarea	Descripción	Habilidades requeridas

	<pre> # Replace with your
	  desired pool name
	       description
	       = "regional
	  pool" # Replace with
	  your desired pool
	  description
	       cidr
	    = ["10.0.0.0/23"]
	  # Replace with your
	  desired pool CIDR
	       locale
	      = "us-east-1"
	  # Replace with your
	  desired pool locale
	       ram_share
	_principals =
	  ["arn:aws:organiza
	tions::01234567890
	1:ou/ou-ab1c2de345
	/ou-ab1c2de345"]
	  # Replace with your
	  desired principal
	  ARN to share with
	  via Resource Access
	  Manager (RAM)
	     }
	   }
	}
	
	output "my_regio
	nal_pool_id" {
	   description = "The
	  ID of the regional
	  pool"
	   value =
	  module.ipam.pools_
	level_1["my-region
	al-pool"].id #
	  Replace with your
	  desired resource name
	  if changed above</pre>	

Tarea	Descripción	Habilidades requeridas

	<pre>}
	
	# Create the IPAM
	 top-level and
	 resource pool
	terraform apply</pre>
	Anote el ID del grupo de recursos que se muestra después de la creación. Necesitará ese ID al enviar la solicitud de cuenta. Si olvida el ID del grupo de recursos, puede obtenerlo más adelante en la Consola de administr ación de AWS.
	
	Important
	Asegúrese de que los grupos creados CIDRs no se superpong an con ningún otro grupo de su región de trabajo. Puede crear un grupo sin un CIDR, pero no podrá utilizar el grupo para asignaciones hasta que le haya aprovisio nado un CIDR. Puede añadir elementos CIDRs a un grupo en	

Tarea	Descripción	Habilidades requeridas
	cualquier momento editando el grupo.	

Integración de IPAM con AFT

Tarea	Descripción	Habilidades requeridas

Comience a crear la personalización de la cuenta.	Para iniciar una nueva personalización de la cuenta, ejecute los siguientes comandos desde su terminal:
	`# Default name for customization repo`
	`cd aft-account-customizations # Replace with your actual repo name if different than the default`
	`mkdir -p APG-AFT-IPAM/terraform # Replace APG-AFT-IPAM with your desired customization name`
	`cd APG-AFT-IPAM/terraform`
		DevOps ingeniero

Cree el archivo `aft-providers.jinja` .	Agregue código dinámico al archivo `aft-providers.jinja` que especifique el backend y el proveedor de Terraform que va a usar. Utilice los siguientes pasos:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	1. Cree un archivo `aft-providers.jinja` nuevo en el directorio `terraform` . 2. Abra el archivo, añada el siguiente código y guarde el archivo. `provider "aws" { region = "{{ provider_region }}" assume_role { role_arn = "{{ target_admin_role_arn }}" } default_tags { tags = { managed_by = "AFT" } } }`	

Tarea	Descripción	Habilidades requeridas

Cree el archivo `backend.jinja` .	Agregue código dinámico al archivo `backend.jinja` que especifique el backend y el proveedor de Terraform que va a usar.
	
	Utilice los siguientes pasos:
	
	1. Cree un archivo `backend.jinja` nuevo en el directorio `terraform` .
	2. Abra el archivo, añada el siguiente código y guarde el archivo.
	
	``
	## Auto generated
	 backend.tf ##
	## Updated on:
	 {{ timestamp }} ##
	
	{% if tf_distri
	bution_type == "oss"
	 -%}
	terraform {
	  required_version
	 = ">= {{ tf_versio
	n }}"
	  backend "s3" {
	  region =
	 "{{ region }}"
	  bucket =
	 "{{ bucket }}"
	  key =
	 "{{ key }}"
	  dynamodb_table
	 = "{{ dynamodb_
	table }}"
	``
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	<pre> encrypt =
	 "true"
	    kms_key_id =
	 "{{ kms_key_id }}"
	    role_arn
	  = "{{ aft_admin
	_role_arn }}"
	  }
	}
	{% else -%}
	terraform {
	    backend "remote" {
	        organizat
	ion = "{{ terraform
	_org_name }}"
	        workspaces {
	        name =
	 "{{ terraform
	_workspace_name }}"
	        }
	    }
	}
	{% endif %}</pre>	

Tarea	Descripción	Habilidades requeridas

Cree el archivo `main.tf`.	Cree un `main.tf` archivo nuevo y añada código que defina dos fuentes de datos que recuperan dos valores de AWS Systems Manager (`aws_ssm`) y crean la VPC.
	
	Utilice los siguientes pasos:
	
	1. Cree un archivo `main.tf` nuevo en el directorio `terraform` .
	2. Abra el archivo, añada el siguiente código y guarde el archivo.
	
	`# Define data sources`
	`data "aws_ssm_`
	`parameter" "vpc_ipam`
	`_id" {`
	`  name = "/aft/acc`
	`ount-request/custo`
	`m-fields/vpc-`
	`ipam-id" # Value`
	` is defined in the`
	` account-request.tf`
	` file`
	`}`
	
	`data "aws_ssm_`
	`parameter" "vpc_netm`
	`ask" {`
	`  name = "/aft/acc`
	`ount-request/custo`
	`m-fields/vpc-ipam-`
	`netmask" # Value`
	` is defined in the`
	` account-request.tf`
	` file`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	}
	
	# Create new VPC
	resource "aws_vpc"
	 "vpc1" {
	
	 ipv4_ipam_pool_id
	 = data.aws_ssm_param
	eter.vpc_ipam_id.v
	alue # Retrieved from
	 SSM - this is how we
	 integrate with IPAM
	 ipv4_netmask_lengt
	h = data.aws_
	ssm_parameter.vpc_
	netmask.value #
	 Retrieved from SSM
	
	 assign_generated_i
	pv6_cidr_block
	 = var.enable_ipv6 ?
	 true : null
	 ipv6_cidr_block
	 =
	 var.ipv6_cidr
	 ipv6_ipam_pool_id
	 =
	 var.ipv6_ipam_pool
	_id
	 ipv6_netmask_lengt
	h =
	 var.ipv6_netmask_l
	ength
	 ipv6_cidr_block_ne
	twork_border_group =
	 var.ipv6_cidr_bloc
	k_network_border_g
	roup
	
	 instance_tenancy
	 =	

Tarea	Descripción	Habilidades requeridas

	<pre> var.instance_tenancy
	  enable_dns_hostnames = var.enable_dns_hostnames
	  enable_dns_support = var.enable_dns_support
	  enable_network_address_usage_metrics = var.enable_network_address_usage_metrics
	
	  tags = var.tags
	
	  lifecycle {
	  ignore_changes = [
	  tags, # Any changes made to VPC tags after creation will not be overwritten - remove to revert these changes during future 'terraform apply' operations
	  ]
	  }
	}</pre>	

Tarea	Descripción	Habilidades requeridas

Cree el archivo `variables.tf` .	Cree un archivo `variables.tf` que indique las variables que usa el módulo de Terraform.
	
	Utilice los siguientes pasos:
	
	1. Cree un archivo `variables.tf` nuevo en el directorio `terraform` .
	2. Abra el archivo, añada el siguiente código y guarde el archivo.
	
	`# Copied from AWS VPC module`
	`# https://github.com/terraform-aws-modules/terraform-aws-vpc/blob/master/variables.tf`
	
	`variable "name" {`
	`  description = "Name to be used on all the resources as identifier"`
	`  type        = string`
	`  default     = ""`
	`}`
	
	`variable "enable_ipv6" {`
	`  description = "Requests an Amazon-provided IPv6 CIDR block with a /56 prefix length for the VPC. You cannot`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	specify the range of IP addresses, or the size of the CIDR block"
	type = bool
	default = false
	}
	
	variable "ipv6_cidr" {
	description = "(Optional) IPv6 CIDR block to request from an IPAM Pool. Can be set explicitly or derived from IPAM using `ipv6_netmask_length`"
	type = string
	default = null
	}
	
	variable "ipv6_ipam_pool_id" {
	description = "(Optional) IPAM Pool ID for a IPv6 pool. Conflicts with `assign_generated_ipv6_cidr_block`"
	type = string
	default = null
	}
	
	variable "ipv6_netmask_length" {
	description = "(Optional) Netmask length to request from IPAM Pool. Conflicts with `ipv6_cidr_block`.	

Tarea	Descripción	Habilidades requeridas
	``` This can be omitted if IPAM pool as a `allocation_defaul t_netmask_length` set. Valid values: `56`" type = number default = null } variable "ipv6_cid r_block_network_bo rder_group" { description = "By default when an IPv6 CIDR is assigned to a VPC a default ipv6_cidr_block_ne twork_border_group will be set to the region of the VPC. This can be changed to restrict advertise ment of public addresses to specific Network Border Groups such as LocalZones" type = string default = null } variable "instance _tenancy" { description = "A tenancy option for instances launched into the VPC" type = string default = "default" } ```	

Tarea	Descripción	Habilidades requeridas

	<pre>variable "enable_dns_hostnames" {
	  description = "Should be true to enable DNS hostnames in the VPC"
	  type = bool
	  default = true
	}
	
	variable "enable_dns_support" {
	  description = "Should be true to enable DNS support in the VPC"
	  type = bool
	  default = true
	}
	
	variable "enable_network_address_usage_metrics" {
	  description = "Determines whether network address usage metrics are enabled for the VPC"
	  type = bool
	  default = null
	}
	
	variable "tags" {
	  description = "A map of tags to add to all resources"
	  type = map(string)
	  default = {}
	}</pre>	

Tarea	Descripción	Habilidades requeridas

Cree el archivo `terraform.tfvars` .	Cree un archivo `terraform.tfvars` que defina los valores de las variables que se pasan al archivo `main.tf`.
	
	Utilice los siguientes pasos:
	
	1. Cree un archivo `terraform.tfvars` nuevo en el directorio `terraform` .
	2. Abra el archivo, añada el siguiente código y guarde el archivo.
	
	`name = "demo-ipam"`
	`enable_ipv6 = false`
	`enable_dns_hostnames = true`
	`enable_dns_support = true`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Cree el archivo `outputs.tf` .	Cree un nuevo `outputs.tf` archivo que exponga algunos valores en CodeBuild.
	
	Utilice los siguientes pasos:
	
	1. Cree un archivo `outputs.tf` nuevo en el directorio `terraform` .
	2. Abra el archivo, añada el siguiente código y guarde el archivo.
	
	``
	# Output VPC ID and
	 ARN in CodeBuild
	output "vpc1" {
	  description = "VPC
	 1 information"
	  value = {
	  id = try(aws_v
	pc.vpc1.id, null)
	  arn = try(aws_v
	pc.vpc1.arn, null)
	  }
	}
	``
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Confirme la personalización.	Para confirmar la nueva personalización en el repositorio de personalizaciones de la cuenta, ejecute los siguientes comandos:
	`# Assumes you are still in the /terraform directory`
	`cd .. # Skip if you are in the account customization root directory (APG-AFT-IPAM)`
	`git add .`
	`git commit -m "APG customization"`
	`git push origin`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Aplique la personalización.	Agregue el código al archivo `account-requests.tf` que solicita una nueva cuenta con la personalización de la cuenta recién creada. Los campos personalizados crean los parámetros de Systems Manager en la cuenta de venta que son necesario s para crear la VPC con el CIDR asignado por IPv4 IPAM correcto. Utilice los siguientes pasos: 1. En un terminal, vaya al directorio `aft-account-request/terraform` . 2. Abra el archivo `account-requests.tf` , añada y modifique el siguiente código con sus valores y guarde el archivo. `module "sandbox_account_01" { source = "./modules/aft-account-request" control_tower_parameters = { AccountEmail = "john.doe@example.com"`	AWS DevOps

Tarea	Descripción	Habilidades requeridas

	<pre> AccountName =
	 "sandbox-account-0
	1"
	    # Syntax for top-
	level OU
	    ManagedOr
	ganizationalUnit =
	 "Sandbox"
	    # Syntax for
	 nested OU
	    # ManagedOr
	ganizationalUnit =
	 "Sandbox (ou-xfe5-
	a8hb8ml8)"
	    SSOUserEmail
	 = "john.doe@example.
	com"
	    SSOUserFirstName
	 = "John"
	    SSOUserLastName
	 = "Doe"
	  }
	
	  account_tags = {
	    "ABC:Owner"
	 = "john.doe@example.
	com"
	    "ABC:Division"
	 = "ENT"
	    "ABC:Environment"
	 = "Dev"
	    "ABC:CostCenter"
	 = "123456"
	    "ABC:Vended"
	 = "true"
	    "ABC:DivCode"
	 = "102"
	    "ABC:BUCode"
	 = "ABC003"
	    "ABC:Project"
	 = "123456"
	  }</pre>	

Tarea	Descripción	Habilidades requeridas

```
  change_management_
parameters = {
    change_re
quested_by = "John
 Doe"
    change_reason
       = "testing
 the account vending
 process"
  }

  custom_fields = {
    vpc-ipam-id =
 "ipam-pool-123456a
b789041cd2"
    vpc-ipam-netmask
 = "24"

  }

  account_customizat
ions_name = "APG-AFT-
IPAM" # Do not change
 this value
}
```

> **Important**
>
> Asegúrese de que el `vpc-ipam-netmask` valor sea menor o igual a la asignación `netmask` del grupo de IPAM y de que haya suficientes recursos IPs disponibles en el

Tarea	Descripción	Habilidades requeridas

	grupo de IPAM para asignarlos a la VPC.
	3. Para confirmar la nueva cuenta en el repositorio de solicitudes de cuentas, utilice los siguientes comandos:
	`git add .`
	`git commit -m 'requested APG account'`
	`git push origin`	

Tarea	Descripción	Habilidades requeridas
Valide la personalización.	Inicie sesión en la cuenta recién creada y compruebe que la personalización se haya aplicado correctamente. Utilice los siguientes pasos: 1. Abra la página AWS IAM Identity Center de inicio de sesión y autentíquese como el usuario que especificó en el `account-requests.tf` archivo. 2. En la lista de cuentas del Centro de Identidad de IAM, elija la cuenta que ha vendido anteriorm ente e inicie sesión con el rol. AWS `AdministratorAccess` 3. Ve a la consola de VPC y selecciona Tu. VPCs 4. Seleccione el ID de la VPC que acaba de crear. 5. Elija la pestaña CIDRs. Debería ver un CIDR asignado a IPAM. IPv4 6. (Opcional) Inicie sesión en su cuenta de administr ador delegado de IPAM y compruebe que la asignació n se muestra en la consola de IPAM.	DevOps ingeniero

Resolución de problemas

Problema	Solución
Se producen errores en la creación o administración de los recursos a causa de permisos inadecuados.	Revise las funciones y políticas AWS Identity and Access Management (de IAM) asociadas a Step Functions y otros servicios involucrados en la implementación. CodeBuild Confirme que tengan los permisos necesarios. Si tiene problemas con los permisos, ajuste las políticas de IAM para conceder el acceso necesario.
Servicio de AWS Las cuotas se alcanzan durante la implementación.	Antes de implementar la canalización, compruebe Servicio de AWS las cuotas de recursos, como los buckets de Amazon Simple Storage Service (Amazon S3), las funciones y las funciones de IAM. AWS Lambda Si es necesario, solicite un aumento de las cuotas. Para obtener más información, consulte Servicio de AWS Service Quotas en la Referencia general de AWS .

Recursos relacionados

Servicio de AWS documentación

- AWS Control Tower Guía del usuario
- Cómo funciona el IPAM
- Security best practices in IAM (Prácticas recomendadas de seguridad en IAM)
- Servicio de AWS cuotas

Otros recursos

- Documentación de Terraform AWS Provider

Automatice la adición o actualización de entradas de registro de Windows con AWS Systems Manager

Appasaheb Bagali, Amazon Web Services

Resumen

AWS Systems Manager es una herramienta de administración remota para instancias de Amazon Elastic Compute Cloud (Amazon EC2). Systems Manager proporciona visibilidad y control sobre su infraestructura en Amazon Web Services. Esta versátil herramienta permite corregir los cambios en el registro de Windows identificados como vulnerabilidades por el informe de análisis de vulnerabilidades de seguridad.

Este patrón describe los pasos para mantener seguras EC2 las instancias que ejecutan el sistema operativo Windows mediante la automatización de los cambios de registro recomendados para la seguridad de su entorno. El patrón emplea Run Command para ejecutar un documento de comandos. Se adjunta el código, y una parte del mismo se incluye en la sección de código.

Requisitos previos y limitaciones

- Una cuenta de AWS activa
- Permisos para acceder a la EC2 instancia y a Systems Manager

Arquitectura

Pila de tecnología de destino

- Una nube privada virtual (VPC), con dos subredes y una puerta de enlace de traducción de direcciones de red (NAT)
- Un documento de comandos de Systems Manager para añadir o actualizar el nombre y el valor del registro
- Systems Manager: ejecute el comando para ejecutar el documento de comandos en las EC2 instancias especificadas

Arquitectura de destino

Tools (Herramientas)

Herramientas

- Políticas y roles de IAM: AWS Identity and Access Management (IAM) es un servicio web que le ayuda a controlar de forma segura el acceso a los recursos de AWS. Utilice IAM para controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos.
- Amazon Simple Storage Service Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet. Está diseñado para facilitar a los desarrolladores recursos de computación escalables basados en Web. En este patrón se usa un bucket de S3 para almacenar los registros de Systems Manager.
- AWS Systems Manager: AWS Systems Manager es un servicio que puede utilizar para ver y controlar su infraestructura en AWS. Systems Manager le ayuda a mantener la seguridad y la conformidad mediante el análisis de sus instancias administradas y el informe sobre las infracciones de las políticas que detecte (o la toma de medidas correctivas con respecto a estas).
- Documento de comandos de AWS Systems Manager: Run Command emplea los documentos de comandos de AWS Systems Manager. La mayoría de los documentos de Command son compatibles con todos los sistemas operativos Linux y Windows, que a su vez son compatibles con Systems Manager.
- AWS Systems Manager Run Command: AWS Systems Manager Run Command le ofrece una forma de gestionar la configuración de sus instancias administradas de forma remota y segura. Run Command le permite automatizar las tareas administrativas comunes y llevar a cabo cambios de configuración únicas a escala.

Código

Puede utilizar el siguiente código de ejemplo para agregar o actualizar un nombre de registro de Microsoft Windows en `Version`, una ruta de registro a `HKCU:\Software\ScriptingGuys\Scripts` y un valor a 2.

```
#Windows registry path which needs to add/update
$registryPath ='HKCU:\\Software\\ScriptingGuys\\Scripts'
#Windows registry Name  which needs to add/update
$Name = 'Version'
#Windows registry value  which needs to add/update
$value = 2
```

```
# Test-Path cmdlet to see if the registry key exists.
IF(!(Test-Path $registryPath))
        {
           New-Item -Path $registryPath -Force | Out-Null
           New-ItemProperty -Path $registryPath -Name $name -Value     $value ` -
PropertyType DWORD -                 Force | Out-        Null
        } ELSE {
                      New-ItemProperty -Path $registryPath -Name $name -Value $value `
 -PropertyType            DWORD        -Force | Out-Null
            }
echo 'Registry Path:'$registryPath
 echo 'Registry Name:'$registryPath
 echo 'Registry Value:'(Get-ItemProperty -Path $registryPath -Name $Name).version
```

Se adjunta el ejemplo de código de notación de JavaScript objetos (JSON) completo del documento de comandos de Systems Manager.

Epics

Configurar una VPC

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	En la consola de administración de AWS, cree una VPC con subredes públicas y privadas y una puerta de enlace NAT. Para obtener más información, consulte la documentación de AWS.	Administrador de la nube
Cree grupos de seguridad.	Asegúrese de que cada grupo de seguridad permita el acceso al Protocolo de escritorio remoto (RDP) desde la dirección IP de origen.	Administrador de la nube

Crear una política y un rol de IAM

Tarea	Descripción	Habilidades requeridas
Cree una política de IAM.	Cree una política de IAM que proporcione acceso a Amazon S3 EC2, Amazon y Systems Manager.	Administrador de la nube
Crear un rol de IAM.	Cree un rol de IAM y adjunte la política de IAM que proporciona acceso a Amazon S3 EC2, Amazon y Systems Manager.	Administrador de la nube

Ejecute la automatización

Tarea	Descripción	Habilidades requeridas
Cree un documento de comandos de Systems Manager.	Cree un documento de comandos de Systems Manager que implemente la adición o actualización de cambios del registro de Microsoft Windows.	Administrador de la nube
Ejecute Run Command de Systems Manager.	Ejecute Run Command de Systems Manager y seleccione el documento de comandos y las instancias de destino de Systems Manager. Se transferirá el cambio de registro de Microsoft Windows en el documento de comandos seleccionado a las instancias de destino.	Administrador de la nube

Recursos relacionados

- AWS Systems Manager
- Documentos de AWS Systems Manager
- AWS Systems Manager Run Command

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Crear automáticamente una RFC en AMS mediante Python

Gnanasekaran Kailasam, Amazon Web Services

Resumen

AWS Managed Services (AMS) facilita poder operar la infraestructura basada en la nube de forma más eficiente y segura proporcionándole una gestión continua de su infraestructura de Amazon Web Services (AWS). Para realizar un cambio en su entorno administrado, debe crear y enviar una solicitud de cambio (RFC) que incluya un ID de tipo de cambio (CT) para una operación o acción concreta.

Sin embargo, la creación manual de una RFC puede tardar unos cinco minutos y es posible que los equipos de tu organización tengan que enviar varias RFCs todos los días. Este patrón le ayuda a automatizar el proceso de creación de las RFC, a reducir el tiempo de creación de cada RFC y a eliminar los errores manuales.

En este patrón, se describe cómo utilizar el código Python para crear automáticamente la RFC `Stop EC2 instance` que detenga las instancias de Amazon Elastic Compute Cloud (Amazon EC2) en su cuenta de AMS. A continuación, puede aplicar el enfoque de este patrón y la automatización de Python a otros tipos de RFC.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AMS Advanced. Para obtener más información al respecto, consulte los planes de operaciones de AMS en la documentación de AWS Managed Services.
- Al menos una instancia de EC2 existente en su cuenta de AMS.
- Comprensión de cómo crear y enviar RFCs en AMS.
- Conocimientos básicos sobre Python.

Limitaciones

- Solo puedes usarlo RFCs para cambios en tu cuenta de AMS. Su cuenta de AWS utiliza procesos diferentes para realizar cambios similares.

Arquitectura

Pila de tecnología

- AMS
- Interfaz de la línea de comandos de AWS (AWS CLI)
- AWS SDK para Python (Boto3)
- Python y sus paquetes necesarios (JSON y Boto3)

Automatización y escala

Este patrón proporciona un código de muestra para automatizar la `Stop EC2 instance` RFC, pero puede utilizar el código y el enfoque de ejemplo de este patrón para otros RFCs.

Tools (Herramientas)

- AWS Managed Services (AMS) facilita poder utilizar la infraestructura de AWS de forma más eficiente y segura.
- AWS CLI: la interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta unificada para administrar los servicios de AWS. En AMS, la API de administración de cambios proporciona operaciones para crear y administrar RFCs.
- AWS SDK para Python (Boto3): el SDK para Python facilita la integración de su aplicación, biblioteca o script de Python con los servicios de AWS.

Código

El archivo `AMS Stop EC2 Instance.zip` (adjunto) contiene el código Python para crear una RFC `Stop EC2 instance`. También puede configurar este código para enviar un único RFC para varias instancias de EC2.

Epics

Opción 1: configurar el entorno para macOS o Linux

Tarea	Descripción	Habilidades requeridas
Instale y valide Python.	1. Abra una ventana de terminal y ejecute el	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	comando `brew install python3`. 2. Valide que Python esté correctamente instalado ejecutando el comando `python --version` . 3. Valide que `pip` esté correctamente instalado ejecutando el comando `pip --version` .	
Instale la CLI de AWS.	Para instalar la CLI de AWS, ejecute el comando `pip install awscli --upgrade –user` .	Administrador de sistemas de AWS
Instalación de Boto3.	Para instalar Boto3, ejecute el comando `pip install boto3`	Administrador de sistemas de AWS
Instale JSON.	Para instalar JSON, ejecute el comando `pip install json`.	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
Configure la CLI de AWS.	Inicie sesión en la consola de administración de AWS, abra la consola de AMS y, a continuación, seleccione Documentación. Descargue el archivo .zip que contiene la CLI de AMS, descomprímalo e instálelo en su máquina local. Después de instalar AMS CLI, ejecute el comando `aws amscm help`. El resultado proporciona información sobre el proceso de gestión de cambios de AMS.	Administrador de sistemas de AWS

Opción 2: configurar el entorno para Windows

Tarea	Descripción	Habilidades requeridas
Instale y valide Python.	1. Abra la página de Versiones de Python para Windows, descargue la última versión y, a continuación, instale Python. 2. Valide que Python esté correctamente instalado ejecutando el comando `python --version .` 3. Valide que `pip` esté correctamente instalado	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	ejecutando el comando `pip --version` .	
Instale la CLI de AWS.	Para instalar la CLI de AWS, ejecute el comando `pip install awscli --upgrade –user`.	Administrador de sistemas de AWS
Instalación de Boto3.	Para instalar Boto3, ejecute el comando `pip install boto3`	Administrador de sistemas de AWS
Instale JSON.	Para instalar JSON, ejecute el comando `pip install json`.	Administrador de sistemas de AWS
Configure la CLI de AWS.	Inicie sesión en la consola de administración de AWS, abra la consola de AMS y, a continuación, seleccione Documentación. Descargue el archivo .zip que contiene la CLI de AMS, descomprímalo e instálelo en su máquina local. Después de instalar AMS CLI, ejecute el comando `aws amscm help`. El resultado proporciona información sobre el proceso de gestión de cambios de AMS.	Administrador de sistemas de AWS

Extraiga el ID de CT y los parámetros de ejecución del RFC

Tarea	Descripción	Habilidades requeridas
Extraiga el ID de CT, la versión y los parámetros de ejecución del RFC	Cada RFC tiene un ID de CT, una versión y unos parámetros de ejecución diferentes. Puede utilizar alguna de las siguientes opciones para extraer esta información: 1. Siga las instrucciones de la sección de Búsqueda de una solicitud de cambio (RFC) con la CLI en los Ejemplos de uso de la RFC de la documentación de AWS Managed Services. 2. Abra un RFC existente de un tipo similar o cree un RFC nuevo como prueba a través de la consola AMS. Utilice el ID de CT y los parámetros de ejecución del RFC. Para obtener más información al respecto, consulte Búsqueda de una RFC con la consola en la documentación de AWS Managed Services. **Note** Para adaptar la automatización de Python de este	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	patrón a otras RFCs, sustituya el tipo de CT y los valores de los parámetros del archivo de código `ams_stop_ec2_instance` Python del `AMS Stop EC2 Instance.zip` archivo (adjunto) por los que extrajo.	

Ejecute la automatización de Python

Tarea	Descripción	Habilidades requeridas
Ejecute la automatización de Python.	1. Descargue el archivo `AMS Stop EC2 Instance.zip` (adjunto) en el equipo local y extraiga el archivo. 2. Actualice `input_instances` con la información de su instancia EC2. 3. Abra una terminal y navegue hasta la ruta del código extraído 4. Ejecute el comando `pythonams_stop_ec2_instance.py` .	Administrador de sistemas de AWS

Recursos relacionados

- ¿Qué son los tipos de cambios?

- Tutorial de CLI: pila de dos niveles de alta disponibilidad (Linux/RHEL)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Detener e iniciar automáticamente una instancia de base de datos de Amazon RDS mediante AWS Systems Manager Maintenance Windows

Ashita Dsilva, Amazon Web Services

Resumen

Este patrón muestra cómo detener e iniciar automáticamente una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) según un cronograma específico (por ejemplo, cerrar una instancia de base de datos fuera del horario laboral para reducir los costos) mediante AWS Systems Manager Maintenance Windows. Para este propósito, Systems Manager es rentable para los casos de uso típicos.

AWS Systems Manager La automatización proporciona los manuales `AWS-StopRdsInstance` y `AWS-StartRdsInstance` guías para detener e iniciar las instancias de base de datos de Amazon RDS. Esto significa que no necesita escribir una lógica personalizada con AWS Lambda funciones ni crear una regla de Amazon CloudWatch Events.

Systems Manager ofrece dos capacidades para programar tareas: State Manager y Maintenance Windows. State Manager establece y mantiene la configuración de estado requerida para los recursos de su cuenta de Amazon Web Services (AWS) una vez o según un programa específico. Maintenance Windows ejecuta tareas en los recursos de su cuenta durante un período de tiempo específico. Si bien puede utilizar el enfoque de este patrón con State Manager o Maintenance Windows, le recomendamos que utilice Maintenance Windows, ya que puede ejecutar una o más tareas en función de la prioridad asignada y también puede ejecutar AWS Lambda funciones y AWS Step Functions tareas. Para más información sobre State Manager y Maintenance Windows, consulte Elegir entre State Manager y Maintenance Windows en la documentación de Systems Manager.

Este patrón proporciona pasos detallados para configurar dos periodos de mantenimiento independientes que utilizan expresiones cron para detener y, a continuación, iniciar una instancia de base de datos de Amazon RDS.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS.
- Una instancia de base de datos de Amazon RDS existente que desee detener e iniciar según un cronograma específico.

- Expresiones cron para el cronograma requerido. Por ejemplo, la expresión `cron(0 9 ? * MON-FRI *)` ejecuta la tarea a las 09:00 todos los lunes, martes, miércoles, jueves y viernes. Para más información, consulte Expresiones Cron y de frecuencia para periodos de mantenimiento en la documentación de Systems Manager.
- Familiaridad con Systems Manager.
- Permisos para iniciar y detener la instancia de RDS. Para más información, consulte la sección Epics.

Limitaciones

- Una instancia de base de datos de Amazon RDS se puede detener durante un máximo de siete días a la vez. Transcurridos siete días, la instancia de la base de datos se reinicia automáticamente para garantizar que reciba las actualizaciones de mantenimiento necesarias.
- No puede detener una instancia de base de datos que tenga una réplica de lectura o que sea una réplica de lectura.
- No puede detener una instancia de base de datos de Amazon RDS para SQL Server que esté en una configuración Multi-AZ.
- Service quotas se aplican a Maintenance Windows y Systems Manager Automation. Para obtener más información sobre las cuotas de servicio, consulte AWS Systems Manager los puntos finales y las cuotas en la Referencia general de AWS documentación.
- Algunas Servicios de AWS no están disponibles en todos Regiones de AWS. Para conocer la disponibilidad de las regiones, consulte Servicios de AWS by Region. Para los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

El siguiente diagrama muestra el flujo de trabajo para detener e iniciar automáticamente una instancia de base de datos de Amazon RDS.

El flujo de trabajo tiene los siguientes pasos:

1. Cree un período de mantenimiento y utilice expresiones cron para definir el cronograma de parada e inicio de sus instancias de la base de datos de Amazon RDS.

2. Registre una tarea de automatización de Systems Manager en el periodo de mantenimiento mediante el manual de procedimientos `AWS-StopRdsInstance` o `AWS-StartRdsInstance`.

3. Registre un objetivo en el periodo de mantenimiento mediante un grupo de recursos basado en etiquetas para sus instancias de la base de datos de Amazon RDS.

Pila de tecnología

- AWS CloudFormation
- AWS Identity and Access Management (YO SOY)
- Amazon RDS
- Systems Manager

Automatizar y escalar

Puede detener e iniciar varias instancias de la base de datos de Amazon RDS al mismo tiempo etiquetando las instancias de la base de datos de Amazon RDS necesarias, creando un grupo de recursos que incluya todas las instancias de la base de datos etiquetadas y registrando este grupo de recursos como destino para el período de mantenimiento.

Tools (Herramientas)

- AWS CloudFormationes un servicio que le ayuda a modelar y configurar sus AWS recursos.
- AWS Identity and Access Management (IAM) es un servicio web que le ayuda a controlar de forma segura el acceso a AWS los recursos.
- Amazon Relational Database Service (Amazon RDS) es un servicio web que facilita la configuración, la operación y la escala de una base de datos relacional en Nube de AWS.
- Grupos de recursos de AWSle ayuda a organizar AWS los recursos en grupos, etiquetarlos y gestionar, supervisar y automatizar las tareas en los recursos agrupados.
- AWS Systems Manageres una Servicio de AWS que puede utilizar para ver y controlar su infraestructura AWS. Este patrón utiliza las siguientes características de Systems Manager:
  - AWS Systems Manager La automatización simplifica las tareas comunes de mantenimiento e implementación de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) y otros AWS recursos.
  - AWS Systems Manager Maintenance Windows le ayuda a definir un cronograma para realizar acciones potencialmente disruptivas en sus instancias.

Epics

Crear y configurar el rol de servicio IAM para Systems Manager Automation

Tarea	Descripción	Habilidades requeridas
Configure el rol de servicio de IAM para Systems Manager Automation.	Inicie sesión Consola de administración de AWS y cree un rol de servicio para Systems Manager Automatio n. Puede usar uno de los dos métodos siguientes para crear este rol de servicio: • Se utiliza AWS CloudForm ation para configurar un rol de servicio para Systems Manager Automation • Uso de IAM a fin de configurar roles para Systems Manager Automation El flujo de trabajo de Systems Manager Automation invoca a Amazon RDS mediante un rol de servicio para realizar acciones de inicio y detención en la instancia de la base de datos de Amazon RDS. El rol de servicio debe configurarse con la siguiente política en línea que tenga permisos para iniciar y detener la instancia de la base de datos de Amazon RDS:	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	<pre>{
	    "Version":
	"2012-10-17",
	    "Statement": [
	        {
	            "Sid":
	"RdsStartStop",
	            "Effect":
	"Allow",
	            "Action": [
	
	"rds:StopDBInstance",
	
	"rds:StartDBInstance"
	            ],
	            "Resource":
	"<RDS_Instance_ARN>"
	
	        },
	        {
	            "Sid":
	"RdsDescribe",
	            "Effect":
	"Allow",
	            "Action":
	"rds:DescribeDBIns
	tances",
	            "Resource":
	"*"
	        }
	    ]
	}</pre> Asegúrese de reemplazar `<RDS_Instance_ARN>` por el nombre de recurso de Amazon (ARN) de la instancia de la base de datos de Amazon RDS.	

Tarea	Descripción	Habilidades requeridas
	Si no está familiarizado con el uso de las políticas y roles de IAM, siga las instrucciones de la sección Solution Overview de la entrada en el blog Schedule Amazon RDS stop and start using AWS Systems Manager. **Important** Asegúrese de registrar el ARN del rol de servicio.	

Crear un grupo de recursos

Tarea	Descripción	Habilidades requeridas
Etiquete las instancias de base de datos de Amazon RDS.	Abra la consola de Amazon RDS y etiquete las instancias de la base de datos de Amazon RDS que desee añadir al grupo de recursos. Una etiqueta es un metadato asignado a un AWS recurso y consta de un par clave-valor. Le recomendamos que utilice Acción como clave de etiqueta y StartStopcomo valor. Para obtener más información al respecto, consulte Cómo añadir, publicar y eliminar	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	etiquetas en la documentación de Amazon RDS.	
Cree un grupo de recursos para las instancias de la base de datos de Amazon RDS etiquetadas.	Abra la consola de Grupos de recursos de AWS y cree un grupo de recursos basado en la etiqueta que creó para las instancias de la base de datos de Amazon RDS. En Criterios de agrupació n, asegúrese de elegir AWS: :RDS:: DBInstance para el tipo de recurso y, a continuación, proporcione el par clave-valor de la etiqueta (por ejemplo, «Action-»). StartStop Esto garantiza que el servicio solo compruebe las instancias de la base de datos de Amazon RDS y no otros recursos que tengan esta etiqueta. Asegúrese de registrar el nombre del grupo de recursos. Para obtener más información y pasos detallados, consulte Crear una consulta basada en etiquetas y crear un grupo en la documentación. Grupos de recursos de AWS	Administrador de AWS

Configure un período de mantenimiento para detener las instancias de la base de datos de Amazon RDS

Tarea	Descripción	Habilidades requeridas
Crear un período de mantenimiento.	1. Abra la consola de Systems Manager, elija Maintenance Windows y, a continuación, elija Crear un periodo de mantenimiento. Proporcione un nombre para el período de mantenimiento (por ejemplo, "StopRdsInstance«), introduzca una descripción y, a continuación, desactive la casilla Permitir objetivos no registrados. 2. Elija la expresión CRON/Expresión de frecuencia y proporcione la expresión de programación para definir cuándo deben detenerse las instancias de la base de datos de Amazon RDS. Introduzca 1 para la duración y 0 para dejar de iniciar las tareas. De forma predeterminada, la zona horaria muestra UTC. Puede cambiar la zona horaria para iniciar el período de mantenimiento en función de la marca de tiempo definida en su expresión cron.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	3. Elija Create maintenance window (Crear periodo de mantenimiento). El sistema vuelve a la página del periodo de mantenimiento y el estado del periodo de mantenimiento es Habilitado. **Important** La tarea para detener la instancia de la base de datos se ejecuta casi al instante cuando se inicia y no abarca todo el periodo de mantenimiento. Este patrón proporciona los valores mínimos de duración y parada de las tareas de inicio, ya que son los parámetros necesarios para un período de mantenimiento. Para obtener más información y ver los pasos detallados, consulte Crear un periodo mantenimiento (consola) en la documentación de Systems Manager.	

Tarea	Descripción	Habilidades requeridas
Asigne un objetivo al periodo de mantenimiento.	1. En la consola de Systems Manager, elija Maintenance Windows, Acciones y, a continuación, Registrar destinos. 2. En el área Objetivos, especifique Elegir un grupo de recursos y, a continuación, elija el nombre de un grupo de recursos existente en su cuenta. 3. Para los tipos de recursos, elija AWS: :RDS:: DBInstance y, a continuación, elija Register target. Para obtener más información y ver los pasos detallados, consulte Asignar destinos a un periodo de mantenimiento (consola) en la documentación de Systems Manager.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Asigne una tarea al periodo de mantenimiento.	1. En la consola de Systems Manager, elija Maintenance Windows y, a continuación, elija su periodo de mantenimiento. Elija Acciones y después seleccione Registrar tarea de automatización. 2. En Document, elija AWS-StopRdsInstance. 3. En la sección Destinos, elija Seleccionar grupos de destinos registrados y, a continuación, elija el destino del periodo de mantenimiento que registró en el periodo de mantenimiento actual. 4. En Control de velocidad, especifique el 100 % para Simultaneidad y Umbral de error. Puede cambiar los valores de Control de velocidad según sus requisitos para la simultaneidad de tareas y el umbral de error. Para más información al respecto, consulte Acerca de los umbrales de error y simultaneidad en la documentación de Systems Manager.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	5. En la sección Rol de servicio de IAM, en Rol de servicio, deje esta casilla en blanco o cree su propio rol personalizado. Si deja la casilla en blanco, Systems Manager crea automáticamente el rol AWSServiceRoleForAmazonSSM vinculado al servicio y, a continuación, lo asocia a la tarea. Para crear su propio rol personalizado, consulte Crear un rol de servicio personalizado para los periodos de mantenimiento (consola) y, a continuación, asocie ese rol personalizado a la tarea. 6. En la sección Parámetros a introducir, especifique los siguientes parámetros para el manual de procedimientos: • InstanceId: `{{RESOURCE_ID}}` **Note** Para InstanceIdello, se utiliza un pseudoparámetro para extraer el ID de recurso de base de datos	

Tarea	Descripción	Habilidades requeridas
	de Amazon RDS del ARN. Para obtener más información sobre los pseudopar ámetros, consulte Acerca de los pseudopar ámetros en la documentación de Systems Manager. • AutomationAssumeRole: proporcione el ARN del rol de servicio que creó para Systems Manager Automation. 7. Seleccione Registrar tarea de Automation **Important** La opción Rol de servicio define el rol de servicio necesario para que el periodo de mantenimiento ejecute las tareas. Sin embargo, este rol no es idéntico al rol de servicio que creó anteriormente para	

Tarea	Descripción	Habilidades requeridas
	Systems Manager Automation. Para obtener más información y ver los pasos detallados, consulte Asignar tareas a un periodo de mantenimiento (consola) en la documentación de Systems Manager.	

Configurar un período de mantenimiento para iniciar las instancias de la base de datos de Amazon RDS

Tarea	Descripción	Habilidades requeridas
Configure un período de mantenimiento para iniciar las instancias de la base de datos de Amazon RDS.	Repita los pasos de la épica Configurar un período de mantenimiento para detener las instancias de la base de datos de Amazon RDS y configure otro período de mantenimiento para iniciar las instancias de la base de datos de Amazon RDS a una hora programada. **Important** Debe realizar los siguientes cambios al configurar el periodo de mantenimiento para iniciar las	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	instancias de la base de datos: • Utilice un nombre nuevo para la ventana de mantenimiento (por ejemplo, "StartRdsInstance«). • Sustituya la expresión cron por la expresión cron que desee utilizar para iniciar las instancias de la base de datos. • Sustituya el manual de procedimientos de `AWS-StopRdsInstance` por `AWS-StartRdsInstance` en Tarea.	

Recursos relacionados

- Utilice los documentos de automatización de Systems Manager para gestionar las instancias y reducir los costes fuera del horario laboral (entrada AWS del blog)

Centralización de la distribución de paquetes de software en AWS Organizations mediante Terraform

Pradip kumar Pandey, Chintamani Aphale, T.V.R.L.Phani Kumar Dadi, Pratap Kumar Nanda, Aarti Rajput y Mayuri Shinde, Amazon Web Services

Resumen

Las empresas suelen mantener varias Cuentas de AWS distribuidas Regiones de AWS en varias para crear una sólida barrera de aislamiento entre las cargas de trabajo. Para garantizar la seguridad y la conformidad, sus equipos de administración instalan herramientas basadas en agentes CrowdStrike, como, o TrendMicroherramientas para el análisis de seguridad SentinelOne, y el agente de Amazon, el CloudWatch agente de Datadog o AppDynamics los agentes para la supervisión. Estos equipos suelen enfrentarse a desafíos cuando quieren automatizar de forma centralizada la administración y distribución de paquetes de software en este entorno tan amplio.

Distributor, una capacidad de AWS Systems Manager, automatiza el proceso de empaquetado y publicación de software en instancias administradas de Microsoft Windows y Linux en la nube y en los servidores en las instalaciones a través de una única interfaz simplificada. Este patrón demuestra cómo puede utilizar Terraform para simplificar aún más el proceso de administración de la instalación del software y ejecutar scripts en un gran número de instancias y cuentas de miembros con un mínimo esfuerzo. AWS Organizations

Esta solución funciona para instancias de Amazon, Linux y Windows administradas por Systems Manager.

Requisitos previos y limitaciones

- Un paquete de Distributor que incluye el software que se va a instalar
- La versión 0.15.0 o posterior de Terraform
- Instancias de Amazon Elastic Compute Cloud (Amazon EC2) administradas por Systems Manager y con permisos básicos para acceder a Amazon Simple Storage Service (Amazon S3) en la cuenta de destino
- Una zona de aterrizaje para su organización que se configura mediante AWS Control Tower
- (Opcional) Generador de cuentas paraTerraform (AFT)

Arquitectura

Detalles del recurso

Este patrón usa Account Factory for Terraform (AFT) para crear todos los AWS recursos necesarios y la canalización de código para implementar los recursos en una cuenta de implementación. La canalización de código se ejecuta en dos repositorios:

- La personalización global contiene el código de Terraform que se aplicará a todas las cuentas registradas en AFT.
- Las personalizaciones de la cuenta contienen el código de Terraform que se ejecutará en la cuenta de implementación.

También puede implementar esta solución sin usar AFT; para ello, ejecute los comandos de Terraform en la carpeta de personalizaciones de la cuenta.

El código de Terraform implementa los siguientes recursos:

- AWS Identity and Access Management Función y políticas (IAM)
  - SystemsManager- AutomationExecutionRole concede al usuario permisos para ejecutar automatizaciones en las cuentas de destino.
  - SystemsManager- AutomationAdministrationRole concede al usuario permisos para ejecutar automatizaciones en varias cuentas y unidades organizativas ()OUs.
- Archivos comprimidos y manifest.json para el paquete
  - En Systems Manager, un paquete incluye al menos un archivo .zip de software o activos instalables.
  - El manifiesto de JSON incluye indicadores a los archivos de código del paquete.
- Bucket de S3
  - Los paquetes distribuidos que se comparten entre la organización se almacenan de forma segura en un bucket de Amazon S3.
- AWS Systems Manager documentos (documentos SSM)
  - `DistributeSoftwarePackage` contiene la lógica para distribuir el paquete de software a todas las instancias de destino de las cuentas de miembros.
  - `AddSoftwarePackageToDistributor`contiene la lógica para empaquetar los activos de software instalables y añadirlos a la automatización, una capacidad de. AWS Systems Manager
- Asociación de de Systems Manager

- Se utiliza una asociación de Systems Manager para implementar la solución.

Arquitectura y flujo de trabajo

El siguiente diagrama muestra los siguientes pasos:

1. Para ejecutar la solución desde una cuenta centralizada, debe cargar sus paquetes o software junto con los pasos de implementación en un bucket de S3.
2. El paquete personalizado estará disponible en la sección Documentos de la consola de Systems Manager, en la pestaña De mi propiedad.
3. State Manager, una función de Systems Manager, crea, programa y ejecuta una asociación del paquete en toda la organización. La asociación especifica que el paquete de software debe estar instalado y ejecutándose en un nodo administrado para poder instalarse en el nodo de destino.
4. La asociación indica a Systems Manager que instale el paquete en el nodo de destino.
5. Para cualquier instalación o cambio posterior, los usuarios pueden ejecutar la misma asociación de forma periódica o manual desde una única ubicación para realizar implementaciones en todas las cuentas.
6. En las cuentas de miembros, Automation envía los comandos de implementación a Distributor.
7. Distributor reparte los paquetes de software en todas las instancias.

Esta solución utiliza la cuenta de administración que AWS Organizations contiene, pero también puede designar una cuenta (administrador delegado) para que la gestione en nombre de la organización.

Tools (Herramientas)

Servicios de AWS

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos. Este patrón utiliza Amazon S3 para centralizar y almacenar de forma segura el paquete distribuido.
- AWS Systems Manager lo ayuda a administrar las aplicaciones y la infraestructura que se ejecutan en la Nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo necesario para detectar y resolver problemas operativos y le ayuda a administrar sus AWS

recursos de forma segura y a escala. Este patrón utiliza las siguientes capacidades de Systems Manager:

  - Distributor lo ayuda a empaquetar y publicar el software en nodos administrados de Systems Manager.
  - La automatización simplifica las tareas habituales de mantenimiento, implementación y corrección de muchos servicios. AWS
  - Documents realiza acciones en las instancias gestionadas por Systems Manager en toda la organización y las cuentas.
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar varias AWS cuentas en una organización que puede crear y administrar de forma centralizada.

Otras herramientas

- Terraform es una herramienta de infraestructura como código (iAC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.

Repositorio de código

Las instrucciones y el código de este patrón están disponibles en el repositorio GitHub centralizado de distribución de paquetes.

Prácticas recomendadas

- Para asignar etiquetas a una asociación, use AWS Command Line Interface (AWS CLI) o Herramientas de AWS para PowerShell. No se admite agregar etiquetas a una asociación mediante la consola de Systems Manager. Para obtener más información, consulte Etiquetado de recursos de Systems Manager en la documentación de Systems Manager.
- Para ejecutar una asociación con una versión nueva de un documento compartido desde otra cuenta, debe establecer la versión del documento en `default`.
- Para etiquetar solo el nodo de destino, utilice una clave de etiqueta. Si quiere dirigir los nodos mediante varias claves de etiqueta, utilice la opción de grupo de recursos.

Epics

Configuración de las cuentas y los archivos de origen

Tarea	Descripción	Habilidades requeridas

Clonar el repositorio.	1. Clona el repositorio GitHub centralizado de distribución de paquetes:
	`git clone https://github.com/aws-samples/aws-organization-centralised-package-distribution`
	2. El repositorio de código de Terraform requiere dos carpetas de personalización administradas por AFT. Confirme que la copia local del repositorio contiene esas carpetas:
	`$ cd centralised-package-distribution`
	`$ ls`
	`global-customization account-customization`
		DevOps ingeniero

Actualice las variables globales.	En el archivo `global-customization/variables.tf` , actualice los siguientes parámetros de entrada: Estas variables se aplican a todas las cuentas creadas y administradas por AFT.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• `account_id` : ID de la cuenta donde se implement ará la solución Distributor. • `aws_region` : El Región de AWS lugar donde se desplegará la asociación.	
Actualice las variables de la cuenta.	En el archivo `account-c ustomization/varia bles.tf` , actualice los siguientes parámetros de entrada: Estas variables se aplican únicamente a cuentas creadas y administradas específicamente por AFT. • `package_bucket_nam e` : nombre del bucket de S3 que contiene el archivo de distribución de paquetes. • `package_name` : nombre del archivo de distribución de paquetes. • `package_version` : versión del paquete del instalador.	DevOps ingeniero

Personalización de los parámetros y los archivos de implementación

Tarea	Descripción	Habilidades requeridas
Actualice los parámetros de entrada de la asociación de State Manager.	Actualice los siguientes parámetros de entrada del archivo `account-`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	`customization/association.tf` para definir el estado que desea mantener en las instancias. Puede utilizar los valores de parámetros predeterminados si admiten su caso de uso.
	• `targetAccounts` : la unidad organizativa (OU) de IDs AWS Organizations que representa las cuentas con las instancias de destino para su distribución. OU IDs comienza con «tú».
	• `targetRegions` : El Regiones de AWS (por ejemplo, «us-east-1″ o «ap-southeast-2") donde se ejecutan las instancias de destino.
	• `action`: especifique si desea instalar o desinstalar el paquete.
	• `installationType` : uno de los siguientes tipos de instalación:
	  • `uninstall` : el paquete está desinstalado.
	  • `reinstall` : la aplicación se desconecta hasta que se complete el proceso de reinstalación.	

Tarea	Descripción	Habilidades requeridas
	• `In-place update`: la aplicación está disponibl e mientras se añaden archivos nuevos o actualizados a la instalaci ón. • `name`: el nombre del paquete que se va a instalar o desinstalar. • `version`: la versión del paquete que se va a instalar o desinstalar. Si no hay instalada ninguna versión del paquete, el sistema devuelve un error. • `bucketName` : el nombre del bucket de S3 en el que se implementó el paquete. Este bucket debe estar formado únicamente por los paquetes y el archivo de manifiesto. • `bucketPrefix` : el prefijo de S3 donde se almacenan los activos del paquete. • `AutomationAssumeRo le` : nombre de recurso de Amazon (ARN) de `SystemsManager-Aut omationAdministrat ionRole` .	

Tarea	Descripción	Habilidades requeridas
Prepare los archivos comprimidos y el archivo `manifest.json` para el paquete.	Este patrón proporciona ejemplos de archivos PowerShell instalables (.msi para Windows y .rpm para Linux) con scripts de instalación y desinstalación en la carpeta. `account-customization/package` 1. Sustituya los archivos PowerShell instalables por sus propios archivos o proporcione el archivo instalable, los scripts de instalación y desinstalación y el archivo de manifiesto para crear un paquete en la carpeta de su cuenta. `account-customization` 2. Personalice el archivo `manifest.json` predeterminado que Terraform genera en la carpeta `account-customization` según sus necesidades.	DevOps ingeniero

Ejecución de los comandos de Terraform para aprovisionar recursos

Tarea	Descripción	Habilidades requeridas

Inicialice la configuración de Terraform.	Para implementar la solución automáticamente con AFT, inserte el código en AWS CodeCommit:
	`$ git add *`
	`$ git commit -m "message"`
	`$ git push`
	También puede implement ar esta solución sin usar AFT; para ello, ejecute un comando de Terraform de la carpeta `account-customization` . Para inicializar el directorio de trabajo que contiene los archivos Terraform, ejecute:
	`$ terraform init`
		DevOps ingeniero

Previsualice los cambios.	Para obtener una vista previa de los cambios que Terraform realizará en la infraestructura, ejecute el comando: `$ terraform plan` Este comando evalúa la configuración de Terraform para determinar el estado deseado de los recursos que	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	se han declarado. También compara el estado deseado con la infraestructura real que se va a aprovisionar en el espacio de trabajo.	
Aplique los cambios.	Ejecute el siguiente comando para implementar los cambios que realizó en los archivos `variables.tf` : `$ terraform apply`	DevOps ingeniero

Valide los recursos

Tarea	Descripción	Habilidades requeridas
Valide la creación de documentos SSM.	1. En el panel de navegación izquierdo de la consola de Systems Manager, elija Documentos. 2. Elija la pestaña De mi propiedad. Debería ver los paquetes `DistributeSoftwarePackage` y `AddSoftwarePackageToDistributor` .	DevOps ingeniero
Valide la implementación correcta de las automatizaciones.	1. En el panel de navegación izquierdo de la consola de Systems Manager, elija Automation.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	2. En la lista de ejecuciones de Automation, debería ver las implementaciones más recientes `DistributeSoftwarePackage` y `AddSoftwarePackageToDistributor`. 3. Elija el ID de ejecución para comprobar que se han completado correctamente.	
Compruebe que el paquete se haya implementado en las instancias de cuentas de miembros de destino.	1. En el panel de navegación de la consola de Systems Manager, elija Ejecutar comando. 2. En el historial de comandos, verá cada invocación y su estado. 3. Elija cualquier ID de comando para ver el historial de implementación de cada instancia de destino. 4. Elija el ID de instancia y consulte la sección de resultados para ver la distribución.	DevOps ingeniero

Resolución de problemas

Problema	Solución
La asociación de State Manager ha devuelto un error o se encuentra en estado pendiente.	Consulte la información de solución de problemas en el Centro de AWS conocimiento.
No se pudo ejecutar una asociación programada.	Es posible que la especificación de su programación no sea válida. Actualmente, State Manager no permite especificar meses en expresiones cron para asociaciones. Utilice expresiones de frecuencia o cron para confirmar la programación.

Recursos relacionados

- Distribución centralizada de paquetes (GitHub repositorio)
- Generador de cuentas para Terraform (AFT)
- Casos de uso y mejores prácticas (AWS Systems Manager documentación)

Configure el registro para las aplicaciones.NET en Amazon CloudWatch Logs mediante NLog

Bibhuti Sahu y Rob Hill (AWS), Amazon Web Services

Resumen

Este patrón describe cómo utilizar el marco de registro de NLog código abierto para registrar el uso y los eventos de las aplicaciones.NET en Amazon CloudWatch Logs. En la CloudWatch consola, puede ver los mensajes de registro de la aplicación prácticamente en tiempo real. También puede configurar métricas y alarmas para recibir notificaciones en caso de que se superen los umbrales de métrica. Con CloudWatch Application Insights, puede ver paneles automatizados o personalizados que muestran los posibles problemas de las aplicaciones monitoreadas. CloudWatch Application Insights está diseñado para ayudarlo a identificar rápidamente los problemas actuales de sus aplicaciones e infraestructura.

Para escribir mensajes de registro en CloudWatch Logs, agregue el `AWS.Logger.NLog` NuGet paquete al proyecto.NET. A continuación, actualiza el `NLog.config` archivo para usar CloudWatch Logs como destino.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una aplicación web o de consola .NET que:
  - Use versiones compatibles de .NET Framework o .NET Core. Para obtener más información, consulte Versiones de producto.
  - Se utiliza NLog para enviar datos de registro a Application Insights.
- Permisos para crear un rol de IAM para un servicio de AWS. Para obtener más información, consulte Permisos de roles de servicios.
- Permisos para transferir un rol a un servicio de AWS. Para obtener más información, consulte Concesión de permisos a un usuario para transferir un rol a un servicio de AWS.

Versiones de producto

- .NET Framework versión 3.5 o posterior

- .NET Core versiones 1.0.1, 2.0.0 o posterior

Arquitectura

Pila de tecnología de destino

- NLog
- Amazon CloudWatch Logs

Arquitectura de destino

1. La aplicación.NET escribe los datos de registro en el marco de NLog registro.
2. NLog escribe los datos de registro en CloudWatch Logs.
3. Se utilizan CloudWatch alarmas y paneles personalizados para supervisar la aplicación.NET.

Tools (Herramientas)

Servicios de AWS

- Amazon CloudWatch Application Insights le ayuda a observar el estado de sus aplicaciones y los recursos de AWS subyacentes.
- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas, aplicaciones y servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- Las herramientas de AWS PowerShell son un conjunto de PowerShell módulos que le ayudan a programar operaciones en sus recursos de AWS desde la línea de PowerShell comandos.

Otras herramientas

- Registrador. NLoges un NLog objetivo que registra datos de registro en CloudWatch Logs.
- NLoges un marco de registro de código abierto para plataformas .NET que le ayuda a escribir datos de registro en destinos, como bases de datos, archivos de registro o consolas.

- PowerShelles un programa de administración de automatización y configuración de Microsoft que se ejecuta en Windows, Linux y macOS.
- Visual Studio es un entorno de desarrollo integrado (IDE) que incluye compiladores, herramientas de finalización de código, diseñadores gráficos y otras características que facilitan el desarrollo de software.

Prácticas recomendadas

- Establezca una política de retención para el grupo de registro de destino. Esto debe hacerse fuera de la NLog configuración. De forma predeterminada, los datos de registro se almacenan en CloudWatch los registros de forma indefinida.
- Respete las Prácticas recomendadas para administrar las claves de acceso de AWS.

Epics

Configure el acceso y las herramientas

Tarea	Descripción	Habilidades requeridas
Cree una política de IAM.	Siga las instrucciones indicadas en Crear políticas mediante el editor JSON, en la documentación de IAM. Introduce la siguiente política de JSON, que tiene los permisos de privilegios mínimos necesarios para permitir que CloudWatch Logs lea y escriba registros. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow",`	Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	"Action": ["logs:CreateLogGroup", "logs:CreateLogStream", "logs:GetLogEvents", "logs:PutLogEvents", "logs:DescribeLogGroups", "logs:DescribeLogStreams", "logs:PutRetentionPolicy"], "Resource": ["*"] }] }	
Crear un rol de IAM.	Para obtener instrucciones, consulte Creating a Role to Delegate Permissions to an AWS Service en la documentación de IAM. Seleccione la política que creó previamente. Esta es la función que asume CloudWatch Logs para realizar las acciones de registro.	Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Configure las herramientas de AWS para PowerShell.	1. Siga las instrucciones para su sistema operativo que aparecen en Instalación de las herramientas de AWS para PowerShell. 2. Utilice las herramientas de AWS para PowerShell cmdlets para almacenar la clave de acceso y la clave secreta en un perfil. Para obtener instrucciones, consulte Administración de perfiles en las herramientas de AWS para ver PowerShell la documentación.	AWS general

Configuración NLog

Tarea	Descripción	Habilidades requeridas
Instale el NuGet paquete.	1. En Visual Studio, seleccione Archivo y, a continuación, elija Abrir un proyecto o solución. 2. Elija el proyecto en el que desee instalarlo NLog. 3. En Visual Studio, elija Tools, NuGet Package Manager, Package Manager Console. 4. Instale el `AWS.Logger.NLog` NuGet paquete	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	introduciendo el siguiente comando. `Install-Package AWS.Logger.NLog -Version 3.1.0`	

Tarea	Descripción	Habilidades requeridas
Configure el destino de registro.	1. Abra el archivo `NLog.config` . 2. Para el destino `type`, introduzca `AWSTarget` . 3. Para el destino `logGroup`, escriba el nombre del grupo de registro que desea usar. Si el grupo de registro no existe aún, se creará automáticamente un nuevo grupo de registro con el nombre proporcionado. 4. Para el destino`region`, introduzca la región de AWS en la que está configurado CloudWatch Logs. 5. Para el destino `profile`, introduzca el nombre del perfil que creó anteriorm ente para almacenar la clave de acceso y la clave secreta. 6. Guarde y cierre el archivo `NLog.config` . Para obtener una copia de este archivo de configuración, consulte la sección Informaci ón adicional de este patrón. Cuando ejecute la aplicación, NLog escribirá los mensajes	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	de registro y los enviará a CloudWatch Logs.	

Valide y supervise los registros

Tarea	Descripción	Habilidades requeridas
Valide el registro.	Sigue las instrucciones de la documentación sobre cómo ver los datos de registro enviados a CloudWatch CloudWatch Logs. Compruebe que los eventos de registro de la aplicación .NET se estén registrando. Si no constan eventos de registro, consulte la sección Solución de problemas de este patrón.	AWS general
Supervise la pila de la aplicación .NET.	Configure la supervisión CloudWatch según sea necesario para su caso de uso. Puede utilizar CloudWatch Logs Insights, CloudWatch Metrics Insights y CloudWatch Application Insights para supervisar su carga de trabajo de.NET. También puede configurar alarmas para recibir alertas y crear un panel personalizado para supervisar la carga de trabajo desde una vista única.	AWS general

Resolución de problemas

Problema	Solución
Los datos de registro no aparecen en CloudWatch los registros.	Asegúrese de que la política de IAM esté asociada a la función de IAM que asume CloudWatch Logs. Para obtener más instrucciones, consulte la sección Configurar el acceso y las herramientas de la sección Épica.

Recursos relacionados

- Trabajar con grupos de registros y flujos de CloudWatch registros (documentación de registros)
- Amazon CloudWatch Logs y .NET Logging Frameworks (entrada del blog de AWS)

Información adicional

A continuación se muestra un archivo de muestra `NLog.config`.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <configSections>
    <section name="nlog" type="NLog.Config.ConfigSectionHandler, NLog" />
  </configSections>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.7.2" />
  </startup>
  <nlog>
    <extensions>
      <add assembly="NLog.AWS.Logger" />
    </extensions>
    <targets>
      <target name="aws" type="AWSTarget" logGroup="NLog.TestGroup" region="us-east-1"
 profile="demo"/>
    </targets>
    <rules>
      <logger name="*" minlevel="Info" writeTo="aws" />
    </rules>
  </nlog>
```

```
</configuration>
```

Copiar los productos de AWS Service Catalog en diferentes cuentas y regiones de AWS

Sachin Vighe y Santosh Kale, Amazon Web Services

Resumen

AWS Service Catalog es un servicio regional, lo que significa que las carteras y los productos de AWS Service Catalog solo están visibles en la región de AWS en la que se crearon. Si configura un centro de AWS Service Catalog en una nueva región, debe volver a crear sus productos existentes, lo que puede llevar mucho tiempo.

El enfoque de este patrón ayuda a simplificar este proceso al describir cómo copiar productos de un centro de AWS Service Catalog de una cuenta o región de AWS de origen a un nuevo centro de una cuenta o región de destino. Para obtener más información sobre el modelo hub and spoke de AWS Service Catalog, consulte AWS Service Catalog hub and spoke model: How to automate the deployment and management of AWS Service Catalog to many accounts en el blog AWS Management and Governance.

El patrón también proporciona los paquetes de códigos independientes necesarios para copiar los productos de AWS Service Catalog entre cuentas o a otras regiones. Al utilizar este patrón, su organización puede ahorrar tiempo, hacer que las versiones actuales y anteriores del producto estén disponibles en un nuevo centro de AWS Service Catalog, minimizar el riesgo de errores manuales y escalar el enfoque a varias cuentas o regiones.

> **Note**
>
> La sección Epics de este patrón ofrece dos opciones para copiar productos. Puede usar la opción 1 para copiar productos entre cuentas o elegir la opción 2 para copiar productos entre regiones.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Productos de AWS Service Catalog existentes en una cuenta o región de origen.
- Un centro de AWS Service Catalog existente en una cuenta o región de destino.

- Si desea copiar productos entre cuentas, debe compartir e importar la cartera de AWS Service Catalog que contiene los productos a su cuenta de destino. Para obtener más información al respecto, consulte Compartir e importar carteras en la documentación del AWS Service Catalog.

Limitaciones

- Los productos de AWS Service Catalog que desee copiar entre regiones o cuentas no pueden pertenecer a más de una cartera.

Arquitectura

En el siguiente diagrama se muestra la copia de los productos de AWS Service Catalog de una cuenta de origen a una cuenta de destino.

El siguiente diagrama muestra la copia de productos de AWS Service Catalog de una región de origen a una región de destino.

Pila de tecnología

- Amazon CloudWatch
- AWS Identity y Access Management (IAM)
- AWS Lambda
- AWS Service Catalog

Automatizar y escalar

Puede escalar el enfoque de este patrón mediante una función de Lambda que se puede escalar en función del número de solicitudes recibidas o del número de productos de AWS Service Catalog que necesite copiar. Para obtener más información al respecto, consulte el escalado de funciones de Lambda en la documentación de AWS Lambda.

Tools (Herramientas)

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Service Catalog le ayuda a administrar de forma centralizada los catálogos de servicios de TI aprobados para AWS. Los usuarios finales pueden implementar rápidamente solo los servicios de TI aprobados que necesitan, de acuerdo con las limitaciones establecidas por su organización.

Código

Puede usar el paquete (adjunto) `cross-account-copy` para copiar los productos de AWS Service Catalog entre cuentas o el paquete (adjunto) `cross-region-copy` para copiar productos entre regiones.

El paquete `cross-account-copy` contiene los siguientes archivos:

- `copyconf.properties`: el archivo de configuración que contiene los parámetros de región e ID de cuenta de AWS para copiar productos entre cuentas.
- `scProductCopyLambda.py`: la función de Python para copiar productos entre cuentas.
- `createDestAccountRole.sh`: el script para crear un rol de IAM en la cuenta de destino.
- `createSrcAccountRole.sh`: el script para crear un rol de IAM en la cuenta de origen.
- `copyProduct.sh`: el script para crear e invocar la función de Lambda para copiar productos entre cuentas.

El paquete `cross-region-copy` contiene los siguientes archivos:

- `copyconf.properties`: el archivo de configuración que contiene los parámetros de región e ID de cuenta de AWS para copiar productos entre regiones.
- `scProductCopyLambda.py`: la función Python para copiar productos entre regiones.
- `copyProduct.sh`: el script para crear un rol de IAM y crear e invocar la función de Lambda para copiar productos entre regiones.

Epics

Opción 1: copiar los productos de AWS Service Catalog en todas las cuentas

Tarea	Descripción	Habilidades requeridas
Actualizar el archivo de configuración.	1. Descargue el paquete (adjunto) `cross-account-copy` en su máquina local. 2. Actualice el archivo de `copyconf.properties` configuración con los siguientes valores: • `srcRegion` : proporcione la región de origen que contiene los productos. • `destRegion` : indique la región de destino de los productos. • `sourceAccountId` : proporcione el ID de cuenta de AWS de su cuenta de origen. • `destAccountId` : proporcione el ID de cuenta de AWS de su cuenta de destino.	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube
Configure sus credenciales para la AWS CLI en la cuenta de destino.	Configure sus credenciales para acceder a la AWS CLI en su cuenta de destino ejecutando el `aws configure` comando y	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube

Tarea	Descripción	Habilidades requeridas

	proporcionando los siguientes valores:
	
	`$aws configure`
	`AWS Access Key ID`
	` [None]: <your_acc`
	`ess_key_id>`
	`AWS Secret Access Key`
	` [None]: <your_sec`
	`ret_access_key>`
	`Default region name`
	` [None]: Region`
	`Default output format`
	` [None]:`
	
	Para obtener más informaci ón al respecto, consulte Conceptos básicos de configuración en la interfaz de la línea de comandos de AWS.	

Tarea	Descripción	Habilidades requeridas

Configure sus credenciales para la AWS CLI en la cuenta de origen.	Configure sus credencia les para acceder a la AWS CLI en su cuenta de origen ejecutando el comando `aws configure` y proporcio nando los siguientes valores:
	`$aws configure`
	`AWS Access Key ID [None]: <your_access_key_id>`
	`AWS Secret Access Key [None]: <your_secret_access_key>`
	`Default region name [None]: Region`
	`Default output format [None]:`
	Para obtener más informaci ón al respecto, consulte Conceptos básicos de configuración en la interfaz de la línea de comandos de AWS.
		Administrador de AWS, administrador de sistemas de AWS, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree un rol de ejecución para Lambda en su cuenta de destino.	Ejecute el script `createDestAccountRole.sh` en su cuenta de destino. El script implementa las siguientes acciones: • Crea un rol de ejecución para Lambda en la cuenta de destino • Crea y adjunta la política de IAM para la función de ejecución de Lambda	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube
Cree el rol de IAM multicuenta en su cuenta de origen.	Ejecute el script `createSrcAccountRole.sh` en su cuenta de origen. El script implementa las siguientes acciones: • Crea un rol de IAM multicuenta en la cuenta de origen que asume la función de ejecución de Lambda en la cuenta de destino para copiar productos • Crea y adjunta una política de IAM para la función multicuenta en su cuenta de origen	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Ejecute el script CopyProduct en la cuenta de destino.	Ejecute el script `copyProduct.sh` en su cuenta de destino. El script implementa las siguientes acciones: • Crea e invoca la función de Lambda para copiar productos de la cuenta de origen a la cuenta de destino	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube

Opción 2: copiar los productos de AWS Service Catalog de una región de origen a una región de destino

Tarea	Descripción	Habilidades requeridas
Actualizar el archivo de configuración.	1. Descargue el paquete (adjunto) `cross-region-copy` en su máquina local. 2. Actualice el archivo de `copyconf.properties` configuración con los siguientes valores: • `srcRegion` : proporcione la región de origen que contiene los productos. • `destRegion` : indique la región de destino de los productos.	Administrador de sistemas de AWS, administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	• `accountId` : proporcione su ID de cuenta de AWS.	

Configurar la CLI con sus credenciales de AWS.	Configure sus credenciales para acceder a la AWS CLI en su entorno ejecutando el comando `aws configure` y proporcionando los siguientes valores:
	`$aws configure`
	`AWS Access Key ID [None]: <your_access_key_id>`
	`AWS Secret Access Key [None]: <your_secret_access_key>`
	`Default region name [None]: Region`
	`Default output format [None]:`
	Para obtener más información al respecto, consulte Conceptos básicos de configuración en la interfaz de la línea de comandos de AWS.
		Administrador de AWS, administrador de sistemas de AWS, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Ejecute el script CopyProduct.	Ejecute el script `copyProduct.sh` en la región de destino. El script implementa las siguientes acciones: • Crear un rol de ejecución para Lambda • Crea y adjunta la política de IAM para la función de ejecución de Lambda • Crea e invoca la función de Lambda para copiar productos de la región de origen a la región de destino	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube

Recursos relacionados

- Crear un rol de ejecución para Lambda (documentación de AWS Lambda)
- Crear una función de Lambda (documentación de AWS Lambda)
- AWS Service Catalog referencia API
- Documentación de AWS Service Catalog

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Crear una matriz RACI o RASCI para un modelo operativo en la nube

Teddy Germade, Jerome Descreux, Florian Leroux y Josselin LE MINEUR, Amazon Web Services

Resumen

El Cloud Center of Excellence (CCoE) o CEE (Cloud Enablement Engine) es un equipo capacitado y responsable que se centra en la preparación operativa para la nube. Su objetivo principal es transformar la organización de TI de la información de un modelo operativo en las instalaciones a un modelo operativo en la nube. El CCo E debe ser un equipo multifuncional que incluya representantes de la infraestructura, las aplicaciones, las operaciones y la seguridad.

Uno de los componentes clave de un modelo operativo de nube es una matriz RACI o una matriz RASCI. Esto se utiliza para definir las funciones y responsabilidades de todas las partes involucradas en las actividades de migración y las operaciones en la nube. El nombre de la matriz se deriva de los tipos de responsabilidad definidos en la matriz: responsable (R), encargado (A), soporte (S), consultado (C) e informado (I). El tipo de soporte es opcional. Si la incluye, se denomina matriz RASCI y, si la excluye, se denomina matriz RACI.

Empezando por la plantilla adjunta, su equipo CCo electrónico puede crear una matriz RACI o RASCI para su organización. La plantilla contiene los equipos, las funciones y las tareas que son habituales en los modelos operativos de la nube. La base de esta matriz son las tareas relacionadas con la integración de las operaciones y las capacidades de CCo E. Sin embargo, puede personalizar esta plantilla para que se adapte a las necesidades de la estructura y el caso de uso de su organización.

La implementación de una matriz RACI no tiene límites. Este enfoque funciona para grandes organizaciones, empresas emergentes y todo lo demás. En el caso de las organizaciones pequeñas, el mismo recurso puede desempeñar varias funciones.

Epics

Creación de la matriz

Tarea	Descripción	Habilidades requeridas
Identifique a las partes interesadas principales.	Identifique a los principales administradores de servicios y equipos que estén vinculados	Administrador de proyectos

Tarea	Descripción	Habilidades requeridas
	a los objetivos estratégicos de su modelo operativo de nube.	

Tarea	Descripción	Habilidades requeridas

Personalice la plantilla de la matriz.	Descargue la plantilla en la sección de Adjuntos y, a continuación, actualice la matriz RACI o RASCI de la siguiente manera:
	• En la hoja de trabajo de Cloud Teams, actualiza los CCo nombres de las transmisiones electróni cas, los nombres de los equipos y las descripciones de los equipos según sea necesario para tu organizac ión.
	• En la hoja de trabajo de Roles de nube, actualice los roles, los nombres de los equipos y las descripci ones de los roles según sea necesario para su organizac ión.
	• En la hoja de trabajo de RASCI, actualice lo siguiente según sea necesario para su organizac ión:
	  • En la fila 1 y la columna A, actualiza las transmisi ones CCo E.
	  • En la fila 2, actualice los nombres de los equipos.
	  • En la fila 3, actualice los nombres de los roles.
		Administrador de proyectos

Tarea	Descripción	Habilidades requeridas
	• En las columnas D y E, actualice los campos y actividades generales que desee incluir en el diagrama RASCI.	
Planifique las reuniones.	1. Comunique los objetivos de la RASCI a todas las partes interesadas. 2. Planifique una o más reuniones para que pueda asistir un representante autorizado de cada equipo.	Administrador de proyectos

Tarea	Descripción	Habilidades requeridas
Complete la matriz.	En la reunión con todas las partes interesadas, haga lo siguiente: 1. Confirme que esté presente un representante de cada equipo. La participación del equipo es obligatoria para poder asignar con precisión los tipos de responsabilidad para cada tarea. 2. Revise qué es una matriz RASCI y sus objetivos con los participantes. 3. Revise el modelo de responsabilidad compartida con los participantes para que comprendan el alcance de las responsabilidades de su organización en materia de seguridad en la nube. 4. En la hoja de trabajo de RASCI, complete las columnas F a AN para cada tarea o actividad para asignar los siguientes tipos de responsabilidad: • Responsable (R) – Este rol es responsable de realizar el trabajo para completar la tarea. • Encargado (A) – Este rol es el encargado de garantizar que la tarea se	Administrador de proyectos

Tarea	Descripción	Habilidades requeridas
	complete. Esta función también es responsab le de garantizar que se cumplan los requisitos previos y de delegar la tarea a los responsables. • Soporte (S) – Este rol ayuda a los responsab les a completar la tarea. Este tipo de responsab ilidad es opcional y puede optar por excluirlo para crear una matriz RACI más tradicional. • Consultado (C) – Se debe consultar a este rol para obtener opiniones o experiencia sobre la tarea. Dependiendo de la tarea, es posible que este tipo de responsabilidad no sea obligatorio. • Informado (I) – Se debe mantener informado a este rol sobre el progreso de la tarea y se le debe notificar cuando se complete la tarea. • En blanco – Este rol no está involucrado en la actividad o tarea.	

Tarea	Descripción	Habilidades requeridas
Comparta la matriz RASCI.	Cuando la matriz RACI o RASCI esté completa, haga que los líderes la aprueben. Guárdela en un repositorio compartido o en una ubicación central donde todas las partes interesadas puedan acceder a ella. Le recomendamos que utilice procesos de control de documentos estándar para registrar y aprobar las revisiones de la matriz.	Administrador de proyectos

Recursos relacionados

- Modelo de responsabilidad compartida de AWS

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Cree alarmas para métricas personalizadas mediante la detección de CloudWatch anomalías de Amazon

Ram Kandaswamy y Raheem Jiwani, Amazon Web Services

Resumen

En la nube de Amazon Web Services (AWS), puede utilizar Amazon CloudWatch para crear alarmas que supervisen las métricas y envíen notificaciones o para realizar cambios automáticamente si se supera un umbral.

Para evitar verse limitado por umbrales estáticos, puede crear alarmas basadas en patrones anteriores y que lo notifiquen si determinadas métricas están fuera del intervalo operativo normal. Por ejemplo, puede supervisar los tiempos de respuesta de su API desde Amazon API Gateway y recibir notificaciones sobre anomalías que le impidan cumplir un acuerdo de nivel de servicio (SLA).

Este patrón describe cómo utilizar la detección de CloudWatch anomalías para las métricas personalizadas. El patrón le muestra cómo crear una métrica personalizada en Amazon CloudWatch Logs Insights o publicar una métrica personalizada con una función de AWS Lambda y, a continuación, configurar la detección de anomalías y crear notificaciones mediante Amazon Simple Notification Service (Amazon SNS).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un tema de SNS existente, configurado para enviar notificaciones por correo electrónico. Para obtener más información al respecto, consulte Introducción a Amazon SNS en la documentación de Amazon SNS.
- Una aplicación existente, configurada con Logs. CloudWatch

Limitaciones

- CloudWatch las métricas no admiten intervalos de milisegundos. Para obtener más información sobre la granularidad de las métricas normales y personalizadas, consulta Amazon CloudWatch FAQs.

Arquitectura

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Los registros que utilizan métricas creadas y actualizadas por CloudWatch Logs se transmiten a. CloudWatch
2. Se inicia una alarma en función de los umbrales y envía una alerta a un tema de SNS.
3. Amazon SNS le enviará una notificación por correo electrónico.

Pila de tecnología

- CloudWatch
- AWS Lambda
- Amazon SNS

Tools (Herramientas)

- Amazon CloudWatch ofrece una solución de monitorización fiable, escalable y flexible.
- AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores.
- Amazon Simple Notification Service (Amazon SNS) es un servicio administrado que proporciona la entrega de mensajes de los publicadores a los suscriptores.

Epics

Configurar la detección de anomalías para una métrica personalizada

Tarea	Descripción	Habilidades requeridas
Opción 1: Crear una métrica personalizada con una función de Lambda.	Descargue el `lambda_function.py` archivo (adjunto) y, a continuación, sustituya el `lambda_function.py` archivo de muestra del aws-lambda-	DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	developer-guiderepositorio en la documentación de AWS GitHub. Esto le proporciona un ejemplo de función Lambda que envía métricas personalizadas a CloudWatch Logs. La función Lambda utiliza la API Boto3 para integrarse con. CloudWatch Tras ejecutar la función Lambda, puede iniciar sesión en la consola de administración de AWS, abrir la CloudWatch consola y la métrica publicada estará disponible en su espacio de nombres publicado.	

Tarea	Descripción	Habilidades requeridas
Opción 2: crear métricas personalizadas a partir de grupos de CloudWatch registros.	Inicie sesión en la consola de administración de AWS, abra la CloudWatch consola y, a continuación, seleccione Grupos de registro. Seleccione el grupo de registro para el que desea crear una métrica. Elija Acciones y, a continuación, seleccione Crear filtro de métrica. Para Patrón de filtro, introduzca el patrón de filtro que desea utilizar. Para obtener más información, consulte la sintaxis de filtros y patrones en la CloudWatch documentación. Para probar su patrón de filtro, ingrese uno o más eventos de registro en Probar patrón. Cada evento de registro debe estar dentro de una línea, ya que los saltos de línea se utilizan para separar los eventos de registro en el cuadro de Log event messages (Mensajes de eventos de registro). Tras probar el patrón, puede introducir un nombre y un valor para la métrica en Detalles de la métrica.	DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Para obtener más información y los pasos para crear una métrica personalizada, consulte Crear un filtro de métrica para un grupo de registros en la CloudWatch documentación.	

Tarea	Descripción	Habilidades requeridas
Cree una alarma para su métrica personalizada.	En la CloudWatch consola, selecciona Alarmas y, a continuación, selecciona Crear alarma. Seleccione Seleccionar métrica e introduzca el nombre de la métrica que creó anteriormente en el cuadro de búsqueda. Seleccione la pestaña Métricas graficadas y configure las opciones según sus necesidades. En Condiciones, seleccione Detección de anomalías en lugar de Umbrales estáticos. Esto le muestra una banda basada en dos desviaciones estándar predeterminadas. Puede configurar umbrales y ajustarlos según sus necesidades. Elija Siguiente. **Note** La banda es dinámica y depende de la calidad de los puntos de datos. Cuando comience a agregar más datos, la banda y los umbrales se	DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	actualizan automátic amente.	
Configurar notificaciones de SNS.	En Notificación, elija el tema de SNS al que desee enviar la notificación cuando la alarma tenga el estado `ALARM`, `OK` o `INSUFFICIENT_DATA` . Para que la alarma envíe varias notificaciones para el mismo estado de alarma o para estados de alarma diferentes, seleccione Add notificación (Añadir notificac ión). Elija Siguiente. Escriba un nombre y la descripción de la alarma. El nombre solo debe contener caracteres ASCII. A continuación, elija Siguiente. En Obtener vista previa y crear, confirme que la información y las condiciones son las correctas y luego, elija Crear alarma.	DevOps ingeniero, AWS DevOps

Recursos relacionados

- Publicar métricas personalizadas en CloudWatch
- Uso de la detección de CloudWatch anomalías
- Eventos de alarma y Amazon EventBridge

- ¿Cuáles son las prácticas recomendadas que se deben seguir a la hora de introducir métricas personalizadas en Cloud Watch? (video)
- Introducción a CloudWatch Application Insights (vídeo)
- Detecte anomalías con CloudWatch (vídeo)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Crear un IDE de AWS Cloud9 que utilice volúmenes de Amazon EBS con cifrado predeterminado

Janardhan Malyala y Dhrubajyoti Mukherjee, Amazon Web Services

Resumen

Aviso: ya no AWS Cloud9 está disponible para nuevos clientes. Los clientes actuales de AWS Cloud9 pueden seguir utilizando el servicio con normalidad. Más información

Puede utilizar el cifrado predeterminado para reforzar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS) y de las copias de instantáneas en la nube de Amazon Web Services (AWS).

Puede crear un entorno de desarrollo integrado (IDE) de AWS Cloud9 que utilice volúmenes de EBS con cifrado predeterminado. Sin embargo, el rol vinculado al servicio de AWS Identity and Access Management (IAM) de AWS Cloud9 requiere acceso a la clave del AWS Key Management Service (AWS KMS) para estos volúmenes de EBS. Si no se proporciona acceso, el IDE de AWS Cloud9 podría no lanzarse y la depuración podría ser difícil.

Este patrón proporciona los pasos para agregar el rol vinculado al servicio de AWS Cloud9 a la clave de AWS KMS que utilizan los volúmenes de EBS. La configuración descrita en este patrón ayuda a crear y lanzar correctamente un IDE que utilice volúmenes de EBS con cifrado predeterminado.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Cifrado predeterminado activado para los volúmenes de EBS. Para obtener más información sobre el cifrado predeterminado, consulte el cifrado de Amazon EBS en la documentación de Amazon Elastic Compute Cloud (Amazon EC2).
- Una clave KMS existente administrada por el cliente para cifrar los volúmenes de EBS.

> **Note**
>
> No se necesita crear un rol vinculado al servicio para AWS Cloud9. Al crear un entorno de desarrollo de AWS Cloud9, es AWS Cloud9 el que crea el rol vinculado al servicio.

Arquitectura

Pila de tecnología

- AWS Cloud9
- IAM
- AWS KMS

Tools (Herramientas)

- AWS Cloud9 es un entorno de desarrollo integrado (IDE) que ayuda a codificar, crear, ejecutar, probar y depurar software. También ayuda a lanzar software a la nube de AWS.
- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento a nivel de bloques para utilizarlos con instancias de Amazon Elastic Compute Cloud (Amazon). EC2
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.

Epics

Buscar el valor de la clave de cifrado predeterminado

Tarea	Descripción	Habilidades requeridas
Registre el valor de la clave de cifrado predeterminado para los volúmenes de EBS.	Inicie sesión en la consola de administración de AWS y abra la EC2 consola de Amazon. Elija el EC2 panel de control y, a continuación, elija Protección y seguridad de datos en los atributos de la cuenta. En la sección de cifrado de EBS, copie y registre el valor de la	Arquitecto e DevOps ingeniero de nube

Tarea	Descripción	Habilidades requeridas
	clave de cifrado predeterm inada.	

Proporcionar acceso a la clave de AWS KMS

Tarea	Descripción	Habilidades requeridas
Proporcione a AWS Cloud9 acceso a la clave de KMS para los volúmenes de EBS.	1. Abra la consola de AWS KMS y, a continuación, seleccione Customer managed keys (Claves administradas por el cliente). Seleccione la clave de AWS KMS utilizada para el cifrado de Amazon EBS y, a continuación, View key (Ver clave). 2. En la pestaña Key policy (Política de claves), confirme que puede ver el texto de la política de claves. Si no puede ver el formulario de texto, seleccione Change to policy view (Cambiar a la vista de políticas). 3. Seleccione Editar. Agregue el código que aparece en la sección de información adicional a la política y, a continuación, seleccione Save changes (Guardar cambios). Los cambios en la política permiten que	Arquitecto de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	la función vinculada al servicio de AWS Cloud9, `AWSServiceRoleForAWSCloud9` , acceda a la clave. Para obtener más información sobre la actualización de una política de claves, consulte How to change a key policy (Cómo cambiar una política de claves) en la documentación de AWS KMS. ⚠ Important El rol vinculado al servicio para AWS Cloud9 se crea automáticamente al lanzar el primer IDE. Para obtener más información, consulte Creating a service-linked role (Crear un rol vinculado a un servicio) en la documentación de AWS Cloud9.	

Crear y lanzar el IDE

Tarea	Descripción	Habilidades requeridas
Cree e inicie el IDE de AWS Cloud9.	Abra la consola AWS Cloud9 y elija Crear entorno. Configure el IDE de acuerdo con sus requisitos siguiendo los pasos de Creación de un EC2 entorno en la documentación de AWS Cloud9.	Arquitecto e ingeniero de nube DevOps

Recursos relacionados

- Encrypt EBS volumes used by AWS Cloud9 (Cifrar los volúmenes de EBS utilizados por AWS Cloud9)
- Create a service-linked role for AWS Cloud9 (Crear un rol vinculado a un servicio para AWS Cloud9)
- Cree un EC2 entorno en AWS Cloud9

Información adicional

Actualizaciones de las políticas de clave de AWS KMS

Sustituya <aws_accountid> por el ID de la cuenta de AWS.

```
{
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<aws_accountid>:role/aws-service-role/
cloud9.amazonaws.com/AWSServiceRoleForAWSCloud9"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
```

```
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow attachment of persistent resources",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<aws_accountid>:role/aws-service-role/
cloud9.amazonaws.com/AWSServiceRoleForAWSCloud9"
            },
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        }
```

Uso de una clave entre cuentas

Si desea utilizar una clave de KMS entre cuentas, debe utilizar una concesión en combinación con la política de claves de KMS. Esto permite el acceso entre cuentas a la clave. En la misma cuenta que utilizó para crear el entorno de Cloud9, ejecute el siguiente comando en el terminal.

```
aws kms create-grant \
 --region <Region where Cloud9 environment is created> \
 --key-id <The cross-account KMS key ARN> \
 --grantee-principal arn:aws:iam::<The account where Cloud9 environment is
 created>:role/aws-service-role/cloud9.amazonaws.com/AWSServiceRoleForAWSCloud9 \
 --operations "Encrypt" "Decrypt" "ReEncryptFrom" "ReEncryptTo" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "DescribeKey" "CreateGrant"
```

Tras ejecutar este comando, puede crear entornos de Cloud9 mediante el cifrado de EBS con una clave de otra cuenta.

Crea automáticamente CloudWatch paneles de Amazon basados en etiquetas

Janak Vadaria, Vinodkumar Mandalapu y RAJNEESH TYAGI, Amazon Web Services

Resumen

Crear diferentes CloudWatch paneles de Amazon de forma manual puede llevar mucho tiempo, especialmente cuando hay que crear y actualizar varios recursos para escalar automáticamente el entorno. Una solución que cree y actualice sus CloudWatch paneles automáticamente puede ahorrarle tiempo. Este patrón le ayuda a implementar un proceso totalmente automatizado que AWS Cloud Development Kit (AWS CDK) crea y actualiza CloudWatch paneles para sus AWS recursos en función de los eventos de cambio de etiquetas, para mostrar las métricas de Golden Signals.

En la ingeniería de confiabilidad del sitio (SRE), Golden Signals se refiere a un conjunto integral de métricas que ofrecen una visión amplia de un servicio desde la perspectiva del usuario o del consumidor. Estas métricas se componen de la latencia, el tráfico, los errores y la saturación. Para obtener más información, consulte ¿Qué es la ingeniería de confiabilidad de sitios (SRE)? en el AWS sitio web.

La solución que proporciona este patrón se basa en eventos. Una vez desplegado, supervisa de forma continua los eventos de cambio de etiquetas y actualiza automáticamente los CloudWatch paneles y las alarmas.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- AWS Command Line Interface (AWS CLI), instalado y configurado
- Requisitos previos para la versión 2 AWS CDK
- Un entorno de arranque en AWS
- Python versión 3
- AWS SDK para Python (Boto3), instalado
- La versión 18 o posterior de Node.js
- El administrador de paquetes de nodos (npm), instalado y configurado para AWS CDK
- Familiaridad moderada (nivel 200) con el y AWS CDK AWS CodePipeline

Limitaciones

Actualmente, esta solución crea paneles automatizados únicamente para los siguientes servicios de AWS:

- Amazon Relational Database Service (Amazon RDS)
- AWS Auto Scaling
- Amazon Simple Notification Service (Amazon SNS)
- Amazon DynamoDB
- AWS Lambda

Arquitectura

Pila de tecnología de destino

- CloudWatch cuadros de mando
- CloudWatch alarmas

Arquitectura de destino

1. Un evento de cambio de AWS etiqueta para las etiquetas de la aplicación configuradas o los cambios de código inicia una canalización AWS CodePipeline para crear e implementar paneles actualizados. CloudWatch
2. AWS CodeBuild ejecuta un script de Python para buscar los recursos que tienen etiquetas configuradas y almacena el recurso IDs en un archivo local en un CodeBuild entorno.
3. CodeBuild ejecuta cdk synth para generar CloudFormation plantillas que despliegan CloudWatch paneles y alarmas.
4. CodePipeline despliega las CloudFormation plantillas en la región y especificadas. Cuenta de AWS
5. Cuando la CloudFormation pila se haya desplegado correctamente, podrá ver los CloudWatch paneles y las alarmas.

Automatización y escala

Esta solución se ha automatizado mediante el uso de AWS CDK. Puedes encontrar el código en el CloudWatch repositorio de GitHub Golden Signals Dashboards en Amazon. Para un escalado adicional y para crear paneles personalizados, puede configurar varias claves y valores de etiquetas.

Tools (Herramientas)

Servicios de Amazon

- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes, incluidas AWS Lambda funciones, puntos de enlace de invocación HTTP que utilizan destinos de API o buses de eventos, entre otros. Cuentas de AWS
- AWS CodePipeline permite diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software y automatizar los pasos necesarios para lanzar los cambios en el software de manera continua.
- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Prácticas recomendadas

Como práctica recomendada, puede usar el cifrado y la autenticación para los repositorios de origen que se conectan a sus canalizaciones. Para obtener más información sobre las mejores prácticas, consulte las CodePipeline mejores prácticas y los casos de uso en la CodePipeline documentación.

Epics

Configuración e implementación de la aplicación de ejemplo

Tarea	Descripción	Habilidades requeridas
Configure implemente la aplicación de ejemplo.	1. Clona el repositorio de código de GitHub muestra mediante el comando: `git clone https://github.com/aws-samples/golden-signals-dashboards-sample-app` 2. Navegue hasta el repositorio clonado de su equipo y abra el archivo `src/project-settings.ts` con el editor que elija. 3. Cambie el valor `projectSettings` constante de acuerdo con las etiquetas de sus AWS recursos y las asignaciones de aplicaciones. 4. Establezca las variables de entorno `AWS_ACCOUNT` , `AWS_REGION` y `GS_DASHBOARD_INSTANCE` . • `AWS_ACCOUNT` Establézcalo en el ID de cuenta de tu AWS cuenta.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• Establezca `AWS_REGION` en la región en donde desea implementar la aplicación de ejemplo. • Configure `GS_DASHBOARD_INSTANCE` en `dev`, `test` o `prod`, en función de su entorno de desarrollo. (Se recomienda `test` para el procedimiento de prueba descrito en este patrón). 5. AWS CLI Configúrala con tus AWS credenciales. Para obtener más información, consulte Establecer y ver los valores de configuración mediante los comandos de la AWS CLI documentación. 6. Ejecute el siguiente comando para implementar la aplicación de ejemplo de panel de Golden Signals: `sh deploy.sh`	

Tarea	Descripción	Habilidades requeridas
Cree paneles y alarmas de forma automática.	Tras implementar la aplicación de ejemplo, puede crear cualquiera de los recursos compatibles con esta solución con los valores de etiqueta esperados, lo que creará automáticamente los paneles y las alarmas especificados. Para probar esta solución, cree una AWS Lambda función: 1. Inicie sesión Consola de administración de AWS en el Región de AWS lugar donde implementó la aplicación de muestra. 2. Abra la consola Lambda en. https://console.aws.amazon.com/lambda/ 3. Elija Crear una función y luego introduzca un nombre de función. 4. En el panel Configuración avanzada, seleccione Habilitar etiquetas y, a continuación, Añadir nueva etiqueta. Introduzca la clave y el valor siguientes: • Clave: `AutoDashboard` • Valor: `True` 5. Elija Crear función.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	La función de Lambda inicia inmediatamente una canalización de código, que crea automáticamente los paneles y las alarmas para esa función de Lambda concreta. 6. Para ver los paneles y las alarmas automatizados, abra la CloudWatch consola en. https://console.aws.amazon.com/cloudwatch/ Puede ver los paneles y las alarmas personalizados de la función que especificó en la `projectSettings` constante (APP1-lambda de forma predeterminada). 7. Seleccione el panel de la función de Lambda para ver los paneles automatizados adicionales que se crearon como parte de esta solución. 8. Repita estos pasos para otros servicios, como Amazon RDS, Amazon SNS y DynamoDB AWS Auto Scaling, para generar los paneles asociados. Para obtener un ejemplo de Amazon RDS, consulte	

Tarea	Descripción	Habilidades requeridas
	la sección Información adicional.	

Eliminación de la aplicación de ejemplo

Tarea	Descripción	Habilidades requeridas
Elimine el constructo `golden-signals-dashboard` .	1. Para eliminar todas las CloudFormation pilas creadas por la aplicación de muestra, debe volver a configurar las variables `AWS_ACCOUNT` de `GS_DASHBOARD_INSTANCE` entorno y. `AWS_REGION` El comando `destroy.sh` requiere estas configuraciones. • `AWS_ACCOUNT` es el identificador de su AWS cuenta. • `AWS_REGION` es la región en la que implementó la aplicación de ejemplo. • `GS_DASHBOARD_INSTANCE` es `dev`, `test` o `prod`, en función de su configuración anterior. 2. AWS CLI Configúrala con tus AWS credenciales.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	3. Ejecute el siguiente comando para eliminar la aplicación de muestra y todas las CloudFormation pilas asociadas: `sh destroy.sh`	

Resolución de problemas

Problema	Solución
No se encontró el comando de Python (en referencia a `findresources.sh` , línea 8).	Compruebe la versión de la instalación de Python. Si ha instalado la versión 3 de Python, sustituya `python` por `python3` en la línea 8 del archivo `resources.sh` y vuelva a ejecutar el comando `sh deploy.sh` para implementar la solución.

Recursos relacionados

- Bootstrapping (documentación)AWS CDK
- Uso de perfiles con nombre asignado (documentación)AWS CLI
- AWS CDK Taller

Información adicional

En la siguiente ilustración se muestra un panel de ejemplo para Amazon RDS que se crea como parte de esta solución.

Documentación del diseño de su AWS Landing Zone

Michael Daehnert, Florian Langer y Michael Lodemann, Amazon Web Services

Resumen

Una zona de aterrizaje es un entorno con varias cuentas bien diseñado, que se basa en prácticas recomendadas de seguridad y cumplimiento. Es el contenedor de toda la empresa que contiene todas las unidades organizativas (OUs) Cuentas de AWS, los usuarios y otros recursos. Una landing zone puede ampliarse para adaptarse a las necesidades de una empresa de cualquier tamaño. AWS tiene dos opciones para crear tu landing zone: una landing zone basada en servicios AWS Control Towero una landing zone personalizada que tú construyas. Cada opción requiere un nivel de AWS conocimiento diferente.

AWS creado AWS Control Tower para ayudarte a ahorrar tiempo mediante la automatización de la configuración de una landing zone. AWS Control Tower está gestionado por AWS las mejores prácticas y directrices, y las utiliza para ayudarle a crear su entorno fundamental. AWS Control Tower utiliza servicios integrados, como AWS Service Catalogy AWS Organizations, para aprovisionar cuentas en tu landing zone y gestionar el acceso a esas cuentas.

AWS Los proyectos de landing zone varían en cuanto a los requisitos, los detalles de implementación y los elementos de acción operativa. Hay aspectos de personalización que deben abordarse con cada implementación de zona de aterrizaje. Esto incluye (pero no se limita a) cómo se gestiona la administración del acceso, qué tecnología se utiliza y cuáles son los requisitos de supervisión para lograr la excelencia operativa. Este patrón proporciona una plantilla que lo ayuda a documentar su proyecto de zona de aterrizaje. Al usar la plantilla, puede documentar el proyecto más rápidamente y ayudar a sus equipos de desarrollo y operaciones a entender su zona de aterrizaje.

Requisitos previos y limitaciones

Limitaciones

Este patrón no describe qué es una zona de aterrizaje ni cómo implementarla. Para obtener más información sobre estos temas, consulte la sección Recursos relacionados.

Epics

Creación del documento de diseño

Tarea	Descripción	Habilidades requeridas
Identifique a las partes interesadas principales.	Identifique los principales administradores de servicios y equipos que estén vinculados a su zona de aterrizaje.	Administrador de proyectos
Personalice la plantilla.	Descargue la plantilla en la sección de Adjuntos y, a continuación, actualice la plantilla de la siguiente manera: 1. Elimine todas las secciones que no se apliquen a la zona de aterrizaje o a los procesos de su organizac ión. 2. Añada cualquier sección que sea exclusiva de su organización.	Administrador de proyectos
Complete la plantilla.	En las reuniones con las partes interesadas o mediante un write-and-review proceso, complete la plantilla de la siguiente manera: 1. Utilice las instrucciones y la información de los recuadros azules para completar cada sección. 2. Sustituya o elimine los campos amarillos por	Administrador de proyectos

Tarea	Descripción	Habilidades requeridas
	valores personalizados para su organización. 3. Sustituya o elimine cualquier campo de imagen por su arquitectura o diagrama de flujo personalizados. 4. Complete la sección Historial de revisiones y colaboradores de la plantilla .	
Comparta el documento de diseño.	Cuando la documentación de diseño de la zona de aterrizaje esté completa, guárdela en un repositorio compartido o en una ubicación central donde todas las partes interesadas puedan acceder a ella. Le recomendamos que utilice procesos de control de documentos estándar para registrar y aprobar las revisiones del documento de diseño.	Administrador de proyectos

Recursos relacionados

- AWS Control Tower documentación
  - Planifica tu AWS Control Tower landing zone
  - AWS estrategia multicuenta para tu AWS Control Tower landing zone
  - Consejos administrativos para la configuración de la landing zone
  - Expectativas para la configuración de la zona de aterrizaje

- Personalizaciones para AWS Control Tower (biblioteca de AWS soluciones)
- Configuración de un entorno multicuenta seguro y escalable (AWS guíaAWS prescriptiva)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Mejore el rendimiento operativo habilitando Amazon DevOps Guru en varias regiones y cuentas de AWS y OUs con la CDK de AWS

Dr. Rahul Sharad Gaikwad, Amazon Web Services

Resumen

Este patrón muestra los pasos para habilitar el servicio Amazon DevOps Guru en varias regiones, cuentas y unidades organizativas () de Amazon Web Services (AWSOUs) mediante el kit de desarrollo en la nube de AWS (AWS CDK) en TypeScript. Puede usar las pilas de CDK de AWS para implementar AWS CloudFormation StackSets desde la cuenta de administrador (principal) de AWS para habilitar Amazon DevOps Guru en varias cuentas, en lugar de iniciar sesión en cada cuenta y habilitar DevOps Guru individualmente para cada una de ellas.

Amazon DevOps Guru ofrece funciones de operaciones de inteligencia artificial (AIOps) para ayudarlo a mejorar la disponibilidad de sus aplicaciones y resolver los problemas operativos con mayor rapidez. DevOps Guru reduce el esfuerzo manual al aplicar recomendaciones basadas en el aprendizaje automático (ML), sin necesidad de conocimientos de aprendizaje automático. DevOps Guru analiza sus recursos y datos operativos. Si detecta alguna anomalía, proporciona métricas, eventos y recomendaciones para ayudarle a solucionar el problema.

Este patrón describe tres opciones de implementación para habilitar Amazon DevOps Guru:

- Para todos, apile recursos en varias cuentas y regiones
- Para todos, apile los recursos en todas partes OUs
- Para recursos de pila específicos en varias cuentas y regiones

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada. (Consulte Instalación, actualización y desinstalación de la CLI de AWS en la documentación de la CLI de AWS).
- Kit de herramientas de AWS CDK, instalado y configurado. (Consulte el kit de herramientas de AWS CDK en la documentación de AWS CDK).

- Node Package Manager (npm), instalado y configurado para la AWS CDK en. TypeScript (Consulte Descarga e instalación de Node.js y npm en la documentación de npm).
- Python3 instalado y configurado para ejecutar un script de Python para inyectar tráfico en la aplicación sin servidor de muestra. (Consulte Configuración y uso de Python en la documentación de Python).
- Pip, instalado y configurado para instalar la biblioteca de solicitudes de Python. (Consulte las instrucciones de instalación de pip en el PyPI sitio web).

Versiones de producto

- Kit de herramientas de AWS CDK, versión 1.107.0 o posterior
- npm versión 7.9.0 o posterior
- Node.js: versión 15.3.0 o posterior

Arquitectura

Tecnologías

La arquitectura de este patrón incluye los siguientes servicios:

- El DevOps gurú de Amazon
- AWS CloudFormation
- Amazon API Gateway
- AWS Lambda
- Amazon DynamoDB
- Amazon CloudWatch
- AWS CloudTrail

Pilas de CDK de AWS

El patrón utiliza las siguientes pilas de CDK de AWS:

- `CdkStackSetAdminRole`: crea un rol de administrador de AWS Identity and Access Management (IAM) para establecer una relación de confianza entre las cuentas de administrador y de destino.
- `CdkStackSetExecRole`: crea un rol de IAM para confiar en la cuenta de administrador.

- `CdkDevopsGuruStackMultiAccReg`— Permite que DevOps Guru funcione en varias regiones y cuentas de AWS para todas las pilas, y configura las notificaciones del Amazon Simple Notification Service (Amazon SNS).
- `CdkDevopsGuruStackMultiAccRegSpecStacks`— Permite que DevOps Guru funcione en varias regiones y cuentas de AWS para pilas específicas, y configura las notificaciones de Amazon SNS.
- `CdkDevopsguruStackOrgUnit`— Permite el cruce OUs de DevOps Guru y configura las notificaciones de Amazon SNS.
- `CdkInfrastructureStack`: implementa ejemplos de componentes de aplicaciones sin servidor, como API Gateway, Lambda y DynamoDB, en la cuenta de administrador para demostrar la inyección de errores y la generación de información.

Arquitectura de aplicación de muestra

El siguiente diagrama ilustra la arquitectura de un ejemplo de aplicación sin servidor que se ha implementado en varias cuentas y regiones. El patrón utiliza la cuenta de administrador para implementar todas las pilas de CDK de AWS. También utiliza la cuenta de administrador como una de las cuentas de destino para configurar DevOps Guru.

1. Cuando DevOps Guru está activado, primero toma como base el comportamiento de cada recurso y, a continuación, ingiere los datos operativos de CloudWatch las métricas vendidas.
2. Si detecta una anomalía, la correlaciona con los eventos de origen y genera información. CloudTrail
3. La información proporciona una secuencia correlacionada de eventos junto con recomendaciones prescritas para que el operador pueda identificar el recurso responsable.
4. Amazon SNS envía mensajes de notificación al operador.

Automatización y escala

El GitHub repositorio que se proporciona con este patrón utiliza la CDK de AWS como herramienta de infraestructura como código (IaC) para crear la configuración de esta arquitectura. AWS CDK lo ayuda a organizar los recursos y habilitar DevOps Guru en varias cuentas, regiones y. OUs

Tools (Herramientas)

Servicios de AWS

- AWS CDK: el Kit de desarrollo en la nube de AWS (AWS CDK) le ayuda a definir su infraestructura de nube como código en uno de los cinco lenguajes de programación compatibles: JavaScript Python TypeScript, Java y C#.
- AWS CLI: Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta unificada que proporciona una interfaz de la línea de comandos coherente para interactuar con los servicios y recursos de AWS.

Código

El código fuente de este patrón está disponible en el GitHub repositorio Amazon DevOps Guru CDK Samples. El código CDK de AWS está escrito TypeScript. Para clonar y utilizar el repositorio, siga las instrucciones de la siguiente sección.

> **Important**
>
> Algunas de las historias de este patrón incluyen ejemplos de comandos de AWS CDK y AWS CLI formateados para Unix, Linux y macOS. Para Windows, sustituya la barra diagonal invertida (\) utilizada como carácter de continuación de Unix al final de cada línea por el signo de intercalación (^).

Epics

Prepare los recursos de AWS para la implementación

Tarea	Descripción	Habilidades requeridas
Configure los perfiles con nombre de AWS.	Configure sus perfiles con nombre de AWS de la siguiente manera para implementar pilas en un entorno de varias cuentas.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	Para la cuenta de administrador:
	
	`$aws configure --profile administrator`
	`AWS Access Key ID [****]: <your-administrator-access-key-ID>`
	`AWS Secret Access Key [****]: <your-administrator-secret-access-key>`
	`Default region name [None]: <your-administrator-region>`
	`Default output format [None]: json`
	
	Para la cuenta de destino:
	
	`$aws configure --profile target`
	`AWS Access Key ID [****: <your-target-access-key-ID>`
	`AWS Secret Access Key [****]: <your-target-secret-access-key>`
	`Default region name [None]: <your-target-region>`
	`Default output format [None]: json`
	
	Para obtener más información, consulte Uso de perfiles con nombre en la documentación de la CLI de AWS.	

Tarea	Descripción	Habilidades requeridas
Compruebe las configuraciones de los perfiles de AWS.	(Opcional) Puede verificar las configuraciones de su perfil de AWS en los archivos `credentials` y `config` siguiendo las instrucciones en Cómo establecer y ver los ajustes de configuración en la la documentación de la CLI de AWS.	DevOps ingeniero
Verifique la versión de AWS CDK.	Compruebe la versión del kit de herramientas de AWS CDK mediante el siguiente comando: `$cdk --version` Este patrón requiere la versión 1.107.0 o posterior. Si tiene una versión anterior de AWS CDK siga las instrucciones de la documentación de AWS CDK para actualizarla.	DevOps ingeniero
Clonar el código del proyecto.	Clona el GitHub repositorio de este patrón mediante el comando: `$git clone https://github.com/aws-samples/amazon-devopsguru-cdk-samples.git`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Instale las dependencias de los paquetes y compile los TypeScript archivos.	Instale las dependencias del paquete y compile los TypeScript archivos ejecutando los siguientes comandos:
	`$cd amazon-devopsguru-cdk-samples`
	`$npm install`
	`$npm fund`
	Estos comandos instalan todos los paquetes del repositorio de muestra.
	Important
	Si se muestra algún error acerca de paquetes que faltan, utilice uno de los siguientes comandos:
	`$npm ci`
	—o—
	`$npm install -g @aws-cdk/<package-name>`
	Puede encontrar la lista de nombres y versiones de los paquetes en la sección `Dependencies` del archivo `/amazon-devopsguru`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`-cdk-samples/package.json` . Para obtener más información, consulte npm ci y npm install en la documentación de npm.	

Crear (sintetizar) las pilas de CDK de AWS

Tarea	Descripción	Habilidades requeridas
Configure una dirección de correo electrónico para las notificaciones de Amazon SNS.	Siga estos pasos para proporcionar una dirección de correo electrónico para las notificaciones de Amazon SNS: 1. Edite los archivos `/amazon-devopsguru-cdk-samples/lib/cdk-devopsguru-multi-acc-reg-stack.ts` y `/amazon-devopsguru-cdk-samples/lib/cdk-devopsguru-org-uni-stack.ts` . 2. En la `DevOpsGuruTopic` , sección `Subscription` , actualice el parámetro `Endpoint` con su dirección de correo electrónico. 3. Guardar y cerrar los archivos.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Construya el código del proyecto.	Cree el código del proyecto y sintetice las pilas ejecutando el comando:
	`npm run build && cdk synth`
	Debería ver una salida similar a esta:
	`$npm run build && cdk synth`
	`> cdk-devopsguru@0.1.0 build`
	`> tsc`
	`Successfully synthesized to ~/amazon-devopsguru-cdk-samples/cdk.out`
	`Supply a stack id (CdkDevopsGuruStackMultiAccReg,CdkDevopsGuruStackMultiAccRegSpecStacks, CdkDevopsguruStackOrgUnit, CdkInfrastructureStack, CdkStackSetAdminRole, CdkStackSetExecRole) to display its template.`
	Para obtener más información y conocer los pasos, consulte Su primera aplicación de AWS CDK en la documentación de AWS CDK.
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Enumere las pilas de CDK de AWS.	Ejecute el siguiente comando para enumerar todas las pilas de AWS CDK:
	`$cdk list`
	El comando muestra la lista siguiente:
	`CdkDevopsGuruStack`
	`MultiAccReg`
	`CdkDevopsGuruSt`
	`ackMultiAccRegSpec`
	`Stacks`
	`CdkDevopsguruStackOr`
	`gUnit`
	`CdkInfrastructureStac`
	`k`
	`CdkStackSetAdminRole`
	`CdkStackSetExecRole`
		DevOps ingeniero

Opción 1: Habilita DevOps Guru para todos los recursos acumulados en varias cuentas

Tarea	Descripción	Habilidades requeridas
Implemente las pilas de CDK de AWS para crear roles de IAM.	Este patrón utiliza AWS CloudFormation StackSets para realizar operaciones de apilamiento en varias cuentas. Si va a crear su primer conjunto de pilas, debe crear las siguientes funciones de IAM para configurar los permisos necesarios en sus cuentas de AWS:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• `AWSCloudFormationStackSetAdministrationRole` • `AWSCloudFormationStackSetExecutionRole` **Note** Los roles deben tener estos nombres exactos. 1. Cree el rol `AWSCloudFormationStackSetAdministrationRole` de IAM en la cuenta de administrador (principal) ejecutando el siguiente comando CLI: `$cdk deploy CdkStackSetAdminRole --profile administrator` 2. Cree el rol `AWSCloudFormationStackSetExecutionRole` de IAM en todas las cuentas de destino en las que desee ejecutar las instancias de la pila. Para crear este rol, ejecute estos comandos de CLI:	

Tarea	Descripción	Habilidades requeridas

	<pre>$cdk deploy CdkStackSetExecRole \
	  --parameters AdministratorAccountId=<administrator-account-ID> \
	  --profile administrator
	
	$cdk deploy CdkStackSetExecRole \
	  --parameters AdministratorAccountId=<administrator-account-ID> \
	  --profile target</pre>
	Para obtener más información, consulte Otorgar permisos autogestionados en la CloudFormation documentación de AWS.	

Tarea	Descripción	Habilidades requeridas
Implemente la pila de CDK de AWS para habilitar DevOps Guru en varias cuentas.	La pila `CdkDevopsGuruStackMultiAccReg` de CDK de AWS crea conjuntos de pilas para implementar instancias de pila en varias cuentas y regiones. Para implementar la pila, ejecute el siguiente comando de la CLI con los parámetros especificados: `$cdk deploy CdkDevopsGuruStackMultiAccReg \ --profile administrator \ --parameters AdministratorAccountId=<administrator-account-ID> \ --parameters TargetAccountId=<target-account-ID> \ --parameters RegionIds="<region-1>,<region-2>"` Actualmente, Amazon DevOps Guru está disponible en las regiones de AWS que figuran en las preguntas frecuentes de DevOps Guru.	DevOps ingeniero

Opción 2: habilita DevOps Guru para todos los recursos de la pila OUs

Tarea	Descripción	Habilidades requeridas
Extrae OU IDs.	En la consola de AWS Organizations, identifique IDs las unidades organizativas en las que quiere habilitar DevOps Guru.	DevOps ingeniero
Habilite los permisos administrados por el servicio para. OUs	Si utiliza AWS Organizations para la administración de cuentas, debe conceder permisos gestionados por el servicio para activar DevOps Guru. En lugar de crear las funciones de IAM manualmente, utilice funciones de acceso confiable basadas en la organización y vinculadas a servicios (). SLRs	DevOps ingeniero
Implemente la pila de CDK de AWS para permitir que DevOps Guru OUs atraviese.	La `CdkDevopsguruStackOrgUnit` pila de CDK de AWS permite el servicio DevOps Guru en todas OUs partes. Para implementar la pila, ejecute el siguiente comando con los parámetros especificados: `$cdk deploy CdkDevopsguruStackOrgUnit \ --profile administrator \ --parameters RegionIds="<region-1>,<region-2>" \`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`--parameters OrganizationalUnitIds="<OU-1>,<OU-2>"`	

Opción 3: Habilita DevOps Guru para almacenar recursos de pila específicos en varias cuentas

Tarea	Descripción	Habilidades requeridas

Implemente las pilas de CDK de AWS para crear roles de IAM.	Si aún no ha creado las funciones de IAM requeridas que se muestran en la primera opción, hágalo primero:
	1. Cree el rol `AWSCloudFormationStackSetAdministrationRole` de IAM en la cuenta de administrador (principal) ejecutando el siguiente comando CLI:
	`$cdk deploy CdkStackSetAdminRole --profile administrator`
	2. Cree el rol `AWSCloudFormationStackSetExecutionRole` de IAM en todas las cuentas de destino en las que desee ejecutar las instancias de la pila. Para crear este rol, ejecute los comandos CLI:
	`$cdk deploy CdkStackSetExecRole \`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	<pre>--parameters
	AdministratorAccountId=<administrator-account-ID> \
	--profile administrator
	
	$cdk deploy CdkStackSetExecRole \
	--parameters
	AdministratorAccountId=<administrator-account-ID> \
	--profile target</pre>
	Para obtener más información, consulte Otorgar permisos autogestionados en la CloudFormation documentación de AWS.	

Tarea	Descripción	Habilidades requeridas
Eliminar las pilas existentes.	Si ya utilizaste la primera opción para habilitar DevOps Guru para todos los recursos de la pila, puedes eliminar la pila anterior mediante el siguiente comando: `$cdk destroy CdkDevops GuruStackMultiAccR eg --profile administr ator` O bien, puede cambiar el parámetro `RegionIds` al volver a implementar la pila para evitar el error Las pilas ya existen.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Actualizar la pila de CDK de AWS con una lista de pilas.	1. Edite el archivo `/amazon-devopsguru-cdk-samples/lib/cdk-devopsguru-multi-acc-reg-spec-stack.ts` . 2. En `Resources` , `CloudFormation` , `StackNames` , enumera las pilas para las que quieres activar DevOps Guru. A modo de demostración, el parámetro especifique la pila `CdkInfrastructureStack` , pero puede editar esta entrada en función de sus necesidades. 3. Guarde y cierre el archivo. 4. Para sintetizar y actualizar la plantilla de pila, ejecute: `$cdk synth`	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
Implemente la pila de CDK de AWS para habilitar a DevOps Guru para disponer de recursos de pila específicos en varias cuentas.	La `CdkDevopsGuruStackMultiAccRegSpecStacks` pila de CDK de AWS permite a DevOps Guru disponer de recursos de pila específicos en varias cuentas. Para implementar la pila, ejecute el siguiente comando: `$cdk deploy CdkDevopsGuruStackMultiAccRegSpecStacks \ --profile administrator \ --parameters AdministratorAccountId=<administrator-account-ID> \ --parameters TargetAccountId=<target-account-ID> \ --parameters RegionIds="<region-1>,<region-2>"` **Note** Si ya implementó esta pila para la opción 1, cambie el parámetro `RegionIds` (asegúrese de elegir entre las regiones disponibles) para evitar el error Las pilas ya existen.	DevOps ingeniero

Implementar la pila de infraestructuras CDK de AWS

Tarea	Descripción	Habilidades requeridas
Implemente el ejemplo del paquete de infraestructura sin servidor.	La `CdkInfrastructureStack` pila de CDK de AWS implementa componentes sin servidor, como API Gateway, Lambda y una tabla de DynamoDB para mostrar las ideas de Guru. DevOps Para implementar la pila, ejecute el siguiente comando: `$cdk deploy CdkInfrastructureStack --profile administrator`	DevOps ingeniero
Introducir registros de ejemplo en DynamoDB.	Ejecute el siguiente comando para rellenar la tabla de DynamoDB con registros de ejemplo. Proporcione la ruta correcta para el script `populate-shops-dynamodb-table.json` . `$aws dynamodb batch-write-item \ --request-items file://scripts/populate-shops-dynamodb-table.json \ --profile administrator` El comando muestra el resultado siguiente:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	<pre>{
	"UnprocessedItems"
	: {}
	}</pre>	

Tarea	Descripción	Habilidades requeridas

Compruebe los registros introducidos en DynamoDB.	Para comprobar que la tabla de DynamoDB incluye los registros de muestra del archivo `populate-shops-dynamodb-table.json`, acceda a a URL de la API `ListRestApiEndpointMonitorOperator`, que se publica como salida de la pila de CDK de AWS. También puede encontrar esta URL en la pestaña Salidas de la CloudFormation consola de AWS de la `CdkInfrastructureStack` pila. La salida de AWS CDK sería similar a la siguiente:
	
	`CdkInfrastructureStack.CreateRestApiMonitorOperatorEndpointD1D00045 = https://oure17c5vob.execute-api.<your-region>.amazonaws.com/prod/`
	
	`CdkInfrastructureStack.ListRestApiMonitorOperatorEndpointABBDB8D8 = https://cdff8icfrn4.execute-api.<your-region>.amazonaws.com/prod/`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Espere a que los recursos completen la línea de base.	Esta pila sin servidor tiene algunos recursos. Le recomendamos que espere 2 horas antes de realizar los siguientes pasos. Si implementó esta pila en un entorno de producción, es posible que se tarden hasta 24 horas en completar la línea base, según la cantidad de recursos que haya seleccion ado para monitorear en DevOps Guru.	DevOps ingeniero

Genera ideas de DevOps Guru

Tarea	Descripción	Habilidades requeridas
Actualizar la pila de infraestr ucturas CDK de AWS.	Para probar DevOps Guru Insights, puede realizar algunos cambios de configura ción para reproducir un problema operativo típico. 1. Edite el archivo `/amazon-devopsguru-cdk-samples/lib/infrastructure-stack.ts` . 2. En la sección `DDB Table`, cambie la capacidad de lectura de la tabla de DynamoDB de 5 a 1. 3. Guarde y cierre el archivo.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	4. Ejecute los siguientes comandos para sintetizar e implementar la pila de infraestructura CDK de AWS actualizada:
	
	`$cdk synth`
	`$cdk deploy CdkInfrastructureStack --profile administrator`	

Tarea	Descripción	Habilidades requeridas
Introduzca solicitudes HTTP en la API.	Inyecta tráfico de entrada en forma de solicitudes HTTP en la API `ListRestApiMonitorOperatorEndpointxxxx` : 1. Ejecute el script de Python `/amazon-devopsguru-cdk-samples/scripts/sendAPIRequest.py` . 2. Actualiza la variable `url` con el enlace de la API para `ListRestApiMonitorOperatorEndpointxxxx` . Puede encontrar esta URL en la salida del comando de implementación de AWS CDK o en la consola de AWS Cloudformation, en la pestaña Salidas de la pila. 3. Guarde y cierre el archivo. 4. Ejecute el script de Python mediante el comando siguiente: `$python sendAPIRequest.py` 5. Asegúrese de obtener un código de estado 200. 6. Puede que necesite ejecutar el script a través de varios terminales	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	(preferiblemente cuatro) para inyectar tráfico a una velocidad alta. 7. Una vez que el script se ejecute aproximadamente 10 minutos seguidos, podrá ver una visión operativa en la consola DevOps Guru.	
Revise las ideas de DevOps Guru.	En condiciones estándar, el panel de control de DevOps Guru muestra cero en el contador de información continua. Si detecta una anomalía, emite una alerta en forma de información. En el panel de navegación, selecciona Insights para ver los detalles de la anomalía, incluidos un resumen, métricas agregadas, eventos relevantes y recomenda ciones. Para obtener más información sobre la revisión de información, consulte la entrada del blog Cómo obtener información operativa AIOps con Amazon DevOps Guru.	DevOps ingeniero

Limpieza

Tarea	Descripción	Habilidades requeridas

Limpie y elimine recursos.	Después de seguir este patrón, debe eliminar los recursos que ha creado para evitar incurrir en cargos adicionales. Ejecute estos comandos:
	`$cdk destroy CdkDevops GuruStackMultiAccReg --profile administrator`
	`$cdk destroy CdkDevops guruStackOrgUnit --profile administrator`
	`$cdk destroy CdkDevops GuruStackMultiAccRegSpecStacks --profile administrator`
	`$cdk destroy CdkInfrastructureStack --profile administrator`
	`$cdk destroy CdkStackSetAdminRole --profile administrator`
	`$cdk destroy CdkStackSetExecRole --profile administrator`
	`$cdk destroy CdkStackSetExecRole --profile target`
		DevOps ingeniero

Recursos relacionados

- Obtener información operativa AIOps con Amazon DevOps Guru

- Configure Amazon DevOps Guru fácilmente en varias cuentas y regiones mediante AWS CloudFormation StackSets
- DevOps Taller de gurús

Control de los conjuntos de permisos para varias cuentas mediante Account Factory for Terraform

Anand Krishna Varanasi y Siamak Heshmati, Amazon Web Services

Resumen

Este patrón le ayuda a integrar AWS Control Tower Account Factory Terraform (AFT) con el AWS IAM Identity Centerfin de configurar los permisos de varios Cuentas de AWS a escala. Este enfoque utiliza AWS Lambda funciones personalizadas para automatizar las asignaciones de conjuntos de permisos Cuentas de AWS que se administran como una organización. Esto agiliza el proceso porque no requiere la intervención manual del equipo de ingeniería de la plataforma. Esta solución puede mejorar la eficiencia, la seguridad y la coherencia operativas. Promueve un proceso de incorporación seguro y estandarizado AWS Control Tower, lo que lo hace indispensable para las empresas que priorizan la agilidad y la confiabilidad de su infraestructura de nube.

Requisitos previos y limitaciones

Requisitos previos

- Cuentas de AWS, gestionado mediante AWS Control Tower. Para obtener más información, consulte Primeros pasos con AWS Control Tower.
- Account Factory for Terraform, implementado en una cuenta dedicada en su entorno. Para obtener más información, consulte Deploy AWS Control Tower Account Factory para Terraform.
- Una instancia de IAM Identity Center configurada en su entorno. Para obtener más información, consulte Primeros pasos con IAM Identity Center.
- Un grupo de IAM Identity Center activo y configurado. Para obtener más información, consulte Añadir grupos a su Directorio de IAM Identity Center.
- La versión 3.9 o posterior de Python instalada

Limitaciones

- Esta solución solo se puede usar con cuentas que se administren mediante AWS Control Tower. Esta solución se implementa mediante Account Factory for Terraform.
- Este patrón no incluye instrucciones para configurar una federación de identidades con un origen de identidad. Para obtener más información sobre cómo completar esta configuración, consulte

los tutoriales sobre los orígenes de identidad de IAM Identity Center en la documentación de IAM Identity Center.

Arquitectura

Descripción general de AFT

AFT configura una canalización de Terraform que lo ayuda a aprovisionar y personalizar varias cuentas de AWS Control Tower. AFT sigue un GitOps modelo que automatiza los procesos de aprovisionamiento de cuentas en. AWS Control Tower Usted crea un archivo de Terraform de solicitud de cuenta y lo deposita en el repositorio. Esto inicia el flujo de trabajo de AFT para el aprovisionamiento de cuentas. Una vez completado el aprovisionamiento de la cuenta, AFT puede ejecutar automáticamente pasos de personalización adicionales. Para obtener más información, consulte la arquitectura AFT en la AWS Control Tower documentación.

AFT proporciona los siguientes repositorios principales:

- `aft-account-request`: este repositorio contiene código de Terraform para crear o actualizar Cuentas de AWS.
- `aft-account-customizations`: este repositorio contiene código Terraform para crear o personalizar recursos por cuenta.
- `aft-global-customizations`: este repositorio contiene código Terraform para crear o personalizar recursos para todas las cuentas a escala.
- `aft-account-provisioning-customizations`: este repositorio administra las personalizaciones que se aplican solo a cuentas específicas creadas y administradas con AFT. Por ejemplo, puede utilizar este repositorio para personalizar las asignaciones de usuarios o grupos en IAM Identity Center o para automatizar el cierre de cuentas.

Descripción general de la solución

Esta solución personalizada incluye una máquina de AWS Step Functions estados y una AWS Lambda función que asigna conjuntos de permisos a usuarios y grupos para varias cuentas. La máquina de estados implementada mediante este patrón funciona junto con la máquina de estados `aft_account_provisioning_customizations` de AFT preexistente. Un usuario envía una solicitud para actualizar las asignaciones de usuarios y grupos del IAM Identity Center al crear una nueva Cuenta de AWS cuenta o después de crearla. Para ello, insertan un cambio en el repositorio de `aft-account-request`. La solicitud para crear o actualizar una cuenta inicia una transmisión

en Amazon DynamoDB Streams. Esto inicia la función Lambda, que actualiza los usuarios y grupos del IAM Identity Center para el destino. Cuentas de AWS

A continuación se muestra un ejemplo de los parámetros que puede proporcionar en la función de Lambda para la asignación de conjuntos de permisos a los usuarios y grupos de destino:

```
custom_fields = {
    "InstanceArn"         = "<Organization ID>",
    "PermissionSetArn"    = "<Permission set ARN>",
    "PrincipalId"         = "<Principal ID>",
  }
```

Los parámetros de esta instrucción son los siguientes:

- `InstanceArn`: el nombre de recurso de Amazon (ARN) de la organización.
- `PermissionSetArn`: el ARN del conjunto de permisos.
- `PrincipalId`: el identificador de un usuario o grupo de IAM Identity Center al que se aplicará el conjunto de permisos

> **Note**
>
> Debe crear el conjunto de permisos, los usuarios y los grupos de destino antes de ejecutar esta solución.

Si bien el valor `InstanceArn` debe permanecer coherente, puede modificar la función de Lambda para asignar varios conjuntos de permisos a varias identidades de destino. Los parámetros de los conjuntos de permisos deben terminar en `PermissionSetArn` y los parámetros de los usuarios y grupos deben terminar en `PrincipalId`. Debe definir ambos atributos. A continuación se muestra un ejemplo de cómo definir varios conjuntos de permisos y dirigirse a usuarios y grupos:

```
custom_fields = {
    "InstanceArn"                    = "<Organization ID>",
    "AdminAccessPermissionSetArn"    = "<Admin privileges permission set ARN>",
    "AdminAccessPrincipalId"         = "<Admin principal ID>",
    "ReadOnlyAccessPermissionSetArn" = "<Read-only privileges permission set ARN>",
    "ReadOnlyAccessPrincipalId"      = "<Read-only principal ID>",
  }
```

El siguiente diagrama muestra un step-by-step flujo de trabajo que muestra cómo la solución actualiza los conjuntos de permisos para los usuarios y grupos del objetivo Cuentas de AWS a escala. Cuando el usuario inicia una solicitud de creación de cuenta, AFT inicia la máquina de estados `aft-account-provisioning-framework` de Step Functions. Esta máquina de estados inicia la función de Lambda `extract-alternate-sso`. La función Lambda asigna conjuntos de permisos a los usuarios y grupos del destino. Cuentas de AWS Estos usuarios o grupos pueden proceder de cualquier origen de identidad configurado en IAM Identity Center. Algunos ejemplos de orígenes de identidad son Okta, Active Directory o Ping Identity.

El diagrama muestra el siguiente flujo de trabajo al crear cuentas nuevas:

1. Un usuario envía un cambio de `custom_fields` al repositorio de `aft-account-request`.
2. AWS CodePipeline inicia un AWS CodeBuild trabajo que registra los metadatos definidos por el usuario en la tabla de `aft-request-audit` Amazon DynamoDB. Esta tabla tiene atributos para registrar metadatos definidos por el usuario. El atributo `ddb_event_name` define el tipo de operación de AFT:
   - Si el valor es`INSERT`, la solución asigna los permisos establecidos a las identidades de destino cuando se crea la nueva. Cuenta de AWS
   - Si el valor es`UPDATE`, la solución asigna los permisos establecidos a las identidades de destino después de crearlas Cuenta de AWS .
3. Amazon DynamoDB Streams inicia la función de Lambda `aft_alternate_sso_extract`.
4. La función `aft_alternate_sso_extract` Lambda asume una función AWS Identity and Access Management (IAM) en la AWS Control Tower cuenta de administración.
5. La función Lambda asigna los conjuntos de permisos a los usuarios y grupos de destino mediante una llamada a la API AWS SDK para Python (Boto3) create_account_assignment al Centro de identidades de IAM. Recupera el conjunto de permisos y las asignaciones de identidad de la tabla `aft-request-audit` de Amazon DynamoDB.
6. Cuando se completa el flujo de trabajo de Step Functions, los conjuntos de permisos se asignan a las identidades de destino.

Automatización y escala

AFT funciona a escala mediante el Servicios de AWS uso de CodePipeline DynamoDB y Lambda, que son altamente escalables. AWS CodeBuild Para una automatización adicional, puede integrar

esta solución con un sistema de gestión de incidencias o tickets, como Jira. Para obtener más información, consulte la sección Información adicional de este patrón.

Tools (Herramientas)

Servicios de AWS

- Account Factory for Terraform (AFT) es la principal herramienta de esta solución. El `aft-account-provisioning-customizations` repositorio contiene el código de Terraform para crear personalizaciones Cuentas de AWS, como asignaciones personalizadas para usuarios o grupos del IAM Identity Center.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Step Functionses un servicio de organización sin servidor que le ayuda a combinar AWS Lambda funciones y otras Servicios de AWS para crear aplicaciones críticas para la empresa.

Otras herramientas

- Python es un lenguaje de programación informático de uso general.
- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.

Repositorio de código

El repositorio de código para AFT está disponible en el repositorio GitHub AWS Control Tower Account Factory for Terraform. El código de este patrón está disponible en el repositorio Govern SSO Assignments para Cuentas de AWS usar Account Factory for Terraform (AFT).

Prácticas recomendadas

- Comprenda el modelo de responsabilidad compartida de AWS.
- Siga las recomendaciones de seguridad para. AWS Control Tower Para obtener más información, consulte Seguridad en AWS Control Tower.

- Siga el principio de privilegio mínimo Para obtener más información, consulte Aplicar permisos de privilegio mínimo.
- Cree conjuntos de permisos y roles de IAM específicos para grupos y unidades de negocio.

Epics

Implementar la solución

Tarea	Descripción	Habilidades requeridas
Crear un rol de IAM.	En la cuenta AWS Control Tower de administración, utilice Terraform para crear un rol de IAM. Este rol tiene acceso entre cuentas y una política de confianza que permite el acceso federado desde el proveedor de identidades. También tiene permisos para conceder acceso a otras cuentas a través de ella. AWS Control Tower La función de Lambda asumirá este rol. Haga lo siguiente: 1. Descarga el `AFTCrossAccountRole.tf` archivo del repositorio GitHub de códigos. 2. Modifique el `AFTCrossAccountRole.tf` archivo según sea necesario para su AWS entorno.	AWS DevOps, arquitecto de nube

Tarea	Descripción	Habilidades requeridas

	3. En Terraform, introduzca los siguientes comandos para crear este rol de IAM:
	
	`terraform init`
	`terraform plan`
	`terraform apply`
	
	4. Valide que el rol se haya implementado correctamente y que tenga el acceso entre cuentas esperado.	

Tarea	Descripción	Habilidades requeridas
Personalice la solución para su entorno.	1. Ingresa el siguiente comando para clonar las asignaciones de Govern SSO para Cuentas de AWS usar el repositorio Account Factory for Terraform (AFT) en tu estación de trabajo local. `git clone https://github.com/aws-samples/aft-custom-sso-assignment.git` 2. En la carpeta `aft-account-provisioning-customizations/terraform` , abra el archivo `variables.tf` . 3. Modifique las variables según sea necesario para su entorno. 4. Guarde y cierre el archivo `variables.tf` . 5. Abra el archivo `account-request.tf` en su repositorio de `aft-account-request` . 6. Modifique los parámetros `custom_fields` para definir los conjuntos de permisos y los usuarios y grupos de destino. Para obtener más informaci	AWS DevOps, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	ón, consulte la sección Arquitectura de este patrón. 7. Guarde y cierre el archivo `account-request.tf` .	
Implemente la solución.	1. En el repositorio clonado, copie el contenido de la carpeta `terraform` y péguelo en la carpeta `terraform` del repositorio `aft-account-provisioning-customizations` . 2. En la cuenta de administración de AFT, inicie la canalización de `ct-aft-account-provisioning-customizations` . Esta acción implementa la solución personalizada. Para obtener instrucciones, consulte Iniciar una canalización en CodePipeline. 3. Valide que los recursos se hayan implementado correctamente en la cuenta de administración de AFT.	AWS DevOps, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
Configure una conexión de repositorio de código.	Configure una conexión entre el repositorio de código donde almacenará los archivos de configuración y su Cuenta de AWS. Para obtener instrucciones, consulta la sección sobre cómo añadir proveedores de fuentes de terceros a las canalizaciones que se CodeConnections encuentra en la AWS CodePipeline documentación.	AWS DevOps, arquitecto de nube

Uso de la solución

Tarea	Descripción	Habilidades requeridas
Inicie la canalización de AFT para implementar una nueva cuenta.	Siga las instrucciones de Aprovisione una nueva cuenta con AFT para iniciar la canalización que crea una nueva Cuenta de AWS en su AWS Control Tower entorno. Espere a que se complete la creación de la cuenta.	AWS DevOps, arquitecto de nube
Valide los cambios.	1. Abra la consola de AWS IAM Identity Center. 2. En la lista de cuentas, elija la cuenta que acaba de crear. 3. Valide que se hayan asignado los conjuntos de permisos para conceder	AWS DevOps, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	acceso a los usuarios y grupos de destino.	

Resolución de problemas

Problema	Solución
La asignación del conjunto de permisos no funciona.	Asegúrese de que el ARN del grupo, el ID de la organización y los parámetros de Lambda sean correctos. Para ver ejemplos, consulte la sección de Información general de la solución de este patrón.
La actualización del código en el repositorio no inicia la canalización.	Este problema está relacionado con la conectividad entre tu repositorio Cuenta de AWS y el tuyo. En el Consola de administración de AWS, valide que la conexión esté activa. Para obtener más información, consulte GitHub las conexiones en la AWS CodePipeline documentación.

Información adicional

Integración con una herramienta de gestión de tickets

Puede optar por integrar esta solución con una herramienta de gestión de incidencias o incidencias, como Jira o ServiceNow. En el diagrama siguiente se muestra un ejemplo de flujo de trabajo de esta opción. Puede integrar la herramienta de gestión de tickets con los repositorios de soluciones de AFT mediante los conectores de su herramienta. Para ver los conectores de Jira, consulte Integrar Jira con. GitHub Para ver los ServiceNow conectores, consulte Integrar con. GitHub Incluso puede crear soluciones personalizadas que requieran que los usuarios proporcionen un ID de ticket como parte de la aprobación de la solicitud de extracción. Si se aprueba una solicitud para crear una nueva Cuenta de AWS mediante AFT, ese evento podría iniciar un flujo de trabajo que añada campos

personalizados al `aft-account-request` GitHub repositorio. Puede diseñar cualquier flujo de trabajo personalizado que cumpla con los requisitos de su caso de uso.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Los usuarios solicitan una asignación de conjuntos de permisos personalizada en una herramienta de administración de tickets, como Jira.
2. Una vez aprobado el caso, se inicia un flujo de trabajo para actualizar la asignación del conjunto de permisos. (Opcional) Puede utilizar complementos para la automatización personalizada de este paso.
3. Los operadores envían el código de Terraform con los parámetros del conjunto de permisos actualizados al repositorio de `aft-account-request` en una ramificación de desarrollo o característica.
4. GitHub Las acciones se inician AWS CodeBuild mediante una llamada a OpenID Connect (OIDC). CodeBuild realiza escaneos de seguridad de infraestructura como código (IaC) mediante herramientas como tfsec y checkov. Advierte a los operadores de cualquier infracción de seguridad.
5. Si no se detecta ninguna infracción, GitHub Actions crea una solicitud de extracción automática y asigna una revisión del código a sus propietarios. También crea una etiqueta para la solicitud de extracción.
6. Si el propietario del código aprueba la revisión del código, se inicia otro flujo de trabajo de GitHub Actions. Comprueba los estándares de las solicitudes de extracción, que incluyen:
   - Si el título de la solicitud de extracción cumple con los requisitos.
   - Si el cuerpo de la solicitud de extracción contiene números de caso aprobados.
   - Si la solicitud de extracción está correctamente etiquetada.
7. Si las solicitudes de extracción cumplen con los estándares, GitHub Actions inicia el flujo de trabajo del producto AFT. Utiliza el inicio de la `ct-aft-account-request` canalización AWS CodePipeline. Esta canalización inicia la máquina de estado `aft-account-provisioning-framework` personalizada en Step Functions. Esta máquina de estado funciona como se describió anteriormente en la sección de Información general de la solución de este patrón.

Implementación del Generador de cuentas para Terraform (AFT) mediante una canalización de arranque

Vinicius Elias y Edgar Costa Filho, Amazon Web Services

Resumen

Este patrón proporciona un método sencillo y seguro para implementar AWS Control Tower Account Factory for Terraform (AFT) desde la cuenta de administración de AWS Organizations. El núcleo de la solución es una CloudFormation plantilla que automatiza la configuración de AFT mediante la creación de una canalización de Terraform, que está estructurada para adaptarse fácilmente a la implementación inicial o a las actualizaciones posteriores.

La seguridad y la integridad de los datos son las principales prioridades AWS, por lo que el archivo de estado de Terraform, que es un componente fundamental que rastrea el estado de la infraestructura y las configuraciones administradas, se almacena de forma segura en un depósito de Amazon Simple Storage Service (Amazon S3). Este bucket está configurado con varias medidas de seguridad, como el cifrado del servidor y políticas para bloquear el acceso público, a fin de garantizar que el estado de Terraform esté protegido contra el acceso no autorizado y las filtraciones de datos.

La cuenta de administración organiza y supervisa todo el entorno, por lo que es un recurso fundamental. AWS Control Tower Este patrón sigue las AWS mejores prácticas y garantiza que el proceso de implementación no solo sea eficiente, sino que también se alinee con los estándares de seguridad y gobernanza, a fin de ofrecer una forma integral, segura y eficiente de implementar la AFT en su entorno. AWS

Para obtener más información sobre AFT, consulte la documentación de AWS Control Tower.

Requisitos previos y limitaciones

Requisitos previos

- Un entorno básico de AWS múltiples cuentas con las siguientes cuentas como mínimo: cuenta de administración, cuenta de Log Archive, cuenta de auditoría y una cuenta adicional para la administración de AFT.
- Un AWS Control Tower entorno establecido. La cuenta de administración debe estar configurada correctamente, ya que la CloudFormation plantilla se implementará en ella.

- Los permisos necesarios en la cuenta AWS de administración. Necesitará permisos suficientes para crear y administrar recursos, como depósitos, AWS Lambda funciones AWS Identity and Access Management (IAM) y AWS CodePipeline proyectos de S3.
- Familiaridad con Terraform. Es importante comprender los conceptos básicos y el flujo de trabajo de Terraform porque la implementación implica generar y administrar las configuraciones de Terraform.

Limitaciones

- Tenga en cuenta las cuotas de los recursos de AWS de su cuenta. La implementación puede crear varios recursos y encontrar cuotas de servicio podría impedir el proceso de implementación.
- La plantilla está diseñada para versiones específicas de Terraform y Servicios de AWS. La actualización o el cambio de versiones pueden requerir modificaciones en la plantilla.
- La plantilla no admite los servicios del sistema de control de versiones (VCS) autogestionado, como Enterprise. GitHub

Versiones de producto

- Terraform, versión 1.6.6 o posterior
- Versión 1.11 o posteriores de AFT

Arquitectura

Pila de tecnología de destino

- CloudFormation
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- Amazon EventBridge
- IAM
- AWS Lambda
- Amazon S3

Arquitectura de destino

En el siguiente diagrama se ilustra la implementación descrita en este patrón.

El flujo de trabajo consta de tres tareas principales: creación de los recursos, generación del contenido y ejecución de la canalización.

Creación de los recursos

La CloudFormation plantilla que se proporciona con este patrón crea y configura todos los recursos necesarios, en función de los parámetros que selecciones al implementar la plantilla. Como mínimo, la plantilla crea los siguientes recursos:

- Una CodePipeline canalización para implementar la AFT
- Un bucket de S3 para almacenar el archivo de estado de Terraform asociado a la implementación de AFT
- Dos CodeBuild proyectos para implementar el plan Terraform y aplicar comandos en diferentes etapas del proceso
- Funciones y servicios de IAM CodeBuild CodePipeline
- Un segundo bucket de S3 para almacenar artefactos de tiempo de ejecución de la canalización

Según el proveedor de VCS que seleccione (CodeCommit o el VCS externo), la plantilla crea los siguientes recursos.

- Para CodeCommit:
  - Un CodeCommit repositorio para almacenar el código de arranque de AFT Terraform
  - Una EventBridge regla para capturar los cambios CodeCommit del repositorio en la sucursal `main`
  - Otra función de IAM para la regla EventBridge
- Para cualquier otro proveedor de VCS externo, como: GitHub
  - Una conexión AWS CodeConnections

Además, al seleccionar CodeCommit como proveedor de VCS, si se establece el `Generate AFT Files` parámetro `entrue`, la plantilla crea los siguientes recursos adicionales para generar el contenido:

- Un depósito de S3 para almacenar el contenido generado y usarlo como fuente del repositorio CodeCommit
- Una función de Lambda para procesar los parámetros dados y generar el contenido apropiado
- Una función de IAM para ejecutar la función de Lambda
- Un recurso CloudFormation personalizado que ejecuta la función Lambda cuando se implementa la plantilla

Generación del contenido

Para generar los archivos de arranque de AFT y su contenido, la solución utiliza una función de Lambda y un bucket de S3. La función crea una carpeta en el bucket y, a continuación, crea dos archivos dentro de la carpeta: `main.tf` y `backend.tf`. La función también procesa los CloudFormation parámetros proporcionados y rellena estos archivos con código predefinido, sustituyendo los valores de los parámetros respectivos.

Para ver el código que se utiliza como plantilla para generar los archivos, consulte el GitHub repositorio de la solución. Básicamente, los archivos se generan de la siguiente manera.

main.tf

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory?
ref=<aft_version>"

  # Required variables
  ct_management_account_id  = "<ct_management_account_id>"
  log_archive_account_id    = "<log_archive_account_id>"
  audit_account_id          = "<audit_account_id>"
  aft_management_account_id = "<aft_management_account_id>"
  ct_home_region            = "<ct_home_region>"

  # Optional variables
  tf_backend_secondary_region = "<tf_backend_secondary_region>"
  aft_metrics_reporting       = "<false|true>"

  # AFT Feature flags
  aft_feature_cloudtrail_data_events      = "<false|true>"
  aft_feature_enterprise_support          = "<false|true>"
  aft_feature_delete_default_vpcs_enabled = "<false|true>"
```

```
  # Terraform variables
  terraform_version      = "<terraform_version>"
  terraform_distribution = "<terraform_distribution>"

  # VCS variables (if you have chosen an external VCS)
  vcs_provider                                = "<github|githubenterprise|gitlab|
gitlabselfmanaged|bitbucket>"
  account_request_repo_name                   = "<org-name>/aft-account-request"
  account_customizations_repo_name            = "<org-name>/aft-account-
customizations"
  account_provisioning_customizations_repo_name = "<org-name>/aft-account-provisioning-
customizations"
  global_customizations_repo_name             = "<org-name>/aft-global-
customizations"

}
```

backend.tf

```
terraform {
  backend "s3" {
    region = "<aft-main-region>"
    bucket = "<s3-bucket-name>"
    key    = "aft-setup.tfstate"
  }
}
```

Durante la creación del CodeCommit repositorio, si estableces el `Generate AFT Files` parámetro en`true`, la plantilla utilizará el depósito de S3 con el contenido generado como fuente de la `main` rama para rellenar automáticamente el repositorio.

Ejecutando la canalización

Una vez creados los recursos y configurados los archivos de arranque, se ejecuta la canalización. La primera etapa (Origen) busca el código fuente de la ramificación principal del repositorio, y la segunda etapa (Compilación) ejecuta el comando de planificación de Terraform y genera los resultados para su revisión. En la tercera etapa (Aprobación), la canalización espera a que se lleve a cabo una acción manual para aprobar o rechazar la última etapa (Implementación). En la última etapa, la canalización ejecuta el comando `apply` de Terraform utilizando como entrada el resultado del comando `plan` de Terraform anterior. Por último, un rol entre cuentas y los permisos de la cuenta de administración se utilizan para crear los recursos de AFT en la cuenta de administración de AFT.

> **Note**
>
> Si selecciona un proveedor de VCS externo, deberá autorizar la conexión con las credenciales de su proveedor de VCS. Para completar la configuración, sigue los pasos que se indican en la documentación de la consola de AWS Developer Tools sobre cómo actualizar una conexión pendiente.

Tools (Herramientas)

Servicios de AWS

- CloudFormationle ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en Cuentas de AWS todas las regiones.
- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- AWS CodeCommit es un servicio de control de versiones que permite almacenar y administrar repositorios de Git de forma privada sin necesidad de administrar su propio sistema de control de origen.
- AWS CodePipeline permite diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software y automatizar los pasos necesarios para lanzar los cambios en el software de manera continua.
- AWS CodeConnectionspermite que AWS los recursos y servicios, por ejemplo CodePipeline, se conecten a repositorios de código externos, por ejemplo. GitHub
- AWS Lambda es un servicio de computación que ejecuta código como respuesta a eventos y administra automáticamente los recursos de computación, lo que proporciona una forma rápida de crear una aplicación moderna y sin servidor para producción.
- AWS SDK para Python (Boto3)es un kit de desarrollo de software que le ayuda a integrar su aplicación, biblioteca o script de Python con Servicios de AWS.

Otras herramientas

- Terraform es una herramienta de infraestructura como código (IaC) que le permite crear, cambiar y versionar la infraestructura de manera segura y eficiente. Esto incluye componentes de bajo nivel,

como instancias de computación, almacenamiento y redes, y componentes de alto nivel, como entradas de DNS y característica de SaaS.

- Python es un lenguaje de programación potente y fácil de aprender. Cuenta con estructuras de datos eficientes y de alto nivel y proporciona un enfoque simple pero efectivo de la programación orientada a objetos.

Repositorio de código

El código de este patrón está disponible en el repositorio bootstrap Pipeline de GitHub AFT.

Para ver el repositorio AFT oficial, consulte AWS Control Tower Account Factory for Terraform en GitHub.

Prácticas recomendadas

Al implementar AFT mediante la CloudFormation plantilla proporcionada, le recomendamos que siga las mejores prácticas para garantizar una implementación segura, eficiente y exitosa. Las pautas y recomendaciones clave para implementar y operar AFT incluyen lo siguiente:

- Revisión exhaustiva de los parámetros: revise y comprenda detenidamente cada parámetro de la CloudFormation plantilla. La configuración correcta de los parámetros es crucial para la configuración y el funcionamiento correctos de AFT.
- Actualizaciones periódicas de la plantilla: mantenga la plantilla actualizada con las últimas AWS funciones y versiones de Terraform. Las actualizaciones periódicas lo ayudarán a aprovechar las nuevas funciones y a mantener la seguridad.
- Control de versiones: fije la versión de su módulo de AFT y, si es posible, utilice una implementación de AFT independiente para realizar las pruebas.
- Alcance: utilice AFT únicamente para implementar barreras de protección y personalizaciones de infraestructura. No use AFT para implementar la aplicación.
- Lint y validación: la canalización de AFT requiere una configuración de Terraform de tipo Lint y que esté validada. Ejecute Lint, valide y pruebe todo antes de enviar la configuración a los repositorios de AFT.
- Módulos de Terraform: cree código de Terraform reutilizable como módulos y especifique siempre las versiones de Terraform y del AWS proveedor para que se ajusten a los requisitos de su organización.

Epics

Configure y configure el entorno AWS

Tarea	Descripción	Habilidades requeridas
Prepare el AWS Control Tower entorno.	Instálelo y AWS Control Tower configúrelo en su AWS entorno para garantiza r una administración y un gobierno centralizados para su Cuentas de AWS. Para obtener más información, consulte Primeros pasos AWS Control Tower en la AWS Control Tower documentación.	Administrador de la nube
Iniciar la cuenta de administr ación de AFT.	Utilice AWS Control Tower Account Factory para lanzar una nueva Cuenta de AWS que sirva como su cuenta de administración de AFT. Para obtener más información, consulte Aprovisionar cuentas con AWS Service Catalog Account Factory en la AWS Control Tower documentación.	Administrador de la nube

Implemente la CloudFormation plantilla en la cuenta de administración

Tarea	Descripción	Habilidades requeridas
Inicie la CloudFormation plantilla.	En esta epopeya, despliega la CloudFormation plantilla proporcionada con esta solución para configurar la canalización de arranque de	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	AFT en su cuenta AWS de administración. La canalización implementa la solución AFT en la cuenta de administración de AFT que configuró en la épica anterior. Paso 1: Abre la consola CloudFormation • Inicie sesión en la CloudFormation consola Consola de administración de AWS y ábrala. Asegúrese de operar en la región AWS Control Tower principal correcta. Paso 2: crear una nueva pila 1. Elija crear una nueva pila. 2. Selecciona la opción de cargar un archivo de plantilla y carga la CloudFormation plantilla que viene con este patrón. Paso 3: configurar los parámetros de la pila • `VCS Provider`: seleccione el proveedor del sistema de control de versiones (VCS) que desee utilizar. Puedes seleccionar un VCS externo,	

Tarea	Descripción	Habilidades requeridas
	por ejemplo GitHub, o usarlo CodeCommit si tu cuenta tiene permiso para usar el servicio. • `Repository Name` : especifique el nombre del repositorio para almacenar el módulo de arranque de AFT. Para los proveedores de VCS externos, utilice la ruta completa, incluido el nombre de la organización (por ejemplo, `my-github-org/my-repo`). • `Branch Name`: especifique la ramificación del repositorio de origen. • `CodeBuild Docker Image`: Elija el archivo que desee utilizar como imagen base de CodeBuild Docker. • Si configura el proveedor de VCS en una opción distinta de CodeCommit, vaya al paso 8. Paso 4: decidir la generación de archivos • Si lo ha seleccionado CodeCommit como proveedor de VCS, puede utilizar el `Generate AFT Files` parámetro para	

Tarea	Descripción	Habilidades requeridas
	controlar la generación de los archivos de despliegue de AFT predeterminados. Establezca este parámetro en: • `true` para crear y almacenar automátic amente los archivos de implementación de AFT en el repositorio especific ado. • `false` si desea gestionar manualmente la creación del archivo o si ya tiene los archivos en su lugar. • Si ha seleccionado `false`, vaya al paso 8; de lo contrario, siga primero los pasos 5-7. Paso 5: Rellene los detalles de AWS Control Tower la cuenta AFT • Si establece el `Generate AFT Files` parámetro en`true`, proporcione la siguiente información AWS Control Tower y la informaci ón específica de la cuenta AFT. • `Log Archive Account ID`: El ID de la cuenta	

Tarea	Descripción	Habilidades requeridas
	de Log Archive es. AWS Control Tower • `Audit Account ID`: El ID de la cuenta de auditoría en AWS Control Tower. • `AFT Management Account ID`: ID de la cuenta de administración de AFT que creó en la primera épica. • `AFT Main Region`y`AFT Secondary Region`: El principal y el secundario Regiones de AWS para el despliegue de AFT. Paso 6: configurar las opciones de AFT • Configure los informes de métricas: • `AFT Enable Metrics Reporting` : habilite o deshabilite los informes de métricas de AFT. Para obtener más informaci ón, consulte las métricas operativas en la AWS Control Tower documenta ción. • Defina las opciones de características de AFT:	

Tarea	Descripción	Habilidades requeridas
	• `Enable AFT CloudTrail Data Events`: Habilite CloudTrail los eventos de datos en todas las cuentas administradas por AFT. Para obtener más información, consulte AWS CloudTrail los eventos de datos en la AWS Control Tower documentación. • `Enable AFT Enterprise Support` : habilite Enterprise Support en todas las cuentas administradas de AFT. Para obtener más información, consulte el plan AWS Enterprise Support en la AWS Control Tower documentación. • `Enable AFT Delete Default VPC`: Elimine todo únicamente VPCs en la cuenta de administración de AFT. Para obtener más información, consulte Eliminar la VPC AWS predeterminada en la AWS Control Tower documentación.	

Tarea	Descripción	Habilidades requeridas
	Paso 7: especificar las versiones • `AFT Terraform Version`: elija la versión de Terraform que usar en las canalizaciones de AFT. • `AFT Version`: defina la versión de AFT para la implementación. Mantenga la configuración predeterminada (`latest`) para usar la versión de AFT más reciente. Paso 8: revisar y crear la pila • Revise todos los parámetros y configuraciones. Si todo está en orden, proceda a crear la pila. Paso 9: supervisar la creación de la pila • CloudFormation aprovisiona y configura los recursos que ha definido. Supervise el proceso de creación de la pila en la CloudFormation consola. Este proceso podría tardar varios minutos.	

Tarea	Descripción	Habilidades requeridas
	Paso 10: comprobar la implementación • Cuando el estado de la pila muestre CREATE_COMPLETE, compruebe que todos los recursos se hayan creado correctamente. • En la sección Salidas, anote el valor de `Terraform BackendBucketName` .	

Relleno y validación del repositorio y la canalización de arranque de AFT

Tarea	Descripción	Habilidades requeridas
Opción 1: Rellenar el repositorio de arranque de AFT para un VCS externo.	Si configura el proveedor de VCS como un VCS externo (no lo haga CodeCommit), siga estos pasos. (Opcional) Tras implementar la CloudFormation plantilla , puede rellenar o validar el contenido del repositorio bootstrap de AFT recién creado y comprobar si la canalización se ha ejecutado correctamente. Paso 1: actualizar la conexión 1. En la CodePipeline consola, en el panel de navegación,	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	seleccione Configuración, Conexiones. 2. Seleccione la conexión `aft-vcs-connection` . El estado debería ser `Pending`. 3. Elija Actualizar conexión pendiente y siga las instrucciones de Update a pending connection en la documentación de la consola de las herramientas para desarrolladores. 4. Cuando el estado de la conexión sea `Available` , vaya al siguiente paso. Paso 2: rellenar el repositorio 1. Utilice sus credenciales de VCS externas para clonar el repositorio que especificó en la plantilla en su máquina local. Si ha mantenido el nombre predeterminado, el repositorio se llamará `aft-setup` . 2. En el repositorio, cree una carpeta llamada `terraform` con dos archivos vacíos dentro: `backend.tf` y `main.tf`.	

Tarea	Descripción	Habilidades requeridas

	3. Abra el archivo `backend.tf` y agregue este fragmento de código:
	
	`terraform {`
	`  backend "s3" {`
	`  region = "<aft-main-region>"`
	`  bucket = "<s3-bucket-name>"`
	`  key  = "aft-setup"`
	`  }`
	`}`
	
	En el archivo:
	• Sustituya `<aft-main-region>` por la región de AFT principal. Debe coincidir con la región AWS Control Tower principal.
	• Sustituya `<s3-bucket-name>` por el nombre del bucket de backend de Terraform. Puede encontrarlo en el `Terraform BackendBucketName` resultado generado por la CloudFormation plantilla que implementó anteriormente.
	4. Abra el archivo `main.tf` y utilice uno de los ejemplos disponibles en el repositor	

Tarea	Descripción	Habilidades requeridas
	io de AFT para implement ar AFT. Por ejemplo, puedes trabajar con tu proveedor de VCS preferido (CodeCommit GitHub, o Bitbucket) o personalizar la VPC de AFT. Para ver más opciones de entrada de AFT, consulte el archivo README en el repositorio de AFT. Paso 2: confirmar y enviar los cambios • Una vez que haya creado y rellenado la carpeta y los archivos, confirme los cambios y cargue el código en el repositor io. La canalización se inicia automáticamente, se ejecuta en las etapas Origen y Compilación y, a continuación, espera a que se lleve a cabo una acción de aprobación antes de la etapa Implementación.	

Tarea	Descripción	Habilidades requeridas
Opción 2: llene el repositorio bootstrap de AFT para. CodeCommit	Si configuras el proveedor de VCS en CodeCommit, sigue estos pasos. (Opcional) Tras implementar la CloudFormation plantilla , puede rellenar o validar el contenido del repositorio bootstrap de AFT recién creado y comprobar si la canalización se ha ejecutado correctamente. Si establece el parámetro `Generate AFT Files` en `true`, pase a la siguiente historia (validación de la canalización). Paso 1: rellenar el repositorio 1. Abra la consola de AWS CodeCommit y seleccione el repositorio recién creado. Si ha mantenido el nombre predeterminado, el nombre del repositorio debería ser `aft-setup` . 2. Clone el repositorio en su máquina local mediante SSH, HTTPS o HTTPS (GRC) y ábralo en un editor. 3. Cree una carpeta llamada `terraform` y dos	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	archivos vacíos dentro: `backend.tf` y `main.tf`. 4. Abra el archivo `backend.tf` y agregue este fragmento de código: `terraform { backend "s3" { region = "<aft-main-region>" bucket = "<s3-bucket-name>" key = "aft-setup" } }` En el archivo: • Sustituya `<aft-main-region>` por la región de AFT principal. Debe coincidir con la región AWS Control Tower principal. • Sustituya `<s3-bucket-name>` por el nombre del bucket de backend de Terraform. Puede encontrarlo en el `Terraform BackendBucketName` resultado generado por la CloudFormation plantilla que implementó anteriormente.	

Tarea	Descripción	Habilidades requeridas
	5. Abra el archivo `main.tf` y utilice uno de los ejemplos disponibles en el repositorio de AFT para implementar AFT. Por ejemplo, puedes trabajar con tu proveedor de sistema de control de versiones (VCS) preferido (CodeCommit GitHub, o Bitbucket) o personalizar la VPC de AFT. Para ver más opciones de entrada de AFT, consulte el archivo README en el repositorio de AFT. Paso 2: confirmar y enviar los cambios • Una vez que haya creado y rellenado la carpeta y los archivos, confirme los cambios y cargue el código en el repositorio. La canalización se inicia automáticamente, se ejecuta en las etapas Origen y Compilación y, a continuación, espera a que se lleve a cabo una acción de aprobación antes de la etapa Implementación.	

Tarea	Descripción	Habilidades requeridas
Validar la canalización de arranque de AFT.	Paso 1: Ver la canalización • Abre la CodePipeline consola y comprueba si la `aft-bootstrap-pipeline` canalización se inició correctamente. Debería estar ejecutando un plan de Terraform o esperando una acción de aprobación manual. Paso 2: aprobar los resultados del plan de Terraform • Para revisar los resultados del plan de Terraform, puede consultar los registros de ejecución de la etapa Compilación y, a continuación, aprobar o rechazar la ejecución en la etapa Aprobación. Si la aprueba, la canalización empezará a implementar los recursos de AFT en la cuenta de administración de AFT proporcionada. Paso 3: esperar a la implementación • Espere a que la canalización se ejecute correctamente. Este proceso tarda	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	unos 30 minutos. Los errores que pueda encontrar suelen deberse a las cuotas de la API. En estos casos, puede volver a ejecutar la canalización para continuar con la implementación. Paso 4: comprobar los recursos creados • Acceda a la cuenta de administración de AFT y confirme que se hayan creado los recursos.	

Resolución de problemas

Problema	Solución
La función Lambda personalizada incluida en la CloudFormation plantilla falla durante la implementación.	Compruebe la función Lambda en los CloudWatch registros de Amazon para identificar el error. Los registros proporcionan información detallada y pueden ayudar a identificar el problema específico. Confirme que la función de Lambda tiene los permisos necesarios y que las variables del entorno se han configurado correctamente.
Se producen errores en la creación o administración de los recursos a causa de permisos inadecuados.	Revise las funciones y políticas de IAM asociadas a la función CodeBuild Lambda y otros servicios involucrados en la implementación. Confirme que tengan los permisos necesarios. Si tiene problemas con los

Problema	Solución
	permisos, ajuste las políticas de IAM para conceder el acceso necesario.
Está utilizando una versión anticuada de la CloudFormation plantilla con versiones más recientes Servicios de AWS o de Terraform.	Actualiza la CloudFormation plantilla con regularidad para que sea compatible con las versiones más recientes AWS y las de Terraform. Consulte las notas de la versión o la documentación para ver si hay cambios o requisitos específicos de la versión.
Servicio de AWS Las cuotas se alcanzan durante el despliegue.	Antes de implementar la canalización, compruebe Servicio de AWS las cuotas de recursos, como los buckets de S3, las funciones de IAM y las funciones de Lambda. Solicite aumentos si fuera necesario. Para obtener más información, consulte Servicio de AWS las cuotas en el sitio web. AWS
Se producen errores debido a parámetros de entrada incorrectos en la CloudFormation plantilla.	Compruebe todos los parámetros de entrada para ver si hay errores tipográficos o valores incorrectos. Confirme que los identificadores de recursos, como los nombres de cuentas IDs y regiones, sean correctos.

Recursos relacionados

Para implementar este patrón correctamente, revise los siguientes recursos. En estos recursos se proporciona información y orientación adicionales que pueden tener un valor incalculable para configurar y administrar AFT mediante CloudFormation.

AWSdocumentación:

- AWS Control Tower La guía del usuario ofrece información detallada sobre la configuración y la administración AWS Control Tower.
- CloudFormation la documentación proporciona información sobre las CloudFormation plantillas, las pilas y la administración de recursos.

Políticas de IAM y prácticas recomendadas:

- Las prácticas recomendadas de seguridad en IAM explican cómo ayudar a proteger los AWS recursos mediante el uso de las funciones y políticas de IAM.

Terraform en: AWS

- La documentación de Terraform AWS Provider proporciona información completa sobre el uso de Terraform con. AWS

Servicio de AWS cuotas:

- Servicio de AWS cuotas proporciona información sobre cómo ver Servicio de AWS las cuotas y cómo solicitar aumentos.

Administre los productos de AWS Service Catalog en varias cuentas y regiones de AWS

Ram Kandaswamy, Amazon Web Services

Resumen

Service Catalog, de Amazon Web Services (AWS), simplifica y acelera la gobernanza y la distribución de plantillas de infraestructura como código (IaC) para las empresas. Utiliza las CloudFormation plantillas de AWS para definir un conjunto de recursos de AWS (pilas) necesarios para un producto. AWS CloudFormation StackSets amplía esta funcionalidad al permitirle crear, actualizar o eliminar pilas en varias cuentas y regiones de AWS con una sola operación.

Los administradores de AWS Service Catalog crean productos mediante CloudFormation plantillas creadas por desarrolladores y las publican. A continuación, estos productos se asocian a una cartera y se imponen restricciones en materia de gobernanza. Para que sus productos estén disponibles para los usuarios de otras cuentas o unidades organizativas de AWS (OUs), normalmente comparte su cartera con ellos. Este patrón describe un enfoque alternativo para administrar las ofertas de productos de AWS Service Catalog que se basa en AWS CloudFormation StackSets. En lugar de compartir carteras, se usan restricciones de conjuntos de pilas para establecer las regiones y cuentas de AWS en las que se puede implementar y usar su producto. Con este enfoque, puede aprovisionar sus productos de AWS Service Catalog en varias cuentas y regiones de AWS OUs, y administrarlos desde una ubicación central, a la vez que cumple con sus requisitos de gobierno.

Ventajas de este enfoque:

- El producto se aprovisiona y administra desde la cuenta principal y no se comparte con otras cuentas.
- Este enfoque proporciona una vista consolidada de todos los productos aprovisionados (pilas) basados en un producto específico.
- La configuración con AWS Service Management Connector es más sencilla, ya que solo se dirige a una cuenta.
- Es más fácil consultar y usar los productos de AWS Service Catalog.

Requisitos previos y limitaciones

Requisitos previos

- CloudFormation Plantillas de AWS para iAC y control de versiones
- Configuración de múltiples cuentas y AWS Service Catalog para aprovisionar y administrar los recursos de AWS

Limitaciones

- Este enfoque utiliza AWS CloudFormation StackSets y se StackSets aplican las siguientes limitaciones:
  - StackSets no admite el despliegue CloudFormation de plantillas a través de macros. Si utiliza una macro para preprocesar la plantilla, no podrá utilizar una implementación StackSets basada.
  - StackSets ofrece la posibilidad de desasociar una pila del conjunto de pilas, de forma que puedas segmentar una pila específica para solucionar un problema. Sin embargo, una pila disociada no se puede volver a asociar al conjunto de pilas.
- AWS Service Catalog genera StackSet nombres automáticamente. Actualmente, la solución no es personalizable.

Arquitectura

Arquitectura de destino

1. El usuario crea una CloudFormation plantilla de AWS para aprovisionar los recursos de AWS, en formato JSON o YAML.
2. La CloudFormation plantilla crea un producto en AWS Service Catalog, que se añade a una cartera.
3. El usuario crea un producto aprovisionado, que crea CloudFormation pilas en las cuentas de destino.
4. Cada pila aprovisiona los recursos especificados en las CloudFormation plantillas.

Tools (Herramientas)

Servicios de AWS

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Service Catalog le ayuda a administrar de forma centralizada los catálogos de servicios de TI aprobados para AWS. Los usuarios finales pueden implementar rápidamente solo los servicios de TI aprobados que necesitan, de acuerdo con las limitaciones establecidas por su organización.

Epics

Aprovisione productos entre cuentas

Tarea	Descripción	Habilidades requeridas
Cree una cartera.	Una cartera es un contenedor que incluye uno o más productos agrupados en función de criterios específicos. El uso de una cartera para sus productos le ayuda a aplicar restricciones comunes a todo su conjunto de productos. Para crear una cartera, siga las instrucciones de la documentación de AWS Service Catalog. Si usa la CLI de AWS, aquí tiene un comando de ejemplo: `aws servicecatalog create-portfolio --provider-name my-provider --display-name my-portfolio`	AWS Service Catalog, IAM

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte la documentación de AWS CLI.	
Cree una CloudFormation plantilla.	Cree una CloudFormation plantilla que describa los recursos. Los valores de las propiedades de los recursos deben parametrizarse cuando proceda.	AWS CloudFormation, JSON/YAML

Tarea	Descripción	Habilidades requeridas
Cree un producto con información sobre la versión.	La CloudFormation plantilla se convierte en un producto cuando se publica en AWS Service Catalog. Proporcione valores para los parámetro s de detalle de versión opcionales, como el título de la versión y la descripción. Estos datos le resultarán útiles para realizar consultas sobre el producto más adelante. Para crear un producto, siga las instrucciones de la documentación de AWS Service Catalog. Si utiliza la CLI de AWS, aquí tiene un comando de ejemplo: `aws servicecatalog create-product --cli-input-json file://create-product-input.json` `create-product-input.json` es el archivo que transfiere los parámetros del producto. Para obtener un ejemplo de este archivo, consulte la sección Información adicional. Para obtener más información, consulte la documentación de AWS CLI.	AWS Service Catalog

Tarea	Descripción	Habilidades requeridas
Aplique restricciones.	Aplique restricciones de conjunto de paquetes a la cartera para configurar las opciones de implementación del producto, como múltiples permisos, cuentas y regiones de AWS. Para obtener instrucciones, consulte la documentación de AWS Service Catalog.	AWS Service Catalog
Añada permisos.	Conceda permisos a los usuarios para que lancen los productos de la cartera. Para obtener instrucciones sobre su consola, consulte la documentación de AWS Service Catalog. Si usa la CLI de AWS, aquí tiene un comando de ejemplo: `aws servicecatalog associate-principal-with-portfolio \ --portfolio-id port-2s6abcdefwdh4 \ --principal-arn arn:aws:iam::444455556666:role/Admin \ --principal-type IAM` Para obtener más información, consulte la documentación de AWS CLI.	AWS Service Catalog, IAM

Tarea	Descripción	Habilidades requeridas
Aprovisione el producto.	Un producto aprovisionado es una instancia con recursos de un producto. Al aprovisionar un producto a partir de una CloudFormation plantilla, se lanza una CloudFormation pila y sus recursos subyacentes. Aprovisione el producto definiendo las regiones y cuentas de AWS aplicables en función de las restricciones del conjunto de pilas. En el AWS de CLI, se muestra un ejemplo de comando: `aws servicecatalog provision-product \ --product-id prod-abcdfz3syn2rg \ --provisioning-artifact-id pa-abc347pcsccfm \ --provisioned-product-name "mytestpp name3"` Para obtener más información, consulte la documentación de AWS CLI.	AWS Service Catalog

Recursos relacionados

Referencias

- Información general sobre AWS Service Catalog

- Uso de AWS CloudFormation StackSets

Tutoriales y videos

- AWS re:Invent 2019: Automatícelo todo: opciones y prácticas recomendadas (video)

Información adicional

Al usar el `create-product` comando, el `cli-input-json` parámetro apunta a un archivo que especifica información como el propietario del producto, el correo electrónico de soporte y los detalles de la CloudFormation plantilla. A continuación se muestra un ejemplo de este archivo:

```
{
   "Owner": "Test admin",
      "SupportDescription": "Testing",
         "Name": "SNS",
            "SupportEmail": "example@example.com",
            "ProductType": "CLOUD_FORMATION_TEMPLATE",
               "AcceptLanguage": "en",
                  "ProvisioningArtifactParameters": {
                     "Description": "SNS product",
                        "DisableTemplateValidation": true,
                           "Info": {
                              "LoadTemplateFromURL": "<url>"
                     },
                           "Name": "version 1"
}
```

Supervisión de los clústeres de SAP RHEL Pacemaker mediante los servicios de AWS

Harsh Thoria, Randy Germann y RAVEENDRA Voore, Amazon Web Services

Resumen

Este patrón describe los pasos para monitorear y configurar las alertas de un clúster Pacemaker de Red Hat Enterprise Linux (RHEL) para aplicaciones SAP y servicios de bases de datos SAP HANA mediante Amazon y CloudWatch Amazon Simple Notification Service (Amazon SNS).

La configuración le permite monitorear los recursos del clúster SAP SCS o ASCS, Enqueue Replication Server (ERS) y SAP HANA cuando se encuentran en estado «detenido» con la ayuda de flujos de CloudWatch registro, filtros de métricas y alarmas. Amazon SNS envía un correo electrónico al equipo de infraestructura o de SAP Basis sobre el estado del clúster detenido.

Puede crear los AWS recursos para este patrón mediante AWS CloudFormation scripts o consolas de servicio. AWS Este patrón presupone que está utilizando las consolas; no proporciona CloudFormation scripts ni cubre el despliegue de infraestructura para CloudWatch Amazon SNS. Los comandos de Pacemaker se utilizan para establecer la configuración de alertas del clúster.

Requisitos previos y limitaciones

Requisitos previos

- Una AWS cuenta activa.
- Amazon SNS configurado para enviar notificaciones por correo electrónico o móvil.
- Un clúster SAP ASCS/ERS para ABAP o SCS/ERS Java y SAP HANA Database RHEL Pacemaker. Para obtener instrucciones, consulte lo siguiente:
  - SAP HANA cluster setup
  - Configuración de un clúster de SAP Netweaver ABAP/Java

Limitaciones

- Actualmente, esta solución funciona con los clústeres basados en Pacemaker de la versión 7.3 y posteriores de RHEL. No se ha probado en sistemas operativos SUSE.

Versiones de producto

- RHEL 7.3 y versiones posteriores

Arquitectura

Pila de tecnología de destino

- Agente controlado por eventos de alerta de RHEL Pacemaker
- Amazon Elastic Compute Cloud (Amazon EC2)
- CloudWatch alarma
- CloudWatch grupo de registros y filtro de métricas
- Amazon SNS

Arquitectura de destino

En el siguiente diagrama se muestran los componentes y flujos de trabajo de esta solución.

Automatización y escala

- Puede automatizar la creación de AWS recursos mediante CloudFormation scripts. También puede utilizar filtros de métricas adicionales para escalar y cubrir varios clústeres.

Tools (Herramientas)

Servicios de AWS

- Amazon le CloudWatch ayuda a supervisar las métricas de sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.

Herramientas

- CloudWatch agent (unified) es una herramienta que recopila métricas, registros y rastreos a nivel del sistema de EC2 las instancias y recupera métricas personalizadas de sus aplicaciones.

- El agente de alertas de Pacemaker (para la versión 7.3 y posteriores de RHEL) es una herramienta que inicia una acción cuando se produce un cambio (como cuando un recurso se detiene o se reinicia) en un clúster de Pacemaker.

Prácticas recomendadas

- Para conocer las mejores prácticas sobre el uso de cargas de trabajo de SAP en AWS, consulte SAP Lens for the AWS Well-Architected Framework.
- Tenga en cuenta los costos que implica configurar la CloudWatch supervisión de los clústeres de SAP HANA. Para obtener más información, consulte la Documentación de CloudWatch .
- Considere la posibilidad de utilizar un mecanismo de localización o creación de tickets para las alertas de Amazon SNS.
- Compruebe siempre las versiones de alta disponibilidad (HA) de RHEL del paquete RPM para ordenadores, Pacemaker y el AWS agente perimetral.

Epics

Configurar Amazon SNS

Tarea	Descripción	Habilidades requeridas
Cree un tema de SNS.	1. Inicie sesión en la consola Amazon SNS en la v3/home Consola de administración de AWS y ábrala. https://console.aws.amazon.com/sns/ 2. En el panel de Amazon SNS, en Common actions (Acciones comunes), elija Create Topic (Crear tema). 3. En el cuadro de diálogo Crear tema nuevo, en Tipo, seleccione Estándar.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	4. En Nombre del tema, escriba un nombre para el tema (por ejemplo, `my-topic`). 5. Seleccione Crear tema. Se creará un tema de SNS con una política de recursos que le permitirá publicar notificaciones. 6. Copie el ARN del tema (por ejemplo, `arn:aws:sns:us-east-1:111122223333:my-topic`). Usará este ARN en un paso posterior.	

Tarea	Descripción	Habilidades requeridas
Modifique la política de acceso del tema de SNS.	1. En la consola de Amazon SNS, en el panel de navegación, seleccione Temas y, a continuación, seleccione el tema que creó. 2. Seleccione Editar y vaya a la sección Política de acceso. 3. Asegúrese de que la política de acceso incluya CloudWatch uno de los principales servicios a los que se les permite publicar en este tema. Por ejemplo: `{ "Sid": "Allow AWS CloudWatch to Publish to this SNS topic", "Effect": "Allow", "Principal": { "Service": [ "cloudwatch.amazonaws.com" ] }, "Action": "SNS:Publish", "Resource": "arn:aws:sns:us-east-1:111122223333:my-topic" }`	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	4. Seleccione Save changes (Guardar cambios).	

Tarea	Descripción	Habilidades requeridas
Suscríbase al tema de SNS.	1. En la consola de Amazon SNS, seleccione Suscripciones, Crear suscripción. 2. En ARN del tema, pegue el ARN que creó en la primera tarea. 3. En Protocolo, elige Correo electrónico. 4. En Punto de conexión, introduzca la dirección de correo electrónico de la persona o el equipo responsable del clúster de SAP Pacemaker y que debe recibir las notificaciones. Por ejemplo, puede ser la dirección de correo electrónico de la lista de distribución de SAP Basis o del equipo de infraestructura. 5. Seleccione Crear subscripción. 6. Desde su aplicación de correo electrónico, abra el mensaje de AWS Notificaciones y confirme su suscripción. El navegador web muestra una respuesta de confirmación de Amazon SNS.	Administrador de sistemas de AWS

Confirmación de la configuración del clúster

Tarea	Descripción	Habilidades requeridas
Compruebe el estado del clúster	Utilice el comando pcs status para confirmar que los recursos estén en línea.	Administrador de SAP Basis

Configuración de alertas de Pacemaker

Tarea	Descripción	Habilidades requeridas

Configure el agente de alertas de Pacemaker en la instancia del clúster principal.	Inicia sesión en la EC2 instancia del clúster principal y ejecuta los siguientes comandos:
	`install --mode=0755 /usr/share/pacemaker/alerts/alert_file.sh.sample`
	`touch /var/lib/pacemaker/alert_file.sh`
	`touch /var/log/pcmk_alert_file.log`
	`chown hacluster:haclient /var/log/pcmk_alert_file.log`
	`chmod 600 /var/log/pcmk_alert_file.log`
	`pcs alert create id=alert_file description="Log events to a file." path=/var/lib/pacemaker/alert_file.sh`
	`pcs alert recipient add alert_file id=my-alert_logfile value=/va`
		Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	`r/log/pcmk_alert_f ile.log`	

Configure el agente de alertas de Pacemaker en la instancia del clúster secundario.	Inicia sesión en la EC2 instancia del clúster secundari o del clúster secundario y ejecuta los siguientes comandos:
	`install --mode=0755 / usr/share/pacemak er/alerts/alert_fi le.sh.sample`
	`touch /var/lib/ pacemaker/alert_fi le.sh`
	`touch /var/log/ pcmk_alert_file.log`
	`chown hacluster :haclient /var/log/ pcmk_alert_file.log`
	`chmod 600 /var/log/ pcmk_alert_file.log`
		Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas

Confirme que se creó el recurso de alerta de RHEL.	Utilice el siguiente comando para verificar que se ha creado el recurso de la alerta:
	`pcs alert`
	La salida del comando tendrá este aspecto:
	`[root@xxxxxxx ~]# pcs alert`
	`Alerts:`
	` Alert: alert_file (path=/var/lib/pacemaker/alert_file.sh)`
	`  Description: Log events to a file.`
	`  Recipients:`
	`   Recipient: my-alert_logfile (value=/var/log/pcmk_alert_file.log)`
		Administrador de SAP Basis

Configure el CloudWatch agente

Tarea	Descripción	Habilidades requeridas
Instale el CloudWatch agente.	Hay varias formas de instalar el CloudWatch agente en una EC2 instancia. Para usar la línea de comandos, siga estos pasos: 1. Descarga el paquete del CloudWatch agente:	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas

	`wget https://s3.<region>.amazonaws.com/amazoncloudwatch-agent-region/redhat/amd64/latest/amazon-cloudwatch-agent.rpm`
	dónde `<region>` está ubicada la EC2 instancia (por ejemplo,`us-west-2`). Región de AWS
	2. Opcional) Verifique la firma del paquete. Para obtener instrucciones, consulte Verificar la firma del paquete del CloudWatch agente en la CloudWatch documentación.
	3. Instale el paquete en la primera instancia:
	`sudo rpm -U ./amazon-cloudwatch-agent.rpm`
	4. Repita el proceso para la instancia secundaria.
	
	Para obtener más información, consulte la Documentación de CloudWatch .	

Tarea	Descripción	Habilidades requeridas
Adjunte un rol de IAM a la EC2 instancia.	Para permitir que el CloudWatch agente envíe datos desde las instancias, debes adjuntar la CloudWatchAgentServerRolefunción de IAM a cada instancia. O bien, puede añadir una política para el CloudWatch agente a su función de IAM actual. Para obtener más información, consulte la Documentación de CloudWatch .	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure el CloudWatch agente para que supervise el archivo de registro del agente de alertas de Pacemaker en la instancia del clúster principal.	1. Ejecute este comando para configurar la instancia del clúster principal: `sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard` 2. Elija 1 para Linux y, a continuación, seleccione las opciones según la estrategia de supervisión. 3. Para la pregunta ¿Desea supervisar algún archivo de registro?, seleccione Sí e indique la ruta del archivo de registro de Pacemaker mediante el comando pcs alert. En nuestro caso, es `var/log/pcmk_alert_file.log` . 4. Proporcione el nombre del grupo de registro y del flujo de registro. Si no especifica un flujo de registro, el ID de la AWS instancia se utiliza por defecto. 5. Repita los pasos del 1 al 4 para la instancia del clúster secundario.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Inicie el CloudWatch agente en las instancias del clúster principal y secundario.	Para iniciar el agente, ejecute el siguiente comando en las EC2 instancias de los clústeres principal y secundario: `sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json`	Administrador de AWS

Configure CloudWatch los recursos

Tarea	Descripción	Habilidades requeridas
Configure grupos de CloudWatch registros.	1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/ 2. En el panel de navegación, elija Grupos de registro, Crear grupo de registro. 3. Escriba el nombre del grupo de registro y, a continuación, seleccione Crear grupo de registro. El CloudWatch agente transferirá el archivo de	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	alertas de Pacemaker al grupo de CloudWatch registros como una secuencia de registros.	

Tarea	Descripción	Habilidades requeridas
Configure filtros CloudWatch métricos.	Los filtros métricos le ayudan a buscar un patrón, como `stop <cluster-resource-name>` en los flujos de CloudWatch registro. Cuando se identific a este patrón, el filtro de métricas actualiza una métrica personalizada. 1. En la CloudWatch consola, en el panel de navegació n, selecciona Grupos de registros. 2. Seleccione el nombre del grupo de registro que ha creado en la tarea anterior. 3. Elija Actions (Acciones), Create metric filter (Crear filtro de métricas). 4. En Patrón de filtro, introduzca el patrón de filtro que desee utilizar (como `stop ABC_scs`) para establecer una coincidencia con el evento de detención de un recurso de clúster de SAP SCS denominado `ABC_scs`. Para obtener más informaci ón, consulte la sintaxis del patrón de filtro en la	Administrador de AWS, administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	CloudWatch documentación. 5. (Opcional) Para probar el patrón de filtro, en Test Pattern (Patrón de prueba), ingrese uno o más eventos de registro a utilizar para probar el patrón. Cada evento de registro debe especificarse en una línea independiente, ya que los saltos de línea se utilizan para separar los eventos de registro en el cuadro Mensajes de eventos de registro. 6. Elija Next (Siguiente) y luego ingrese un nombre para el filtro. 7. En Detalles de la métrica, en Espacio de nombres métrico, introduzca un nombre para el espacio de CloudWatch nombres en el que se publicará la métrica (por ejemplo,). `sapcluster_monitoring` Si este espacio de nombres no existe todavía, seleccione Crear nuevo. 8. En Nombre de métrica, introduzca un nombre para la nueva métrica (por ejemplo, `sapcluste`	

Tarea	Descripción	Habilidades requeridas
	r_<sid> , donde <sid> es el nombre de identific ación del sistema de SAP). 9. En Valor de métrica, introduzca 1. También puede ingresar un token como $size. Esto incrementa la métrica por el valor del número en el campo size por cada evento de registro que contenga un campo size. 10. En Valor predeterminado, introduzca 0. 11. Elija Create metric filter (Crear filtro de métricas). Cuando el filtro de métricas identifica el patrón en el paso 4, actualiza el valor de la métrica CloudWatch personali zada a 1. **sapcluster_abc** La CloudWatch alarma SAP-Cluster-QA1-AB C monitorea la métrica sapcluster_abc y envía una notificación de SNS cuando el valor de la métrica cambia a 1. Esto indica que el recurso del clúster se ha detenido y que se deben tomar medidas.	

Tarea	Descripción	Habilidades requeridas
Configure una alarma CloudWatch métrica para la métrica de SAP ASCS/SCS y ERS.	Para crear una alarma a partir de una sola métrica, siga estos pasos: 1. En la CloudWatch consola, en el panel de navegación, seleccione Alarmas, Todas las alarmas. 2. Elija Crear alarma. 3. Elija Seleccionar métrica. 4. Busque la métrica personalizada `sapcluster_monitoring` que creó en la tarea anterior. 5. Seleccione el nombre de la métrica para SAP SCS (por ejemplo, `sapcluster_<abc>`), que también se creó en la tarea anterior. 6. En la pestaña Métricas diagramadas, defina lo siguiente: • En Statistic (Estadística), elija Maximum (Máximo). • Para Periodo, seleccione 1 minuto. • En Tipo de umbral, seleccione Estático y establezca el umbral de `sapcluster_<sid>` en un valor mayor o igual a 1. 7. Elija Siguiente.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	8. En Notificación, seleccione el tema de SNS que creó en el primer resumen. 9. En Nombre y Descripción, proporcione el nombre de la alarma y una breve descripción y, a continuación, seleccione Siguiente. 10. Elija Crear alarma.	
Configure una alarma CloudWatch métrica para la métrica de SAP HANA.	Repita los pasos para configurar una alarma CloudWatch métrica de la tarea anterior, con estos cambios: • En el paso 5, elija el nombre de la métrica para SAP HANA (por ejemplo, `sapcluster_db_<abc>`). • Para el paso 6, establezca el umbral de `sapcluster_<sid>` en un valor superior a 0.	Administrador de AWS

Recursos relacionados

- Triggering Scripts for Cluster Events (documentación de RHEL)
- Cree el archivo de configuración del CloudWatch agente con el asistente (CloudWatch documentación)
- Instalación y ejecución del CloudWatch agente en sus servidores (CloudWatch documentación)
- Cree una CloudWatch alarma basada en un umbral estático (CloudWatch documentación)

- Implementación manual de SAP HANA en AWS con clústeres de alta disponibilidad (documentación de SAP en el AWS sitio web)
- NetWeaver Guías de SAP (documentación de SAP en el AWS sitio web)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Supervise la actividad de las aplicaciones mediante CloudWatch Logs Insights

Ram Kandaswamy, Amazon Web Services

Resumen

Este patrón proporciona una solución para detectar y alertar automáticamente sobre las excepciones de las aplicaciones mediante Amazon CloudWatch Logs Insights. Al implementar alertas y análisis de registros automatizados, puede identificar los problemas de las aplicaciones en su entorno de producción y responder a ellos rápidamente.

Los registros desempeñan un papel crucial a la hora de supervisar el comportamiento del sistema, identificar los problemas y garantizar un rendimiento óptimo. Durante un proceso de migración, los archivos de registro tienen un valor incalculable para validar el funcionamiento del sistema en el nuevo entorno, detectar problemas de compatibilidad e identificar cualquier comportamiento inesperado. Los problemas pueden estar relacionados con las operaciones o la seguridad. En el caso de los problemas relacionados con la seguridad, permitir la detección temprana de intentos de acceso no autorizado o actividades sospechosas es esencial para mantener la seguridad y el cumplimiento de las normas. Esta capacidad es de especial importancia cuando se trata de información confidencial o de sistemas críticos.

Este patrón es especialmente valioso para los equipos que necesitan hacer lo siguiente:

- Mantenga una alta disponibilidad de las aplicaciones.
- Responda rápidamente a los problemas de producción.
- Analice los errores específicos de la aplicación que los registros no capturan Servicio de AWS .
- Realice análisis de registros a pedido sin una infraestructura prediseñada.

CloudWatch Logs Insights es ideal para analizar los registros generados por la aplicación cuando el contexto del error solo existe en el código de la aplicación. CloudWatch Logs Insights destaca en las siguientes tareas:

- Consulte datos de registro semiestructurados o no estructurados.
- Realice análisis bajo demanda durante la respuesta a los incidentes.
- Correlaciona los eventos entre varios grupos de registros.
- Cree visualizaciones rápidas sin herramientas externas.

Requisitos previos y limitaciones

Requisitos previos

- Una aplicación de producción implementada en modo activo Cuenta de AWS
- Descripción básica del formato de registro y los patrones de excepción de la aplicación de producción
- Registros de aplicaciones configurados para transmitirse a Amazon CloudWatch Logs

Limitaciones

- Algunos Servicios de AWS no están disponibles en todos Regiones de AWS. Para obtener información sobre la disponibilidad en regiones, consulte AWS Services by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

En el siguiente diagrama, se muestra cómo CloudWatch Logs Insights evalúa los registros de recursos y envía una visualización de datos relevante a un CloudWatch panel de control.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Los recursos publican registros en CloudWatch Logs. Los recursos pueden incluir AWS recursos como instancias de Amazon Elastic Compute Cloud (Amazon EC2) o depósitos de Amazon Simple Storage Service (Amazon S3). Otro ejemplo incluye sistemas locales con un CloudWatch agente instalado en los que se pueden publicar registros. CloudWatch
2. CloudWatch Logs Insights filtra la cadena de patrones correspondiente. Algunos ejemplos de cadenas de patrones de búsqueda son “error”, “exception” o una expresión regular específica.
3. Normalmente, el equipo de soporte de producción o los desarrolladores añaden la visualización de patrones al CloudWatch panel de control.

Automatización y escala

Los desarrolladores pueden automatizar la solución de este patrón mediante el uso de AWS Cloud Development Kit (AWS CDK) AWS CloudFormation,, o AWS SDKs gestionar varios patrones de

cadenas. Los equipos pueden incorporar esta automatización en sus procesos de integración e implementación continuas (CI/CD). DevOps

Tools (Herramientas)

Servicios de AWS

- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas y aplicaciones Servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.

Prácticas recomendadas

Eficiencia de consultas

- Defina y configure grupos de registro para analizar los datos de registro relevantes.
- Use los exploradores de campo para comprender la estructura y los campos disponibles en los datos de registro.
- Escriba consultas eficientes mediante la sintaxis de consultas de CloudWatch Logs Insights.
- Adapte las consultas de muestra a sus requisitos específicos para poder hacer un análisis más rápido.
- Limite los intervalos de tiempo de consulta para reducir los datos escaneados y mejorar el rendimiento.
- Guarde las consultas para usarlas en el futuro a fin de ahorrar tiempo y garantizar un análisis coherente.

Seguridad

- Aplique las políticas de IAM adecuadas a CloudWatch Logs Insights y a los grupos de registros. Cumpla con el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.

- Habilite el cifrado de datos de registro mediante AWS KMS para los datos de registro confidenciales.

Optimización de costos

- CloudWatch Logs Insights cobra por GB de datos escaneados por consulta. Reduzca los intervalos de tiempo y diríjase a grupos de registros específicos para reducir los costos.
- Configure las políticas de retención de registros adecuadas para administrar los costos de almacenamiento.
- Para realizar análisis frecuentes de grandes conjuntos de datos históricos, considere la posibilidad de exportar los registros a Amazon S3 y utilizar Amazon Athena.
- Revise CloudWatch los precios para comprender las implicaciones de costo para su caso de uso.

Epics

Cree un grupo de registro y configure los registros para verlos en el panel de control.

Tarea	Descripción	Habilidades requeridas
Configurar los permisos de IAM.	Para configurar los permisos de IAM, siga estos pasos: 1. Identifique los roles de IAM que usan la aplicación para escribir registros y los usuarios o servicios que crearán paneles, consultas y alarmas. 2. Para el rol de la aplicación, agregue las siguientes acciones y recursos de la API a una política: `{ "Version": "2012-10-17",`	Administrador de AWS DevOps, administrador de sistemas de AWS, administrador de nube, arquitecto de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	<pre>"Statement": [{ "Effect": "Allow", "Action": ["logs:CreateLogGroup", "logs:CreateLogStream", "logs:PutLogEvents"], "Resource": ["arn:aws:logs:*:*:*"] }] }</pre> 3. Para administrar CloudWatch los recursos, añada lo siguiente a una política: <pre>{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": [</pre>	

Tarea	Descripción	Habilidades requeridas

	<pre>"cloudwatch:PutDashboard",
	"cloudwatch:GetDashboard",
	"logs:StartQuery",
	"logs:StopQuery",
	"logs:GetQueryResults",
	"cloudwatch:PutMetricAlarm"
	],
	"Resource": "*"
	}
	]
	}</pre>
	Para obtener información sobre cómo crear políticas de IAM o agregar permisos a las políticas existentes, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente y Edición de políticas de IAM en la Guía del usuario de IAM. Para obtener más información, consulte la referencia sobre gestión de identidad y acceso para Amazon CloudWatch Logs y permisos de CloudWatch Logs en la	

Tarea	Descripción	Habilidades requeridas
	Guía del usuario de Amazon CloudWatch Logs.	

Tarea	Descripción	Habilidades requeridas

Cree un grupo de registros.	Para crear un grupo de registro, utilice una de las siguientes opciones:
	• Cree o abra un archivo CloudFormation de plantilla (formato YAML o JSON) con una `.json` extensión `.yaml` o. (El siguiente código usa el formato YAML). Agregue la siguiente definición de recurso a la sección Recursos de la plantilla:
	`MyLogGroup:`
	`  Type: AWS::Logs`
	`::LogGroup`
	`  Properties:`
	`  LogGroupName: my-`
	`log-group`
	Para obtener más informaci ón, consulta Quick Start: Use AWS CloudFormation to get start with CloudWatch Logs en la Guía del usuario de Amazon CloudWatch Logs.
	• Utilice la CloudWatch consola, tal y como se describe en Crear un grupo de CloudWatch registros en Logs de la Guía del usuario
		Administrador de AWS DevOps, administrador de sistemas de AWS, administr ador de nube, arquitecto de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	de Amazon CloudWatch Logs. • Utilice la CreateLog Groupoperación en la API de CloudWatch Logs.	

Tarea	Descripción	Habilidades requeridas
Genere una consulta CloudWatch de Logs Insights.	Para crear y guardar una consulta de CloudWatch Logs Insights, haga lo siguiente: 1. Abra la CloudWatch consola. 2. Vaya a Información de registros. 3. Utilice uno de los siguientes métodos para crear la consulta: • Comience con una consulta de ejemplo de la sección Consultas. • Escriba una consulta personalizada. • Modifque la siguiente consulta de ejemplo: `fields @timestamp, @message | filter @message like /(?i)exception/|stats count() by bin(30s)` Esta consulta comprueba el archivo de registro, extrae la marca de tiempo y el contenido del mensaje, filtra la palabra “exception” (no distingue mayúsculas de minúsculas) y cuenta las	Administrador de AWS DevOps, administrador de sistemas de AWS, administrador de nube, arquitecto de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	apariciones en intervalos de 30 segundos.	

Tarea	Descripción	Habilidades requeridas
Cree una visualización en un CloudWatch panel de control.	Para usar un CloudWatch panel para crear una visualización, haga lo siguiente: 1. Abra la CloudWatch consola y cree un CloudWatch panel (si aún no tiene uno) o abra un panel existente. 2. Agregue la visualización de supervisión de excepciones. Hay disponibles gráficos de barras, líneas y circulares, en función de las necesidades de su empresa. Para obtener más información, consulte Uso de widgets en los CloudWatch paneles de control en la Guía del usuario de Amazon CloudWatch Logs. Para tener visualizaciones de datos en tiempo real, puede personalizar un widget que se adapte a sus necesidades. Para obtener más información sobre las opciones y capacidades de los paneles, consulte Uso de CloudWatch paneles de Amazon y Creación de CloudWatc	Administrador de AWS DevOps, administrador de sistemas de AWS, administrador de nube, arquitecto de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	h paneles flexibles con variables de panel en la Guía del usuario de Amazon CloudWatch Logs.	

Resolución de problemas

Problema	Solución
No se pueden ver los resultados de la consulta o parece que la consulta no funciona	Comience con una consulta funcional que haya modificado a partir de una consulta de ejemplo. Realice pequeños cambios increment ales en partes de la consulta (como un filtro o un campo) y aproveche la función de generació n de consultas de CloudWatch registros.
Los grupos de registro no crean flujos de registro	En la política de IAM, asegúrese de que el recurso para las operaciones CreateLog Streamy las CreateLogGroupoperaciones tenga un valor de carácter (`*`) comodín. La operación `create` no se realizará correctam ente sin este permiso de comodín.
Tiempo de espera de la consulta o rendimiento lento	Reduzca el intervalo de tiempo, diríjase a grupos de registros específicos o simplifique la consulta. Los patrones complejos de expresion es regulares (`regex`) y los intervalos de tiempo amplios aumentan el tiempo de consulta.
No se devuelven datos para un intervalo de tiempo válido	Compruebe la selección del grupo de registros y compruebe que los registros se están ingiriendo (revise los flujos de registros) y confirme que el patrón de filtrado coincide con el formato de registro.

Recursos relacionados

- Análisis de los datos de registro con CloudWatch Logs Insights
- Amazon CloudWatch FAQs
- Creación de CloudWatch paneles flexibles con variables de panel
- Get started with Logs Insights QL: Query tutorials
- Utilice un lenguaje natural para generar y actualizar las consultas de CloudWatch Logs Insights
- Úselo PutDashboard con un AWS SDK o CLI
- Trabajar con grupos de registros y flujos de registros

Supervise el uso de una imagen de máquina de Amazon compartida en múltiples Cuentas de AWS

Naveen Suthar y Sandeep Gawande, Amazon Web Services

Resumen

Las imágenes de Amazon Machine (AMIs) se utilizan para crear instancias de Amazon Elastic Compute Cloud (Amazon EC2) en su entorno de Amazon Web Services (AWS). Puede crear una cuenta AMIs de AWS independiente y centralizada, que en este patrón se denomina cuenta de creador. A continuación, puede compartir la AMI entre varias Cuentas de AWS que estén en la misma unidad Región de AWS, que en este patrón se denominan cuentas de consumidores. La administración AMIs desde una sola cuenta proporciona escalabilidad y simplifica la gobernanza. En las cuentas de los consumidores, puede hacer referencia a la AMI compartida en las plantillas de lanzamiento de Amazon EC2 Auto Scaling y en los grupos de nodos de Amazon Elastic Kubernetes Service (Amazon EKS).

Cuando una AMI compartida queda obsoleta, se anula su registro o se deja de compartir, los servicios de Servicios de AWS que hacen referencia a la AMI en las cuentas de consumidor no pueden usar esta AMI para inicializar nuevas instancias. Se produce un error en cualquier evento de escalado automático o en el relanzamiento de la misma instancia. Esto puede provocar problemas en el entorno de producción, como el tiempo de inactividad de las aplicaciones o la degradación del rendimiento. Cuando los eventos de uso y uso de la AMI se producen de forma múltiple Cuentas de AWS, puede resultar difícil supervisar esta actividad.

Este patrón ayuda a supervisar el uso y el estado de la AMI compartida en cuentas de la misma región. Utiliza servicios sin servidor Servicios de AWS, como Amazon EventBridge, Amazon AWS Lambda DynamoDB y Amazon Simple Email Service (Amazon SES). La infraestructura se aprovisiona como código (IaC) mediante Terraform. HashiCorp Esta solución proporciona alertas cuando un servicio de una cuenta de consumidor hace referencia a una AMI que ya no está registrada o compartida.

Requisitos previos y limitaciones

Requisitos previos

- Dos o más cuentas activas Cuentas de AWS: una cuenta de creador y una o más cuentas de consumidor
- Una o más AMIs que se comparten desde la cuenta de creador a una cuenta de consumidor

- Terraform CLI, instalada (documentación de Terraform)
- Terraform AWS Provider, configurado (documentación de Terraform)
- (Opcional, pero recomendado) Backend de Terraform, configurado (documentación de Terraform)
- Git, instalado

Limitaciones

- Este patrón monitorea AMIs lo que se ha compartido con cuentas específicas mediante el ID de la cuenta. Este patrón no supervisa los datos AMIs que se han compartido con una organización mediante el ID de la organización.
- AMIs solo se puede compartir con cuentas que estén dentro de la misma Región de AWS. Este patrón se monitorea AMIs dentro de una única región objetivo. Para supervisar el uso AMIs en varias regiones, debe implementar esta solución en cada región.
- Este patrón no monitorea ninguna de las AMIs que se compartieron antes de implementar esta solución. Si desea supervisar las cuentas compartidas anteriormente AMIs, puede dejar de compartir la AMI y, a continuación, volver a compartirla con las cuentas de los consumidores.

Versiones de producto

- Versión de Terraform 1.2.0 o posterior
- Terraform AWS Provider, versión 4.20 o posterior

Arquitectura

Pila de tecnología de destino

Los recursos siguientes se aprovisionan como IaC a través de Terraform:

- Tablas de Amazon DynamoDB
- EventBridge Reglas de Amazon
- AWS Identity and Access Management Función (IAM)
- AWS Lambda funciones
- Amazon SES

Arquitectura de destino

En el diagrama, se muestra el siguiente flujo de trabajo:

1. La AMI de la cuenta de creador se comparte con una cuenta de consumidor de la misma Región de AWS.
2. Cuando se comparte la AMI, una EventBridge regla de la cuenta del creador captura el `ModifyImageAttribute` evento e inicia una función Lambda en la cuenta del creador.
3. La función de Lambda almacena los datos relacionados con la AMI en una tabla de DynamoDB de la cuenta de creador.
4. Cuando una Servicio de AWS cuenta de consumidor utiliza la AMI compartida para lanzar una EC2 instancia de Amazon o cuando la AMI compartida está asociada a una plantilla de lanzamiento, una EventBridge regla de la cuenta de consumidor captura el uso de la AMI compartida.
5. La EventBridge regla inicia una función Lambda en la cuenta del consumidor. La función de Lambda lleva a cabo lo siguiente:
   a. La función de Lambda actualiza los datos relacionados con la AMI en una tabla de DynamoDB de la cuenta de consumidor.
   b. La función de Lambda asume un rol de IAM en la cuenta de creador y actualiza la tabla de Lambda de la cuenta de creador. En la tabla `Mapping`, crea un elemento que asigna el ID de instancia o el ID de plantilla de lanzamiento a su ID de AMI correspondiente.
6. La AMI que se administra de forma centralizada en la cuenta de creador está obsoleta, se ha anulado su registro o ha dejado de compartirse.
7. La EventBridge regla de la cuenta del creador captura el `DeregisterImage` evento `ModifyImageAttribute` o con la `remove` acción e inicia la función Lambda.
8. La función de Lambda comprueba la tabla de DynamoDB para determinar si la AMI se utiliza en alguna de las cuentas de consumidor. Si no hay ninguna instancia IDs o plantilla de lanzamiento IDs asociada a la AMI en la `Mapping` tabla, el proceso se ha completado.
9. Si IDs hay alguna instancia IDs o plantilla de lanzamiento asociada a la AMI de la `Mapping` tabla, la función Lambda utiliza Amazon SES para enviar una notificación por correo electrónico a los suscriptores configurados.

Tools (Herramientas)

Servicios de AWS

- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, AWS Lambda funciones, puntos finales de invocación HTTP que utilizan destinos de API o buses de eventos en otros. Cuentas de AWS
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus recursos de AWS al controlar quién está autenticado y autorizado a usarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Email Service (Amazon SES) facilita poder enviar y recibir correos electrónicos a través de los dominios y direcciones de correo electrónico propios.

Otras herramientas

- HashiCorp Terraform es una herramienta de infraestructura como código (IaC) que facilita usar el código para aprovisionar y administrar los recursos y la infraestructura en la nube.
- Python es un lenguaje de programación informático de uso general.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub cross-account-ami-monitoring-terraform-samples.

Prácticas recomendadas

- Siga las prácticas recomendadas para trabajar con funciones. AWS Lambda
- Siga las mejores prácticas para crear AMIs.
- Al crear el rol de IAM, siga el principio del privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo cada tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.
- Configure el monitoreo y las alertas para las AWS Lambda funciones. Para obtener más información, consulte Supervisión y solución de problemas de funciones de Lambda.

Epics

Personalizar los archivos de configuración de Terraform

Tarea	Descripción	Habilidades requeridas
Cree los perfiles AWS CLI nombrados.	Para la cuenta del creador y para cada cuenta de consumidor, cree un perfil con nombre AWS Command Line Interface (AWS CLI). Para obtener instrucciones, consulte Configurar el AWS CLI en el AWS Centro de recursos de introducción.	DevOps ingeniero
Clonar el repositorio.	Escriba el siguiente comando. Esto clona el repositorio cross-account-ami-monitoring-terraform-samples mediante SSH. GitHub `git clone git@github.com:aws-samples/cross-account-ami-monitoring-terraform-samples.git`	DevOps ingeniero
Actualice el archivo provider.tf.	1. Ingrese el comando siguiente para acceder a la carpeta `terraform` del repositorio clonado. `cd cross-account-ami-monitoring/terraform` 2. Abra el archivo `provider.tf` .	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	3. Actualice las configuraciones de Terraform AWS Provider para la cuenta de creador y la cuenta de consumidor de la siguiente manera: • En `alias`, especifique un nombre para la configuración del proveedor. • Para ello`region`, introduzca el destino Región de AWS en el que desea implementar esta solución. • Para`profile`, introduzca el AWS CLI perfil indicado para acceder a la cuenta. 4. Si va a configurar más de una cuenta de consumidor, cree un perfil para cada cuenta de consumidor adicional. 5. Guarde y cierre el archivo `provider.tf` . Para más información sobre la configuración de proveedores, consulte Configuraciones de varios proveedores en la documentación de Terraform.	

Tarea	Descripción	Habilidades requeridas
Actualice el archivo terraform .tfvars.	1. Abra el archivo `terraform.tfvars` . 2. En el parámetro `account_email_mapping` , configure las alertas para la cuenta de creador y la cuenta de consumidor de la manera siguiente: • En `account`, especifique el ID de la cuenta. • En `email`, especifique la dirección de email a la que desea enviar alertas. Solo puede especificar una dirección de correo electrónico para cada cuenta. 3. Si va a configurar más de una cuenta de consumidor, especifique una cuenta y una dirección de correo electrónico para cada cuenta de consumidor adicional. 4. Guarde y cierre el archivo `terraform.tfvars` .	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Actualice el archivo main.tf.	Siga estos pasos solo si va a implementar esta solución en más de una cuenta de consumidor. Si va a implementar esta solución en una sola cuenta de consumidor, no es necesario modificar este archivo. 1. Abra el archivo `main.tf`. 2. Para cada cuenta de consumidor adicional, cree un módulo nuevo que se base en el módulo `consumer_account_A` de la plantilla. Para cada cuenta de consumidor, el valor de `provider` debe coincidir con el alias que especificó en el archivo `provider.tf` . 3. Guarde y cierre el archivo `main.tf`.	DevOps ingeniero

Implementar la solución mediante Terraform

Tarea	Descripción	Habilidades requeridas
Implemente la solución.	En la CLI de Terraform, introduzca los siguientes comandos para implementar los AWS recursos en las cuentas del creador y del consumidor:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	1. Ingrese el comando siguiente para inicializar Terraform.
	`terraform init`
	2. Ingrese el comando siguiente para validar las configuraciones de Terraform.
	`terraform validate`
	3. Ingrese el comando siguiente para crear un plan de ejecución de Terraform.
	`terraform plan`
	4. Revise los cambios de configuración en el plan de Terraform y confirme que desea implementarlos.
	5. Ingrese el comando siguiente para implementar los recursos.
	`terraform apply`	

Tarea	Descripción	Habilidades requeridas
Verificar la identidad de la dirección de correo electrónico.	Al implementar el plan Terraform, Terraform crea una identidad de dirección de correo electrónico para cada cuenta de consumidor en Amazon SES. Para poder enviar notificaciones a esa dirección de correo electrónico, es necesario verificarla. Para las instrucciones, consulte Verificación de la identidad de una dirección de correo electrónico en la documentación de Amazon SES.	AWS general

Validar la implementación de recursos

Tarea	Descripción	Habilidades requeridas
Valide la implementación en la cuenta de creador.	1. Inicie sesión en la cuenta de creador. 2. En la barra de navegación, confirme que ve la Región de AWS de destino. Si se encuentra en una región diferente, seleccione el nombre de región que se muestra y la región de destino. 3. Abra la consola de DynamoDB.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	4. En el panel de navegación, elija Tablas. 5. En la lista de tablas, compruebe que la tabla `AmiShare` esté presente. 6. Abra la consola de Lambda. 7. Seleccione Funciones en el panel de navegación. 8. En la lista de funciones, compruebe que la función `ami-share` esté presente. 9. Abra la consola de IAM. 10. Seleccione Roles en el panel de navegación. 11. En la lista de roles, compruebe que el rol `external-ddb-role` esté presente. 12. Abra la consola de EventBridge. 13. En el panel de navegación, seleccione Reglas. 14. En la lista de reglas, compruebe que la regla `modify_image_attribute_event` esté presente. 15. Abra la consola de Amazon SES.	

Tarea	Descripción	Habilidades requeridas
	16 En el panel de navegación, seleccione Verified identities (Identidades verificadas). 17 En la lista de identidades, compruebe que se haya registrado y verificado la identidad de una dirección de correo electrónico para cada cuenta de consumidor.	

Tarea	Descripción	Habilidades requeridas
Valide la implementación en la cuenta de consumidor.	1. Inicie sesión en la cuenta de consumidor. 2. En la barra de navegación, confirme que ve la Región de AWS de destino. Si se encuentra en una región diferente, seleccione el nombre de región que se muestra y la región de destino. 3. Abra la consola de DynamoDB. 4. En el panel de navegación, elija Tablas. 5. En la lista de tablas, compruebe que la tabla `Mapping` esté presente. 6. Abra la consola de Lambda. 7. Seleccione Funciones en el panel de navegación. 8. En la lista de funciones , compruebe que las funciones `ami-usage-function` y `ami-deregister-function` estén presentes. 9. Abra la consola de EventBridge . 10. En el panel de navegación, seleccione Reglas. 11. En la lista de reglas, compruebe que las reglas	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`ami_usage_events` y `ami_deregister_events` estén presentes.	

Validar la supervisión

Tarea	Descripción	Habilidades requeridas
Cree una AMI en la cuenta de creador.	1. Cree una AMI privada en la cuenta de creador. Para obtener instrucciones, consulte Crear una AMI a partir de una EC2 instancia de Amazon. 2. Comparta la nueva AMI con una de las cuentas de consumidor. Para obtener instrucciones, consulte Compartir una AMI con específicos Cuentas de AWS.	DevOps ingeniero
Use la AMI en la cuenta de consumidor.	En la cuenta del consumidor, usa la AMI compartida para crear una EC2 instancia de Amazon o una plantilla de lanzamiento. Para obtener instrucciones, consulte Cómo lanzar una EC2 instancia de Amazon desde una AMI personalizada (AWS re:Post Knowledge Center) o Crear una plantilla de lanzamiento para un grupo de Auto Scaling	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	(documentación de Amazon EC2 Auto Scaling).	
Valide la supervisión y las alertas.	1. Inicie sesión en la cuenta de creador. 2. Abre la EC2 consola de Amazon. 3. En el panel de navegación, elija AMIs. 4. Seleccione la AMI en la lista y, a continuación, Actions (Acciones), Edit AMI permissions (Editar permisos de la AMI). 5. En la sección Shared accounts (Cuentas compartidas), seleccione la cuenta de consumidor y, a continuación, Remove selected (Eliminar lo seleccionado). 6. Seleccione Save changes (Guardar cambios). 7. Valide que la dirección de correo electrónico de destino que definió para la cuenta de consumidor reciba una notificación de cancelación del uso compartido de la AMI.	DevOps ingeniero

(Opcional) Deje de monitorear de forma compartida AMIs

Tarea	Descripción	Habilidades requeridas
Elimine los recursos.	1. Introduzca el siguiente comando para eliminar los recursos desplegados por este patrón y dejar de monitorizar los recursos compartidos AMIs. `terraform destroy` 2. Confirme el comando `destroy`; para hacerlo, especifique `yes`.	DevOps ingeniero

Resolución de problemas

Problema	Solución
No he recibido ninguna alerta por correo electrónico.	Puede haber varios motivos por los que no se envió el correo electrónico de Amazon SES. Comprueba lo siguiente: 1. En la sección Epics, utilice la sección Validar el despliegue de recursos para confirmar que la infraestructura se aprovisionó correctamente en todos los casos. Cuentas de AWS 2. Valide los eventos de la función Lambda en Amazon CloudWatch Logs. Para obtener instrucciones, consulte Uso de la CloudWatch consola en la documentación de Lambda. Confirme que los permisos no tengan ningún problema, como una denegación explícita en una política basada en la identidad o en

Problema	Solución
	los recursos. Para obtener más información, consulte Lógica de evaluación de políticas en la documentación de IAM. 3. En Amazon SES, compruebe que el estado de la identidad de la dirección de correo electrónico sea Verified (Verificado). Para obtener más información, consulte Verificación de identidades de correo electrónico.

Recursos relacionados

AWS documentación

- Creación de funciones de Lambda con Python (documentación de Lambda)
- Creación de una AMI (EC2 documentación de Amazon)
- Compartir una AMI con información específica Cuentas de AWS (EC2 documentación de Amazon)
- Anular el registro de la AMI (documentación de Amazon EC2)

Documentación de Terraform

- Instalar Terraform
- Configuración del backend de Terraform
- Proveedor de AWS para Terraform
- Descarga binaria de Terraform

Vea los detalles de la instantánea de EBS de su cuenta u organización de AWS

Arun Chandapillai y Parag Nagwekar, Amazon Web Services

Resumen

Este patrón describe cómo puede generar automáticamente un informe bajo demanda de todas las instantáneas de Amazon Elastic Block Store (Amazon EBS) de su cuenta de Amazon Web Services (AWS) o unidad organizativa (OU) en AWS Organizations.

Amazon EBS es un easy-to-use servicio de almacenamiento en bloques escalable y de alto rendimiento diseñado para Amazon Elastic Compute Cloud (Amazon EC2). Un volumen de EBS proporciona un almacenamiento duradero y persistente que puede adjuntar a sus EC2 instancias. Puede utilizar los volúmenes de EBS como almacenamiento principal para sus datos y realizar una point-in-time copia de seguridad de los volúmenes de EBS mediante la creación de una instantánea. Puede utilizar la Consola de administración de AWS o la Interfaz de la línea de comandos de AWS (AWS CLI) para ver los detalles de instantáneas de EBS específicas. Este patrón proporciona una forma programática de recuperar información sobre todas las instantáneas de EBS de su cuenta o unidad organizativa de AWS.

Puede usar el script que proporciona este patrón para generar un archivo de valores separados por comas (CSV) que contenga la siguiente información sobre cada instantánea: Identificador de cuenta, Identificador de instantánea, Identificador de volumen y tamaño, fecha en que se tomó la instantánea, Identificador de instancia y descripción. Si las instantáneas de EBS están etiquetadas, el informe también incluye los atributos del propietario y del equipo.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Instalación y configuración de la versión 2 de AWS CLI
- Rol de AWS Identity and Access Management (IAM) con los permisos adecuados (permisos de acceso para una cuenta específica o para todas las cuentas de una OU si planea ejecutar el script desde AWS Organizations)

Arquitectura

El siguiente diagrama muestra el flujo de trabajo del script que genera un informe bajo demanda de las instantáneas de EBS distribuidas en varias cuentas de AWS de una OU.

Tools (Herramientas)

Servicios de AWS

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento a nivel de bloques para su uso con instancias. EC2
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Organizations es un servicio de administración de cuentas que le permite agrupar varias cuentas de AWS en una organización que usted crea y administra de manera centralizada.

Código

El código de la aplicación de muestra utilizada en este patrón está disponible en el GitHub repositorio. aws-ebs-snapshots-awsorganizations Siga las instrucciones de la siguiente sección para utilizar los archivos de muestra.

Epics

Descargue el script

Tarea	Descripción	Habilidades requeridas
Descargar el script Python.	Descargue el script GetSnapshotDetailsAllAccountsOU.py del GitHub repositorio.	AWS general

Obtenga los detalles de las instantáneas de EBS para una cuenta de AWS

Tarea	Descripción	Habilidades requeridas

Ejecutar el script de Python .	Ejecute el comando:
	`python3 getsnapsh otinfo.py --file <output-file>.csv --region <region-name>`
	donde `<output-file>` se refiere al archivo de salida CSV en el que desea que se coloque la información sobre las instantáneas de EBS y `<region-name>` es la región de AWS en la que se almacenan las instantáneas. Por ejemplo:
	`python3 getsnapsh otinfo.py --file snapshots.csv --region us-east-1`
		AWS general

Obtenga los detalles de las instantáneas de EBS de una organización

Tarea	Descripción	Habilidades requeridas
Ejecutar el script de Python .	Ejecute el comando: `python3 getsnapsh otinfo.py --file <output-file>.csv --role <IAM-role> --region <region-name>`	AWS general

Tarea	Descripción	Habilidades requeridas
	donde `<output-file>` se refiere al archivo de salida CSV en el que desea que se coloque la información sobre las instantáneas de EBS, `<IAM-role>` es una función que proporciona permisos para acceder a AWS Organizations y `<region-name>` es la región de AWS en la que se almacenan las instantáneas. Por ejemplo: `python3 getsnapshotinfo.py --file snapshots.csv --role <IAM role> --region us-west-2`	

Recursos relacionados

- Documentación de Amazon EBS
- Acciones de Amazon EBS
- Referencia de la API de Amazon EBS
- Mejorar el rendimiento de Amazon EBS
- Recursos de Amazon EBS
- Precios de las instantáneas de EBS

Información adicional

Tipos de instantáneas de EBS

Amazon EBS ofrece tres tipos de instantáneas, según la propiedad y el acceso:

- De su propiedad: de manera predeterminada, solo usted puede crear volúmenes de instantáneas que sean de su propiedad.
- Instantáneas públicas: puede compartir las instantáneas públicamente con todas las demás cuentas de AWS. Para crear una instantánea pública, modifique los permisos de la instantánea para compartirla con las cuentas de AWS que especifique. Los usuarios que autorice podrán usar las instantáneas que comparta para crear sus propios volúmenes de EBS, mientras que la instantánea original se mantendrá sin cambios. Puede también poner las instantáneas no cifradas a disposición del público para todos los usuarios de AWS. Sin embargo, no puede poner sus instantáneas cifradas a disposición del público por razones de seguridad. Las instantáneas públicas representan un riesgo de seguridad importante debido a la posibilidad de exponer datos personales y confidenciales. Recomendamos encarecidamente no compartir las instantáneas de EBS con todas las cuentas de AWS. Para obtener más información acerca de cómo compartir instantáneas, consulte la documentación de AWS.
- Instantáneas privadas: puede compartir instantáneas de forma privada con las cuentas de AWS individuales que especifique. Para compartir la instantánea de forma privada con cuentas de AWS específicas, siga las instrucciones de la documentación de AWS y elija Privado en la configuración de permisos. Los usuarios que autorice podrán usar las instantáneas que comparta para crear sus propios volúmenes de EBS, mientras que la instantánea original se mantendrá sin cambios.

Resúmenes y procedimientos

La siguiente tabla proporciona enlaces a más información sobre las instantáneas de EBS, incluida la forma de reducir los costos de volumen de EBS mediante el resultado y eliminación de las instantáneas no utilizadas, y de archivar las instantáneas a las que se accede con poca frecuencia y que no requieren una recuperación rápida o frecuente.

Para obtener más información	Consulte
Las instantáneas, sus características y limitaciones	Crear instantáneas de Amazon EBS
Cómo crear una instantánea	Consola: Crear una instantánea AWS CLI: comando create-snapshot Por ejemplo:

```
aws ec2 create-snapshot --volume-id
 vol-1234567890abcdef0 --description
 " volume snapshot"
```

Eliminar instantáneas (información general)	Eliminar una instantánea de Amazon EBS
Cómo eliminar una instantánea	Consola: Eliminar una instantánea AWS CLI: comando delete-snapshot Por ejemplo:

```
aws ec2 delete-snapshot --snapshot-id
 snap-1234567890abcdef0
```

Archivado de instantáneas (información general)	Archivar instantáneas de Amazon EBS Archivo de instantáneas de Amazon EBS (publicación de blog)
Cómo archivar una instantánea	Consola: Archivar una instantánea AWS CLI: modify-snapshot-tier comando
¿Cómo recuperar una instantánea archivada?	Consola: restaurar una instantánea archivada AWS CLI: restore-snapshot-tier comando
Precios de las instantáneas	Precios de Amazon EBS

Preguntas frecuentes

¿Cuál es el periodo de archivo mínimo?

El periodo de archivo mínimo es de 90 días.

¿Cuánto tardaría en restaurarse una instantánea archivada?

Puede tardar hasta 72 horas en restaurar una instantánea archivada del nivel de archivo al nivel estándar, según el tamaño de la instantánea.

¿Las instantáneas archivadas son siempre instantáneas completas?

Las instantáneas archivadas siempre son instantáneas completas.

¿Qué instantáneas puede archivar un usuario?

Solo puede archivar instantáneas que posea en su cuenta.

¿Se puede archivar una instantánea del volumen de dispositivo raíz de una Imagen de máquina de Amazon (AMI) registrada?

No. No puede archivar una instantánea del volumen de dispositivo raíz de una AMI registrada.

¿Cuáles son las consideraciones de seguridad al compartir una instantánea?

Cuando comparte una instantánea, concede a otras personas acceso a todos los datos de la instantánea. Comparta instantáneas solo con aquellas personas en las que confíe sus datos.

¿Cómo se comparte una instantánea con otra región de AWS?

Las instantáneas están restringidas a la región en la que se han creado. Para compartir una instantánea con otra región, copie la instantánea en dicha región y, luego, comparta la copia.

¿Puede compartir instantáneas cifradas?

No puede compartir instantáneas que estén cifradas con la clave administrada de AWS predeterminada. Solo puede compartir instantáneas que estén cifradas con una clave administrada por el cliente. Cuando comparta una instantánea cifrada, también deberá compartir la clave administrada por el cliente usada para cifrar la instantánea.

¿Qué pasa con las instantáneas sin cifrar?

Puede compartir instantáneas sin cifrar de forma pública.

Más patrones

- Automatice la creación de cuentas mediante el acelerador de zonas de aterrizaje en AWS
- Automatice las operaciones de AWS infraestructura con Amazon Bedrock
- Automatice la evaluación de recursos de AWS
- Inventario automático de AWS los recursos en varias cuentas y regiones
- Automatice la implementación de productos y la cartera de AWS Service Catalog mediante AWS CDK
- Automatice la gestión dinámica de canalizaciones para implementar soluciones de hotfix en entornos de Gitflow mediante el uso y AWS Service Catalog AWS CodePipeline
- Automatización de la ingesta y visualización de métricas personalizadas de Amazon MWAA en Amazon Managed Grafana mediante Terraform
- Adjunte automáticamente una política gestionada por AWS para Systems Manager a los perfiles de EC2 instancia mediante Cloud Custodian y AWS CDK
- Cifrar automáticamente los volúmenes de Amazon EBS nuevos y existentes
- Construye una AWS landing zone que incluya MongoDB Atlas
- Centralice la supervisión mediante Amazon CloudWatch Observability Access Manager
- Comprueba EC2 las instancias para ver si hay etiquetas obligatorias en el lanzamiento
- Limpie los recursos de AWS Account Factory for Terraform (AFT) de forma segura después de la pérdida de archivos estatales
- Cree una definición de tareas de Amazon ECS y monte un sistema de archivos en EC2 las instancias mediante Amazon EFS
- Cree reglas AWS Config personalizadas mediante AWS CloudFormation Guard políticas
- Personalice los nombres de los roles predeterminados mediante AWS CDK aspectos y trampillas de escape
- Implemente y gestione AWS Control Tower los controles mediante el uso AWS CDK y CloudFormation
- Implemente y gestione AWS Control Tower controles mediante Terraform
- Implemente código en varias regiones de AWS mediante AWS CodePipeline CodeCommit, AWS y AWS CodeBuild
- Implemente aplicaciones en contenedores si se AWS IoT Greengrass V2 ejecutan como un contenedor Docker

- Habilita Amazon de GuardDuty forma condicional mediante plantillas AWS CloudFormation
- Habilite el archivado de DB2 registros directamente en Amazon S3 en una base de datos IBM Db2
- Exporte un informe de las identidades de AWS IAM Identity Center y sus asignaciones mediante PowerShell
- Genere una CloudFormation plantilla de AWS que contenga las reglas administradas por AWS Config mediante Troposphere
- Otorgue a las instancias de SageMaker notebook acceso temporal a un CodeCommit repositorio de otra cuenta de AWS
- Integrar el controlador universal Stonebranch con AWS Mainframe Modernization
- Lance un CodeBuild proyecto en todas las cuentas de AWS mediante Step Functions y una función de proxy Lambda
- Administre los conjuntos de AWS permisos de forma dinámica mediante Terraform
- Migre IIS-hosted aplicaciones a Amazon EC2 mediante appcmd.exe
- Migración de los certificados SSL de Windows a un equilibrador de carga de aplicación mediante ACM
- Supervisar la actividad del usuario raíz de IAM
- Cree una arquitectura IPAM jerárquica y multirregional mediante Terraform AWS
- Optimice las implementaciones sin servidor con varias cuentas mediante los flujos de trabajo y Actions AWS CDK GitHub
- Preserve el espacio IP enrutable en los diseños de VPC de varias cuentas para subredes que no son de carga de trabajo
- Aprovisionamiento de roles de IAM con privilegio mínimo mediante la implementación de una solución de máquina expendedora de roles
- Registre varios Cuentas de AWS con una sola dirección de correo electrónico mediante Amazon SES
- Elimine EC2 las entradas de Amazon Cuentas de AWS de un lado a otro AWS Managed Microsoft AD mediante AWS Lambda la automatización
- Elimine EC2 las entradas de Amazon en el mismo Cuenta de AWS AWS Managed Microsoft AD formulario mediante AWS Lambda la automatización
- Proteja los datos confidenciales de CloudWatch los registros con Amazon Macie
- Envíe notificaciones para una instancia de base de datos de Amazon RDS para SQL Server mediante un servidor SMTP en las instalaciones y el Correo de base de datos

- Configurar un panel de monitoreo de Grafana para AWS ParallelCluster
- Configuración del registro centralizado a escala empresarial mediante Terraform
- Configurar la recuperación de desastres para SAP en IBM Db2 en AWS
- Optimice la gestión EC2 del cumplimiento de Amazon con los agentes de Amazon Bedrock y AWS Config
- Etiquete automáticamente las conexiones de puerta de enlace de tránsito con AWS Organizations
- Utilice las consultas de BMC Discovery para extraer datos de migración para planificar la migración
- Verifique las mejores prácticas operativas para PCI DSS 4.0 mediante AWS Config
- Visualización de los registros y las métricas de AWS Network Firewall mediante Splunk
- Visualice los informes de credenciales de IAM para todas las cuentas de AWS mediante Amazon Quick Sight

Mensajería y comunicaciones

Temas

- Automatizar la configuración de RabbitMQ en Amazon MQ
- Mejorar la calidad de las llamadas en las estaciones de trabajo de los agentes en los centros de contacto de Amazon Connect
- Más patrones

Automatizar la configuración de RabbitMQ en Amazon MQ

Yogesh Bhatia y Afroz Khan, Amazon Web Services

Resumen

Amazon MQ es un servicio de agente de mensajes administrado que proporciona compatibilidad con muchos de los agentes de mensajes más populares. El uso de Amazon MQ con RabbitMQ proporciona un sólido clúster de RabbitMQ que se administra con varios agentes y opciones de configuración. Nube de AWS Amazon MQ proporciona una infraestructura escalable, segura y de alta disponibilidad, y puede procesar una gran cantidad de mensajes por segundo con facilidad. Varias aplicaciones pueden utilizar la infraestructura con distintos hosts virtuales, colas e intercambios. Sin embargo, administrar estas opciones de configuración o crear la infraestructura manualmente puede requerir tiempo y esfuerzo. Este patrón describe una forma de administrar las configuraciones de RabbitMQ en un solo paso, a través de un único archivo. Puede incrustar el código proporcionado con este patrón en cualquier herramienta de integración continua (CI), como Jenkins o Bamboo.

Puede utilizar este patrón para configurar cualquier clúster de RabbitMQ. Lo único que necesita es conectividad con el clúster. Aunque hay muchas otras maneras de administrar las configuraciones de RabbitMQ, esta solución crea configuraciones de aplicaciones completas en un solo paso, para poder administrar las colas y otros detalles con facilidad.

Requisitos previos y limitaciones

Requisitos previos

- AWS Command Line Interface (AWS CLI) instalado y configurado para apuntar a su Cuenta de AWS
- Ansible instalado, para poder ejecutar guías para crear la configuración
- rabbitmqadmin instalado (para obtener instrucciones, consulte la documentación de RabbitMQ)
- Un clúster de RabbitMQ en Amazon MQ, creado con métricas de Amazon saludables CloudWatch

Requisitos adicionales

- Asegúrese de crear las configuraciones para los hosts virtuales y los usuarios por separado y no como parte de JSON.
- Asegúrese de que el JSON de configuración forme parte del repositorio y esté controlado por versiones.

- La versión de la CLI de rabbitmqadmin debe ser la misma que la versión del servidor de RabbitMQ, por lo que la mejor opción es descargar la CLI desde la consola de RabbitMQ.
- Como parte de la canalización, asegúrese de que la sintaxis JSON esté validada antes de cada ejecución.

Versiones de producto

- AWS CLI versión 2.0
- Ansible versión 2.9.13
- rabbitmqadmin versión 3.9.13 (debe ser la misma que la versión del servidor RabbitMQ)

Arquitectura

Pila de tecnología de origen

- Un clúster de RabbitMQ que se ejecute en una máquina virtual (VM) existente en las instalaciones o en un clúster de Kubernetes (en las instalaciones o en la nube)

Pila de tecnología de destino

- Configuraciones de RabbitMQ automatizadas en Amazon MQ para RabbitMQ

Arquitectura de destino

Existen muchas formas de configurar RabbitMQ. Este patrón utiliza la funcionalidad de configuración de importación, en la que un único archivo JSON contiene todas las configuraciones. Este archivo aplica todos los ajustes y se puede administrar mediante un sistema de control de versiones como Bitbucket o Git. Este patrón utiliza Ansible para implementar la configuración a través de la CLI rabbitmqadmin.

Tools (Herramientas)

Servicios de AWS

- Amazon MQ es un servicio de agente de mensajes administrado que facilita la configuración y el funcionamiento de los agentes de mensajes en la nube.

- AWS CloudFormationle ayuda a configurar su AWS infraestructura y a acelerar el aprovisionamiento en la nube con la infraestructura como código.
- AWS CLIle permite interactuar con él Servicios de AWS mediante comandos de una consola de línea de comandos.

Otras herramientas

- rabbitmqadmin es una herramienta de línea de comandos para la API basada en HTTP de RabbitMQ. Se usa para administrar y supervisar los nodos y clústeres de RabbitMQ.
- Ansible es una herramienta de código abierto para automatizar las aplicaciones y la infraestructura de TI.

Repositorio de código

El archivo de configuración JSON utilizado en este patrón y un ejemplo del manual de estrategias de Ansible se incluyen en el archivo adjunto.

Epics

Cree su infraestructura AWS

Tarea	Descripción	Habilidades requeridas
Cree un clúster de RabbitMQ en. AWS	Si aún no tienes un clúster de RabbitMQ, puedes usarlo para AWS CloudFormationcrear la pila. AWS O bien, puede usar el CloudFormation módulo de Ansible para crear la pila. Con este último enfoque, puede usar Ansible para ambas tareas: crear la infraestructura de RabbitMQ y administrar las configuraciones.	AWS general, Ansible

Crear la configuración de Amazon MQ para RabbitMQ

Tarea	Descripción	Habilidades requeridas
Cree un archivo de propiedades.	Descargue el archivo de configuración JSON (`rabbitmqconfig.json`) del archivo adjunto o expórtelo desde la consola RabbitMQ. Modifíquelo para configurar colas, intercambios y enlaces. En el diagrama siguiente, se muestra esta configuración: • Crea dos colas: y `sample-queue1` `sample-queue2` • Crea dos intercambios: `sample-exchange1` y `sample-exchange2` • Implementa el enlace entre las colas y los intercambios Estas configuraciones se realizan en el host virtual raíz (/), según lo exige rabbitmqadmin.	JSON
Obtenga los detalles de la infraestructura de Amazon MQ para RabbitMQ.	Obtenga los siguientes detalles de la infraestructura de RabbitMQ en: AWS • Nombre del agente • Host de RabbitMQ • Nombre de usuario de RabbitMQ (el usuario	AWS general

Tarea	Descripción	Habilidades requeridas
	administrador creado durante la creación del clúster) • Contraseña de RabbitMQ Puede utilizar el Consola de administración de AWS o el AWS CLI para recuperar esta información. Estos detalles permiten que el manual de estrategias de Ansible se conecte a su clúster RabbitMQ Cuenta de AWS y lo utilice para ejecutar comandos. **Important** El ordenador que ejecuta el manual de estrategias de Ansible debe poder acceder al suyo y debe estar ya configurado Cuenta de AWS, tal y como se AWS CLI describe en la sección Requisitos previos.	

Tarea	Descripción	Habilidades requeridas

Creación del archivo `hosts_var` .	Cree el archivo `hosts_var` para Ansible y asegúrese de que todas las variables estén definidas en el archivo. Considere la posibilidad de utilizar Ansible Vault para almacenar la contraseña. Puede configurar el archivo `hosts_var` de la siguiente manera (sustituya los asteriscos por su información):
	`RABBITMQ_HOST: "**********.mq.us-east-2.amazonaws.com"`
	`RABBITMQ_VHOST: "/"`
	`RABBITMQ_USERNAME: "admin"`
	`RABBITMQ_PASSWORD: "*******"`
		Ansible

Tarea	Descripción	Habilidades requeridas
Cree un manual de Ansible.	Para ver un ejemplo de manual, consulte `ansible-rabbit-config.yaml` en el archivo adjunto. Descargue y guarde este archivo. El manual de Ansible importa y administra todas las configuraciones de RabbitMQ, como las colas, los intercambios y los enlaces, que requieren las aplicaciones. Siga las prácticas recomendadas de los manuales de Ansible, como proteger las contraseñas. Utilice Ansible Vault para cifrar las contraseñas y recupere la contraseña de RabbitMQ del archivo cifrado.	Ansible

Implementación de la configuración

Tarea	Descripción	Habilidades requeridas
Ejecute el manual.	Ejecute el manual de Ansible que creó en la Epics anterior. `ansible-playbook ansible-rabbit-config.yaml`	Información general sobre AWS, RabbitMQ y Ansible

Tarea	Descripción	Habilidades requeridas
	Puede verificar las nuevas configuraciones en la consola RabbitMQ.	

Recursos relacionados

- Migración de RabbitMQ a Amazon MQ (entrada del blog)AWS
- Management Command Line Tool (Herramienta de línea de comandos de administración) (Documentación de RabbitMQ)
- Crear o eliminar una pila (documentación de Ansible AWS CloudFormation)
- Migración de aplicaciones basadas en mensajes a Amazon MQ para AWS RabbitMQ (entrada del blog)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Mejorar la calidad de las llamadas en las estaciones de trabajo de los agentes en los centros de contacto de Amazon Connect

Ernest Ozdoba, Amazon Web Services

Resumen

Los problemas de calidad de las llamadas son algunos de las cuestiones más difíciles de solucionar en los centros de contacto. Para evitar problemas de calidad de voz y procedimientos de solución de problemas complejos, debe optimizar el entorno de trabajo y la configuración de la estación de trabajo de sus agentes. Este patrón describe las técnicas de optimización de la calidad de voz para las estaciones de trabajo de los agentes en los centros de contacto de Amazon Connect. Proporciona recomendaciones en las siguientes áreas:

- Ajustes del entorno de trabajo. El entorno de los agentes no afecta a la forma en que se transmite la voz a través de la red, pero sí afecta a la calidad de las llamadas.
- Configuración de la estación de trabajo del agente. Las configuraciones de hardware y red de las estaciones de trabajo de los centros de contacto tienen efectos significativos en la calidad de las llamadas.
- Configuración del navegador. Los agentes utilizan un navegador web para acceder al sitio web del Panel de control de contactos (CCP) de Amazon Connect y comunicarse con los clientes, por lo que la configuración del navegador puede afectar a la calidad de las llamadas.

Los siguientes componentes también pueden afectar a la calidad de las llamadas, pero quedan fuera del ámbito de la estación de trabajo y no están incluidos en este patrón:

- El tráfico fluye a la nube de Amazon Web Services (AWS) a través de AWS Direct Connect, una VPN de túnel completo o una VPN de túnel dividido
- Condiciones de la red cuando se trabaja dentro o fuera de la oficina corporativa
- Conectividad a una red telefónica pública conmutada (PSTN)
- El dispositivo y el operador de telefonía del cliente
- Infraestructura de escritorio virtual (VDI)

Para obtener más información relacionada con estas áreas, consulte Problemas comunes del panel de control de contactos (CCP) y Utilice la utilidad de prueba de punto de conexión en la documentación de Amazon Connect.

Requisitos previos y limitaciones

Requisitos previos

- Los auriculares y las estaciones de trabajo deben cumplir los requisitos especificados en la Guía del administrador de Amazon Connect.

Limitaciones

- Las técnicas de optimización de este patrón se aplican a la calidad de la voz suave de los teléfonos. No se aplican al configurar el CCP de Amazon Connect en el modo de teléfono de escritorio. Sin embargo, puede usar el modo de teléfono de escritorio si la configuración de su teléfono virtual no proporciona una calidad de voz aceptable para la llamada.

Versiones de producto

- Para ver los navegadores y las versiones compatibles, consulte la Guía del administrador de Amazon Connect.

Arquitectura

Este patrón es independiente de la arquitectura porque se centra en la configuración de la estación de trabajo del agente. Como se muestra en el siguiente diagrama, la ruta de voz del agente al cliente depende de los auriculares, el navegador, el sistema operativo, el hardware de la estación de trabajo y la red del agente.

En los centros de contacto de Amazon Connect, la conectividad de audio del usuario se establece con WebRTC. La voz se codifica con el códec de audio interactivo Opus y se cifra con el Protocolo de transporte seguro en tiempo real (SRTP) en tránsito. Son posibles otras arquitecturas de red, incluidas las redes VPN, WAN/LAN privadas e ISP.

Tools (Herramientas)

- Utilidad de prueba de punto de conexión de Amazon Connect: esta utilidad comprueba la conectividad de la red y la configuración del navegador.
- Editores de configuración del navegador para los ajustes de WebRTC:
  - Para Firefox: about:config

  - Para Chrome: chrome: //flags
- Analizador de registros de CCP: esta herramienta le ayuda a analizar los registros de CCP para solucionar problemas.

Epics

Ajusta el entorno de trabajo

Tarea	Descripción	Habilidades requeridas
Reducir el ruido de fondo.	Evitar los entornos ruidosos. Si esto no es posible, optimice el entorno con estos consejos de insonorización: • Absorba el ruido utilizando superficies que disipen el sonido, como cortinas, alfombras y muebles blandos. • Bloquee el ruido colocando barreras entre los escritorios. • Considere la posibilidad de utilizar una solución de cancelación activa del ruido (ANC), como un generador de ruido blanco, para ayudarle a concentrarse y garantizar la privacidad, o bien utilice auriculares con cancelación de ruido. • Evita el eco en sus llamadas. Los espacios grandes y vacíos pueden crear efectos de eco o	Agente, administrador

Tarea	Descripción	Habilidades requeridas
	amplificar los ruidos. Cubrir las superficies que pueden hacer rebotar los sonidos ayudará a reducir los ecos.	

Optimice la configuración de la estación de trabajo del agente

Tarea	Descripción	Habilidades requeridas
Elegir los auriculares adecuados.	• Si el entorno es ruidoso, elija unos auriculares estéreo. Dirigir el sonido a ambos oídos ayuda a los agentes a concentrarse y a escuchar mejor al cliente, y reduce el ruido general al reducir las probabilidades de que los agentes alcen la voz. • Evite utilizar altavoces o audio de computadora incorporado. Para obtener la mejor calidad, usa unos auriculares con cable diseñados específicamente para el uso en centros de contacto. Los auriculares inalámbricos son prácticos , pero pueden provocar un retraso adicional en el audio y reducir la calidad del audio debido a las interferencias de radio y a la transcodi ficación.	Agente, administrador

Tarea	Descripción	Habilidades requeridas
Utilice los auriculares según lo previsto.	• Active las funciones de reducción activa de ruido y mejora de la voz de los auriculares, si están disponibles. Busque ajustes como ANC o ANR. Para obtener instrucciones sobre cómo activar estos ajustes, consulta el manual del usuario de los auriculares. • Ajuste el micrófono para que pueda hablar directamente con él. La mejor posición para colocar el micrófono es justo debajo de la barbilla. La colocación correcta puede marcar una diferencia de 10 decibelios (dB) en el nivel de sonido. La mayoría de los auriculares permiten girar o doblar el brazo del micrófono (brazo), por lo que es importante mantenerlo en el lugar correcto cuando se habla. • Algunos auriculares están equipados con varios micrófonos y funciones avanzadas, como la formación de haces de voz, que ayuda a capturar la voz sin que se produzca un boom. Para asegurarse de que utiliza el micrófono	Agente

Tarea	Descripción	Habilidades requeridas
	principal según lo previsto por el fabricante, consulte el manual del usuario del dispositivo.	
Compruebe los recursos de la estación de trabajo.	Asegúrese de que las computadoras de sus agentes funcionen correctamente. Si utilizan aplicaciones de terceros que consumen recursos, es posible que sus equipos no cumplan con los requisitos mínimos de hardware para ejecutar CCP. Si los agentes tienen problemas con la calidad de las llamadas, asegúrese de que disponen de suficiente potencia de procesamiento (CPU), espacio en disco, ancho de banda de red y memoria suficientes para el CCP. Los agentes deben cerrar todas las aplicacio nes y pestañas innecesarias para mejorar el rendimiento del CCP y la calidad de las llamadas.	Administrador

Tarea	Descripción	Habilidades requeridas
Configure los ajustes de sonido del sistema operativo.	Los ajustes predeterminados para el nivel y el aumento del micrófono suelen funcionar bien. Si descubre que la voz saliente es baja o que el micrófono capta demasiado , puede que le ayude ajustar estos ajustes. Los ajustes del micrófono se encuentran en la configuración de sonido del sistema de la computadora (sonido, entrada en macOS, propiedades del micrófono en Windows). Puede acceder a los ajustes avanzados que pueden afectar a la calidad de la voz a través de las herramientas del sistema o de aplicaciones de terceros. Estos son algunos de los ajustes que puede comprobar: • Frecuencia de muestreo: este valor determina cuántas veces se sondea el sonido por segundo. La configuración predeterm inada suele ser de 44 o 48 kilohercios (kHz). El valor óptimo para Amazon Connect es de 48 kHz. Puede usar la configura ción de su navegador para anular el valor predeterm inado. Para obtener más	Agente, administrador

Tarea	Descripción	Habilidades requeridas
	información, consulte la sección de solución de problemas de la Guía del administrador de Amazon Connect. • Ganancia: este valor determina en qué medida el micrófono amplifica el sonido. Si aumenta la ganancia, es posible que el micrófono capte más ruido de fondo. • Profundidad de bits: este valor de resolución digital describe cuántos niveles de amplitud de sonido se reconocen. Cuanto mayor sea la profundidad de bits, más suave será el sonido de la voz. Sin embargo, muchas redes de telefonía tradicionales utilizan el estándar de modulació n por pulsos codificados (PCM), que solo admite una resolución de 8 bits. • Umbral abierto: es la amplitud de sonido mínima que capta un micrófono. Si tiene problemas con la calidad de la voz, intente restablecer estos valores a su	

Tarea	Descripción	Habilidades requeridas
	configuración predeterminada antes de seguir investigando. Para obtener más informaci ón acerca de estos ajustes y otros ajustes, consulte el manual del dispositivo.	

Tarea	Descripción	Habilidades requeridas
Utilice una red cableada.	Por lo general, la Ethernet cableada tiene una latencia más baja, por lo que es más fácil proporcionar la calidad de transmisión uniforme requerida para la transmisión de datos de voz. Recomendamos un ancho de banda mínimo de 100 KB por llamada. • Si los agentes trabajan desde casa, recomendamos conexiones cableadas antes que conexiones inalámbricas. Escuchar al cliente no debería tardar más de 150 milisegundos. Puede acceder a la prueba de latencia de Amazon Connect desde la utilidad Amazon Connect Endpoint Test Utility. Sin embargo, esta utilidad mide el retraso desde el navegador hasta las regiones de Amazon Connect, no hasta los clientes. La recomendación de demora unidireccional de 150 milisegundos impide que el agente y el cliente hablen entre sí. El valor se mide de un extremo a otro y cada elemento añade un retraso, incluida la parte de	Administrador de red, agente

Tarea	Descripción	Habilidades requeridas
	la llamada entre la región de Amazon Connect y el cliente. • Si los agentes trabajan desde la oficina, el Wi-Fi corporativo es aceptable siempre que los parámetros estén dentro del rango recomendado y se dé prioridad al tráfico del Protocolo de transporte en tiempo real (RTP).	

Tarea	Descripción	Habilidades requeridas
Actualice los controladores de hardware.	Si utiliza auriculares USB o de otro tipo que tengan su propio firmware, le recomendamos que los mantenga actualizados con la última versión. Los auriculares sencillos que utilizan un puerto auxiliar utilizan el dispositivo de audio integrado en la computadora, así que asegúrese de que el controlador de hardware del sistema operativo esté actualizado. En raras ocasiones, una actualización del controlador de audio puede provocar problemas de audio y es posible que tenga que revertirla. Para obtener más información sobre cómo cambiar las versiones del firmware y del controlador, consulte el manual del dispositivo.	Administrador

Tarea	Descripción	Habilidades requeridas
Evite los concentradores y dongles USB.	Cuando conecte los auriculares, evite usar dispositivos adicionales, como dongles, convertidores de tipo de puerto, concentradores y cables de extensión. Estos dispositivos pueden afectar a la calidad de las llamadas. En su lugar, conecte el dispositivo directamente al puerto de la computadora.	Agente

Tarea	Descripción	Habilidades requeridas
Compruebe los registros del CCP.	El analizador de registros CCP proporciona una forma sencilla de comprobar los registros de las aplicaciones. 1. Descargue los registros del CCP después de una llamada. 2. Abra el analizador de Registros del CCP. 3. Arrastre y suelte el archivo de registro para cargarlo y analizarlo. 4. Cuando se haya analizado el registro, se seleccion ará la pestaña Instantán eas y registros de forma predeterminada. Seleccione la pestaña Métricas situada junto a ella para consultar la información. 5. En la sección Métricas de WebRTC: audio_input, compruebe lo siguiente: • El gráfico del nivel de audio, para ver si el nivel de audio recibido es superior a 0. Esto indica que se ha recibido el audio de la persona que llama. • El gráfico de Paquetes para ver los paquetes perdidos. Si este gráfico	Agente (habilidades avanzadas)

Tarea	Descripción	Habilidades requeridas
	muestra aumentos significativos, póngase en contacto con su equipo de soporte de TI. 6. En la sección Métricas de WebRTC: audio_output, compruebe lo siguiente: • El gráfico del Nivel de audio, para confirmar que el audio se envió desde su dispositivo. • El gráfico de Paquetes. Si observa un aumento en la pérdida de paquetes, infórmelo a su equipo de soporte de TI. • El gráfico Jitter Buffer y RTT. Los valores del tiempo de ida y vuelta (RTT) superiores a 300 afectarán a la experienc ia de llamada. Informe de ello a su equipo de soporte de TI.	

Optimizar la configuración del navegador

Tarea	Descripción	Habilidades requeridas
Restaurar la configuración predeterminada de WebRTC.	La WebRTC debe estar habilitada para realizar llamadas telefónicas flexibles con CCP. Le recomenda	Administrador

Tarea	Descripción	Habilidades requeridas
	mos que utilice la configura ción predeterminada de las funciones relacionadas con WebRTC. • En Chrome, puede configurar banderas navegando hasta la URL chrome: //flags. Escriba WebRTC en el cuadro de búsqueda para encontrar configuraciones que puedan interferir con el CCP y establézcalas como Predeterminadas. • En Firefox, escriba about:config en la barra de direcciones y, a continuac ión, escriba WebRTC en el cuadro de búsqueda de la página de configuración. Los ajustes no predeterm inados aparecen en negrita y se pueden cambiar a Predeterminados.	

Tarea	Descripción	Habilidades requeridas
Deshabilite las extensiones del navegador al solucionar problemas.	Algunas extensiones del navegador pueden afectar a la calidad de las llamadas o incluso impedir que las llamadas se conecten correctamente. Use la ventana de incógnito o el modo privado de su navegador y desactive todas las extensiones. Si eso soluciona el problema, revise las extensiones de su navegador y busque complementos sospechos os, o desactívelos de forma individual.	Agente, administrador
Compruebe la frecuencia de muestreo del navegador.	Confirme que la entrada del micrófono esté configura da en la frecuencia de muestreo óptima de 48 kHz. Para obtener instrucciones, consulte la Guía del administr ador de Amazon Connect.	Agente, administrador

Recursos relacionados

Si ha seguido los pasos de este patrón pero sigue teniendo problemas con la calidad de las llamadas, consulte los siguientes recursos para obtener consejos de solución de problemas.

- Revise los problemas más comunes del Panel de control de contactos (CCP).
- Compruebe la conexión con la utilidad de prueba de terminales.
- Siga la guía de solución de problemas para cualquier otro problema.

Si la solución de problemas y los ajustes no resuelven el problema de calidad de las llamadas, es posible que la causa principal sea externa a la estación de trabajo. Para obtener más información sobre la solución de problemas, póngase en contacto con su equipo de soporte de TI.

Más patrones

- Descomponga monolitos en microservicios mediante CQRS y abastecimiento de eventos
- Implemente una ChatOps solución para gestionar los resultados de los escaneos SAST mediante Amazon Q Developer en aplicaciones de chat, acciones personalizadas y CloudFormation
- Integre Amazon API Gateway con Amazon SQS para gestionar el REST asíncrono APIs
- Simplificación del desarrollo y la implementación de los bots de Amazon Lex mediante un flujo de trabajo automatizado

Estrategia de varias cuentas

Temas

- Migrar una cuenta de AWS miembro de AWS Organizations a AWS Control Tower
- Configure alertas para el cierre programático de cuentas en AWS Organizations
- Más patrones

Migrar una cuenta de AWS miembro de AWS Organizations a AWS Control Tower

Rodolfo Jr. Cerrada, Amazon Web Services

Resumen

Este patrón describe cómo migrar y Cuenta de AWS desde AWS Organizations, si es una cuenta de miembro regida por una cuenta de administración, a AWS Control Tower. Al inscribir la cuenta AWS Control Tower, puede aprovechar las funciones y los controles preventivos y de detección que simplifican la gestión de la cuenta. Es posible que también desee migrar su cuenta de miembro si su cuenta de administración de AWS Organizations se ha visto comprometida y si quiere mover las cuentas de los miembros a una nueva organización que esté gobernada por AWS Control TowerAWS Control Tower.

AWS Control Tower proporciona un marco que combina e integra las capacidades de varias otras y Servicios de AWS, entre AWS Organizations otras, garantiza un cumplimiento y una gobernanza uniformes en todo su entorno de múltiples cuentas. Con AWS Control Tower, puede seguir un conjunto de reglas y definiciones prescritas que amplían las capacidades de AWS Organizations. Por ejemplo, puede usar controles para garantizar que los registros de seguridad y los permisos de acceso entre cuentas necesarios se creen y no se modifiquen.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- AWS Control Tower configurarlo en su organización objetivo en AWS Organizations (para obtener instrucciones, consulte Configuración en la AWS Control Tower documentación)
- Credenciales de administrador para AWS Control Tower (miembro del AWSControlTowerAdminsgrupo)
- Credenciales de administrador de la fuente Cuenta de AWS

Limitaciones

- La cuenta de administración de origen AWS Organizations debe ser diferente de la cuenta de administración de destino de AWS Control Tower.

Versiones de producto

- AWS Control Tower versión 2.3 (febrero de 2020) o posterior (consulte las notas de la versión)

Arquitectura

En el diagrama siguiente se ilustra el proceso de migración y la arquitectura de referencia. Este patrón migra Cuenta de AWS de la organización de origen a una organización de destino regida por AWS Control Tower.

El proceso de inscripción consta de estos pasos:

1. La organización de destino envía una invitación para unir la cuenta a la organización.
2. La cuenta acepta la invitación y pasa a ser miembro de la organización de destino.
3. La cuenta se inscribe en una unidad organizativa (OU) registrada AWS Control Tower y se traslada a ella. (Te recomendamos que consultes el AWS Control Tower panel de control para confirmar la inscripción). En este punto, entran en vigor todos los controles que están habilitados en la unidad organizativa registrada.

Tools (Herramientas)

Servicios de AWS

- AWS Organizationses un servicio de administración de cuentas que le permite consolidar varias entidades Cuentas de AWS en una sola entidad (una organización) que puede crear y administrar de forma centralizada.
- AWS Control Towerintegra las capacidades de otros servicios AWS Organizations, entre los que se incluyen AWS IAM Identity Center AWS Service Catalog, y, ayudarle a aplicar y gestionar las normas de gobernanza en materia de seguridad, operaciones y cumplimiento a escala en todas sus organizaciones y cuentas del Nube de AWS.

Epics

Invite a la cuenta a unirse a la nueva organización con AWS Control Tower

Tarea	Descripción	Habilidades requeridas
Inicia sesión en AWS Control Tower.	Inicie sesión en la AWS Control Tower consola como administrador. Actualmente, no existe una forma directa de mover y pasar Cuenta de AWS de una organización de origen a una organización de una unidad organizativa regida por AWS Control Tower. Sin embargo, puede extender AWS Control Tower la gobernanza a una existente Cuenta de AWS al inscribirla en una OU que ya esté gobernada por ella AWS Control Tower. Por eso, debe iniciar sesión en AWS Control Tower para realizar este paso.	Administrador de AWS Control Tower
Invitar la cuenta miembro.	1. Inicia sesión en la AWS Organizations consola y navega hasta la Cuentas de AWSpágina. 2. En la página Añadir una Cuenta de AWS página, selecciona Invitar a una persona existente Cuenta de AWS. 3. Complete la información de la cuenta, incluido el	Administrador de AWS Control Tower

Tarea	Descripción	Habilidades requeridas
	número de cuenta de 12 dígitos (sin guiones), la descripción y las etiquetas opcionales, y seleccione Enviar invitación. **Important** Compruebe que la transferencia de la cuenta no afectará a ninguna aplicación ni a la conectividad de red. Esta acción envía un correo electrónico de invitación con un enlace a la cuenta de miembro. Cuando el administrador de la cuenta siga el enlace y acepte la invitación, la cuenta del miembro aparecerá en la Cuentas de AWSpágina. Para obtener más información, consulte Administrar las invitaciones de cuentas en la AWS Organizations documentación.	

Tarea	Descripción	Habilidades requeridas
Pruebe las aplicaciones y la conectividad.	Cuando la cuenta del miembro se haya registrado en la nueva organización, aparecerá en la OU dentro de una raíz. También aparece en la AWS Control Tower consola, marcada como no inscrita en las cuentas, porque aún no se ha inscrito en la OU AWS Control Tower registrada. Compruebe lo siguiente: • Consulta el AWS Control Tower panel de control para ver si hay alguna infracción de las barandillas. • Comprueba la conectividad de la red (VPN o AWS Direct Connect) para asegurarte de que no se haya visto afectada por la transferencia. • (Propietarios de aplicación) Pruebe las aplicaciones asociadas a esta cuenta para comprobar que se ejecutan según lo previsto, y que la transferencia de la cuenta no ha afectado a las dependencias.	Administrador de AWS Control Tower, administrador de cuentas de miembros, propietarios de aplicación

Prepare la cuenta para la inclusión

Tarea	Descripción	Habilidades requeridas
Revisa los controles y corrige cualquier infracción.	Revise los controles definidos en la unidad organizativa objetivo, especialmente los controles preventivos, y corrija cualquier infracción. Una serie de controles preventivos obligatorios están activados por defecto cuando configuras tu AWS Control Tower landing zone. Estas barreras no se pueden desactivar. Debe revisar estos controles obligatorios y corregir la cuenta del miembro (manualmente o mediante un script) antes de inscribirla. **Note** Los controles preventivos mantienen las cuentas AWS Control Tower registradas en conformidad y previenen el incumplimiento de las políticas. Cualquier infracción de los controles preventiv os podría afectar a la inscripción. Las	Administrador de AWS Control Tower, administrador de cuentas de miembros

Tarea	Descripción	Habilidades requeridas
	infracciones de control de los Detective s aparecen en el AWS Control Tower panel de control, si se detectan, después de una inscripción correcta. No afectarán al proceso de inscripci ón. Para obtener más información, consulte Acerca de los controles en la AWS Control Tower documentación.	
Compruebe si hay problemas de conectividad después de corregir las infracciones de control.	En algunos casos, es posible que tengas que cerrar puertos específicos o deshabilitar servicios para corregir las infracciones de control. Asegúrese de corregir las aplicaciones que usan esos puertos y servicios antes de inscribir la cuenta.	Propietario de la aplicación

Inscribe la cuenta en AWS Control Tower

Tarea	Descripción	Habilidades requeridas
Inicie sesión en AWS Control Tower.	Inicie sesión en la consola de AWS Control Tower. Utilice credenciales de inicio de sesión para AWS Control	Administrador de AWS Control Tower

Tarea	Descripción	Habilidades requeridas
	Tower las que tenga permisos administrativos. No utilice las credenciales del usuario raíz (cuenta de administr ación) para registrar una AWS Organizations cuenta. Aparecerá un mensaje de error.	

Tarea	Descripción	Habilidades requeridas
Inscriba la cuenta.	1. En la página Account Factory AWS Control Tower, selecciona Inscribir cuenta. 2. Rellene los detalles, incluida la dirección de correo electrónico asociada a la cuenta que desea inscribir, el nombre visible que aparecerá AWS Control Tower, la dirección de correo electrónico del centro de identidad de IAM, el nombre y apellidos del propietario de la cuenta y la OU en la que desea inscribir la cuenta. La dirección de correo electrónico de IAM Identity Center es su dirección de correo electrónico de usuario preferida. Puede usar la misma dirección de correo electrónico que la cuenta. 3. Seleccione Enroll account (Inscribir cuenta). Para obtener más información, consulte Acerca de la inscripción de cuentas existentes en la AWS Control Tower documentación.	Administrador de AWS Control Tower

Verifique la cuenta después de la inscripción

Tarea	Descripción	Habilidades requeridas
Verifique la cuenta.	Desde AWS Control Tower, elija Cuentas. La cuenta que acaba de inscribir tendrá el estado inicial Inscribiendo. Cuando se complete la inscripción, su estado cambiará a Inscrito.	Administrador de AWS Control Tower, administrador de cuentas de miembros
Compruebe si hay infracciones de control.	Los controles definidos en la OU se aplicarán automáticamente a la cuenta del miembro inscrito. Supervise el AWS Control Tower panel de control para detectar infracciones y corríjalas en consecuencia. Para obtener más información, consulte Acerca de los controles en la AWS Control Tower documentación.	Administrador de AWS Control Tower, administrador de cuentas de miembros

Resolución de problemas

Problema	Solución
Recibe el mensaje de error: Se ha producido un error desconocido. Vuelva a intentarlo más tarde o póngase en contacto con AWS Support.	Este error se produce al utilizar las credenciales de usuario raíz (cuenta de administración) AWS Control Tower para registrar una cuenta nueva. AWS Service Catalog no puede asignar la cartera o el producto de Account Factory al usuario raíz, lo que genera un mensaje de error. Para corregir este error, introduzca

Problema	Solución
	credenciales de usuario (administrador) que no sean raíz y tengan acceso completo para inscribir la nueva cuenta. Para obtener más información sobre cómo asignar el acceso administrativo a un usuario administrativo, consulte Primeros pasos en la documentación del Centro de identidades de IAM.
La página de AWS Control Tower actividades muestra la acción Get Catastrofic Drift.	Esta acción refleja una revisión del servicio y no indica ningún problema con la AWS Control Tower configuración. No hay que hacer nada más.

Recursos relacionados

Documentación

- Terminología y conceptos (AWS Organizations documentación)
- ¿Qué es AWS Control Tower? (AWS Control Tower documentación)
- Eliminar una cuenta de miembro de una organización (AWS Organizations documentación)
- Configuración (AWS Control Tower documentación)

Tutoriales y videos

- AWS Control Tower taller (taller a su propio ritmo)
- ¿Qué es? AWS Control Tower (vídeo)
- Aprovisionamiento de usuarios en AWS Control Tower (vídeo)

Configure alertas para el cierre programático de cuentas en AWS Organizations

Richard Milner-Watts, Debojit Bhadra y Manav Yadav, Amazon Web Services

Resumen

La CloseAccount API para AWS Organizations le permite cerrar las cuentas de los miembros de una organización mediante programación, sin tener que iniciar sesión en la cuenta con las credenciales raíz. La RemoveAccountFromOrganization API extrae una cuenta de una organización en AWS Organizations, por lo que pasa a ser una cuenta independiente.

Esto APIs podría aumentar el número de operadores que pueden cerrar o eliminar una cuenta de AWS. Todos los usuarios que tengan acceso a la organización a través de AWS Identity and Access Management (IAM) en la cuenta de administración de AWS Organizations pueden llamarlos APIs, por lo que el acceso no se limita al propietario del correo raíz de la cuenta con ningún dispositivo de autenticación multifactor (MFA) asociado.

Este patrón implementa alertas cuando `RemoveAccountFromOrganization` APIs se llama a las `CloseAccount` teclas y, de este modo, puede supervisar estas actividades. Para alertas, utiliza un tema de Amazon Simple Notification Service (Amazon SNS) También puede configurar las notificaciones de Slack mediante un webhook.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una organización en AWS Organizations
- Acceso a la cuenta de administración de la organización, ubicada en la raíz de la organización, para crear los recursos necesarios

Limitaciones

- Como se describe en la referencia de la API de AWS Organizations, la API `CloseAccount` permite cerrar solo el 10 % de las cuentas de los miembros activos en un período continuo de 30 días.

- Cuando se cierra una cuenta de AWS, su estado cambia a SUSPENDIDA. Durante 90 días después de esta transición de estado, AWS Support puede volver a abrir la cuenta. La cuenta se elimina permanentemente después de 90 días.
- Usuarios que tienen acceso a la cuenta de administración de AWS Organizations y APIs que también pueden tener permisos para deshabilitar estas alertas. Si lo que más preocupa es un comportamiento malicioso en lugar de una eliminación accidental, considere la posibilidad de proteger los recursos creados por este patrón con un límite de permisos de IAM.
- La API llama a `CloseAccount` y `RemoveAccountFromOrganization` procesa mediante la región Este de EE. UU. (Norte de Virginia) (`us-east-1`). Por lo tanto, usted debe implementar esta solución en `us-east-1` para poder observar los eventos.

Arquitectura

Pila de tecnología de destino

- AWS Organizations
- AWS CloudTrail
- Amazon EventBridge
- AWS Lambda
- Amazon SNS

Arquitectura de destino

El siguiente diagrama muestra la arquitectura de soluciones para este patrón.

1. AWS Organizations procesa una solicitud `CloseAccount` o `RemoveAccountFromOrganization`.
2. Amazon EventBridge está integrado con AWS CloudTrail para enviar estos eventos al bus de eventos predeterminado.
3. Una EventBridge regla de Amazon personalizada coincide con las solicitudes de AWS Organizations y llama a una función de AWS Lambda.
4. La función de Lambda envía un mensaje a un tema de SNS, al que los usuarios pueden suscribirse para recibir alertas por correo electrónico o para su posterior procesamiento.

5. Si las notificaciones de Slack están habilitadas, la función de Lambda envía un mensaje a un webhook de Slack.

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormation proporciona una forma de modelar un conjunto de recursos relacionados de AWS y de terceros, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de sus ciclos de vida, tratando la infraestructura como código.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que puede utilizar para conectar sus aplicaciones con datos de diversas fuentes. EventBridge recibe un evento, un indicador de un cambio en el entorno, y aplica una regla para enrutar el evento a un objetivo. Las reglas hacen coincidir los eventos con los objetivos o bien en función de la estructura del evento, llamado un patrón de evento, o bien de una programación.
- AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo paga por el tiempo de proceso que consume. No se aplican cargos cuando su código no se está ejecutando.
- AWS Organizations le ayuda a administrar y gobernar su entorno de forma centralizada a medida que hace crecer y escalar sus recursos de AWS. Con AWS Organizations, puede crear nuevas cuentas de AWS y asignar recursos mediante programación, agrupar cuentas para organizar sus flujos de trabajo, aplicar políticas a cuentas o grupos para el control y simplificar la facturación mediante un único método de pago para todas sus cuentas.
- AWS CloudTrail monitorea y registra la actividad de las cuentas en toda su infraestructura de AWS y le permite controlar las acciones de almacenamiento, análisis y corrección.
- Amazon Simple Notification Service (Amazon SNS) es un servicio de mensajería totalmente gestionado para application-to-application la comunicación (A2A) application-to-person y (A2P).

Otras herramientas

- La biblioteca AWS Lambda Powertools para Python es un conjunto de utilidades que proporcionan funciones de seguimiento, registro, métricas y gestión de eventos para las funciones de Lambda.

Code

El código de este patrón se encuentra en el repositorio GitHub AWS Account Closer Notifier.

La solución incluye una CloudFormation plantilla que implementa la arquitectura de este patrón. Utilice la biblioteca AWS Lambda Powertools para Python para proporcionar registro y seguimiento.

Epics

Implementación de la arquitectura

Tarea	Descripción	Habilidades requeridas
Lance la CloudFormation plantilla para la pila de soluciones.	La CloudFormation plantilla para este patrón se encuentra en la rama principal del GitHub repositorio. Implement a las funciones de IAM, EventBridge las reglas, las funciones de Lambda y el tema SNS. Para iniciar la plantilla: 1. Clone el GitHub repositorio para obtener una copia del código de la solución. 2. Abra la consola de administración de AWS para la cuenta de administr ación de AWS Organizat ions. 3. Elija la región EE.UU. Este (Norte de Virginia) (`us-east-1`) y, a continuac ión, abra la CloudFormation consola. 4. Cree la pila utilizando la plantilla `account-c losure-notifier.ym`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	`l` y especificando los siguientes valores: • Nombre de pila: `aws-account-closure-notifier-stack` • Parámetro `ResourcePrefix` : `aws-account-closure-notifier` • Parámetro `SlackNotification` : si se requieren notificaciones de Slack, cambie esta configuración a `true`. • Parámetro `SlackWebhookEndpoint` : si se requieren notificaciones de Slack, especifique la URL del webhook. Para obtener más información sobre el lanzamiento de una CloudFormation pila, consulte la documentación de AWS.	

Tarea	Descripción	Habilidades requeridas
Compruebe que la solución se haya lanzado correctamente.	1. Espere a que la CloudFormation pila alcance el estado CREATE_COMPLETE. 2. Abre la consola. EventBridge `us-east-1` 3. Compruebe que se haya creado una nueva regla con ese nombre `aws-account-closure-notifier-event-rule` .	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Suscríbase al tema de SNS.	(Opcional) Si quiere suscribir se al tema de SNS: 1. Abra la consola de Amazon SNS en `us-east-1` y busque el tema denominado `aws-account-closure-notifier-sns-topic`. 2. Elija el nombre del tema y, a continuación, elija Create subscription (Crear suscripción). 3. En Protocol (Protocolo), elija Email (Correo electrónico). 4. En Endpoint (Punto de conexión), escriba una dirección de correo electrónico que puede utilizar para recibir la notificación y, a continuación, elija Create subscription (Crear suscripción). 5. Revise su bandeja de entrada de correo electrónico para ver si hay algún mensaje de AWS Notifications. Utilice el enlace del correo electrónico para confirmar la suscripción. Para obtener más información acerca de la configuración	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	de notificaciones de SNS, consulte la documentación de Amazon SNS.	

Verificación de la solución

Tarea	Descripción	Habilidades requeridas
Envíe un evento de prueba al bus de eventos predeterminado.	El GitHub repositorio proporciona un ejemplo de evento que puede enviar al bus de eventos EventBridge predeterminado para probarlo. La EventBridge regla también reacciona ante los eventos que utilizan la fuente de eventos personalizada `aaccount.closure.notifier` . **Note** No puede usar la fuente del CloudTrail evento para enviar este evento, ya que no es posible enviar un evento como un servicio de AWS. Para enviar un evento de prueba:	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	1. Abra la EventBridge consola en `us-east-1` . 2. En el panel de navegación, en Buses, elija Event buses (Buses de eventos) y, a continuación, seleccione el bus de eventos predeterminado. 3. Seleccione Send events (Enviar eventos). 4. En Event source (Origen del evento), introduzca `account.closure.notifier` . 5. En Detail type (Tipo de detalle), introduzca `AWS API Call via CloudTrail` . 6. Para ver los detalles del evento, copia y pega el contenido `tests/dummy-event.json` del GitHub repositorio en el cuadro de texto. 7. Seleccione Send (Enviar) para iniciar el flujo de trabajo de notificaciones.	

Tarea	Descripción	Habilidades requeridas
Compruebe que se ha recibido la notificación por correo electrónico.	Compruebe si hay notificaciones en el buzón de correo que se suscribió al tema de SNS. Usted debería recibir un correo electrónico con la información sobre la cuenta que se cerró y la entidad principal que realizó la llamada a la API.	Administrador de AWS
Verifique que se haya recibido la notificación de Slack.	(Opcional) Si especificaste una URL de webhook para el `SlackWebhookEndpoint` parámetro al implementar la CloudFormation plantilla, comprueba el canal de Slack que está asignado al webhook. Debería mostrar un mensaje con la información de la cuenta que se cerró y de la entidad principal que realizó la llamada a la API.	Administrador de AWS

Recursos relacionados

- CloseAccount acción (referencia de la API de AWS Organizations)
- RemoveAccountFromOrganization acción (referencia de la API de AWS Organizations)
- AWS Lambda Powertools para Python

Más patrones

- Automatice la creación de cuentas mediante el acelerador de zonas de aterrizaje en AWS
- Automatice la eliminación de AWS CloudFormation pilas y recursos asociados
- Automatice la gestión dinámica de canalizaciones para implementar soluciones de hotfix en entornos de Gitflow mediante el uso y AWS Service Catalog AWS CodePipeline
- Cree una malla de datos empresarial con Amazon DataZone y AWS CDK AWS CloudFormation
- Centralice la supervisión mediante Amazon CloudWatch Observability Access Manager
- Control de los conjuntos de permisos para varias cuentas mediante Account Factory for Terraform
- Implementa una estrategia de ramificación de Gitflow para entornos de múltiples cuentas DevOps
- Implemente una estrategia GitHub de ramificación de Flow para entornos de cuentas múltiples DevOps
- Implemente una estrategia de ramificación troncal para entornos de cuentas múltiples DevOps
- Administre los conjuntos de AWS permisos de forma dinámica mediante Terraform
- Cree una arquitectura IPAM jerárquica y multirregional mediante Terraform AWS
- Configure la detección de CloudFormation desviaciones en una organización multirregional y multicuenta
- Configurar la resolución de DNS para redes híbridas en un entorno de cuentas múltiples AWS

Seguridad, & cumplimiento de identidad

Temas

- Automatice la respuesta a incidentes y el análisis forense
- Audite automáticamente los grupos de AWS seguridad que permiten el acceso desde direcciones IP públicas
- Corrija automáticamente las instancias y los clústeres de bases de datos de Amazon RDS no cifrados
- Valide e implemente automáticamente las políticas y funciones de IAM mediante CodePipeline IAM Access Analyzer y macros de AWS CloudFormation
- Integración bidireccional AWS Security Hub CSPM con el software de Jira
- Cree una canalización para imágenes de contenedores reforzadas con EC2 Image Builder y Terraform
- Centralización de la administración de claves de acceso de IAM en AWS Organizations mediante Terraform
- Comprueba la versión de registro de acceso, HTTPS y TLS en una CloudFront distribución de Amazon
- Elección de un flujo de autenticación de Amazon Cognito para aplicaciones empresariales
- Cree reglas AWS Config personalizadas mediante AWS CloudFormation Guard políticas
- Cree un informe consolidado de los hallazgos de seguridad de Prowler a partir de múltiples Cuentas de AWS
- Implemente y gestione AWS Control Tower los controles mediante el uso AWS CDK y CloudFormation
- Implemente y gestione AWS Control Tower controles mediante Terraform
- Implemente las automatizaciones de seguridad para la AWS WAF solución mediante Terraform
- Implementación de una canalización que detecte simultáneamente los problemas de seguridad en varios entregables de código
- Implemente controles de acceso basados en atributos de detección para subredes públicas mediante AWS Config
- Implementación de controles de acceso preventivos basados en atributos para las subredes públicas

- Detección de las instancias de bases de datos de Amazon RDS y Aurora que tienen certificados CA vencidos
- Genere dinámicamente una política de IAM con IAM Access Analyzer mediante Step Functions
- Habilita Amazon de GuardDuty forma condicional mediante plantillas AWS CloudFormation
- Habilitar el cifrado transparente de datos en Amazon RDS para SQL Server
- Supervisar y corregir la eliminación programada de las claves de AWS KMS
- Identifique los buckets públicos de Amazon S3 AWS Organizations mediante Security Hub (CSPM)
- Ingesta y análisis de registros de seguridad de AWS en Microsoft Sentinel
- Gestione AWS Organizations las políticas como código mediante AWS CodePipeline Amazon Bedrock
- Administre los conjuntos de AWS IAM Identity Center permisos como código mediante AWS CodePipeline
- Administrar credenciales mediante AWS Secrets Manager
- Supervise ElastiCache los clústeres de Amazon para comprobar el cifrado en reposo
- Supervisar la actividad del usuario raíz de IAM
- Enviar una notificación cuando se cree un usuario de IAM
- Impedir el acceso a Internet de las cuentas mediante una política de control de servicios
- Exporte un informe de las identidades de AWS IAM Identity Center y sus asignaciones mediante PowerShell
- Restrinja el acceso en función de la dirección IP o la geolocalización mediante AWS WAF
- Escanea los repositorios de Git en busca de información confidencial y problemas de seguridad mediante git-secrets
- Proteja las transferencias de archivos mediante Transfer Family, Amazon Cognito y GuardDuty
- Proteja los datos confidenciales de CloudWatch los registros con Amazon Macie
- Asegurar AWS IAM Roles Anywhere con un certificado privado
- Enviar alertas desde AWS Network Firewall a un canal de Slack
- Envío de atributos personalizados a Amazon Cognito e ingesta en los tokens
- Simplifique la administración de certificados privados mediante AWS Private CA y AWS RAM
- Optimice la gestión EC2 del cumplimiento de Amazon con los agentes de Amazon Bedrock y AWS Config
- Actualice las credenciales de la CLI de AWS desde el centro de identidad de IAM de AWS mediante PowerShell

- Uso de Network Firewall para capturar los nombres de dominio de DNS de la indicación del nombre del servidor para el tráfico saliente
- Usa Terraform para habilitar Amazon automáticamente GuardDuty para una organización
- Verifique las mejores prácticas operativas para PCI DSS 4.0 mediante AWS Config
- Más patrones

Automatice la respuesta a incidentes y el análisis forense

Lucas Kauffman y Tomek Jakubowski, Amazon Web Services

Resumen

Este patrón implementa un conjunto de procesos que utilizan AWS Lambda funciones para proporcionar lo siguiente:

- Una forma de iniciar el proceso de respuesta a un incidente con un conocimiento mínimo
- Procesos automatizados y repetibles que están alineados con la Guía de respuesta ante incidentes de seguridad de AWS
- Separación de cuentas para ejecutar los pasos de automatización, almacenar artefactos y crear entornos forenses

El marco forense y de respuesta automática a incidentes sigue un proceso forense digital estándar que consta de las siguientes fases:

1. Contención
2. Adquisición
3. Examen
4. Análisis

Puede realizar investigaciones sobre datos estáticos (por ejemplo, memoria adquirida o imágenes de disco) y sobre datos dinámicos activos pero en sistemas separados.

Para más información, consulte la sección Detalles adicionales.

Requisitos previos y limitaciones

Requisitos previos

- Dos: Cuentas de AWS
  - Cuenta de seguridad, que puede ser una cuenta existente, pero preferiblemente nueva
  - Cuenta forense, preferiblemente nueva
- AWS Organizations configurar

- En las cuentas de los miembros de organizaciones:
  - La función Amazon Elastic Compute Cloud (Amazon EC2) debe tener acceso Get and List a Amazon Simple Storage Service (Amazon S3) y ser accesible por. AWS Systems Manager Se recomienda utilizar la función `AmazonSSMManagedInstanceCore` AWS gestionada. Tenga en cuenta que este rol se asociará automáticamente a la instancia de Amazon EC2 cuando se inicie la respuesta al incidente. Una vez finalizada la respuesta, AWS Identity and Access Management (IAM) eliminará todos los derechos de la instancia.
  - Puntos finales de nube privada virtual (VPC) en la cuenta del AWS miembro y en las VPC de respuesta y análisis de incidentes. Estos puntos de conexión son: S3 Gateway, EC2 Messages, SSM y SSM Messages.
- AWS Command Line Interface (AWS CLI) instalado en las instancias de Amazon EC2. Si las instancias de Amazon EC2 no están AWS CLI instaladas, se necesitará acceso a Internet para que la captura de pantalla del disco y la adquisición de memoria funcionen. En este caso, los scripts se conectarán a Internet para descargar los archivos de AWS CLI instalación y los instalarán en las instancias.

Limitaciones

- Este marco no pretende generar artefactos que puedan considerarse pruebas electrónicas y que puedan presentarse ante un tribunal.
- Actualmente, este patrón solo admite instancias basadas en Linux que se ejecutan en una arquitectura x86.

Arquitectura

Arquitectura de destino

Además de la cuenta de miembro, el entorno de destino consta de dos cuentas principales: una cuenta de seguridad y una cuenta de análisis forense. Se utilizan dos cuentas por las siguientes razones:

- Para separarlas de cualquier otra cuenta de cliente a fin de reducir el radio de explosión en caso de un análisis forense fallido
- Para ayudar a garantizar el aislamiento y la protección de la integridad de los artefactos que se están analizando
- Para mantener la confidencialidad de la investigación

- Para evitar situaciones en las que los actores de la amenaza pudieran haber utilizado todos los recursos inmediatamente disponibles para su empresa comprometida al alcanzar las cuotas de servicio y, Cuenta de AWS por lo tanto, impedirle crear una instancia de Amazon EC2 para realizar investigaciones.

Además, disponer de cuentas de seguridad y de análisis forenses independientes permite crear funciones distintas: un sistema de respuesta para obtener pruebas y otra de investigador para analizarlas. Cada rol tendría acceso a su cuenta independiente.

El siguiente diagrama muestra solo la interacción entre las cuentas. Los detalles de cada cuenta se muestran en los diagramas siguientes y se adjunta un diagrama completo.

En el siguiente diagrama se muestra la cuenta de miembro.

1. Un evento se envía al tema de Amazon Simple Notification Service (Amazon SNS) de Slack.

En el siguiente diagrama se muestra la cuenta de seguridad.

2. El tema de Amazon SNS de la cuenta de seguridad inicia los eventos forenses.

En el siguiente diagrama se muestra la cuenta de análisis forense.

La cuenta de seguridad es donde se crean los dos AWS Step Functions flujos de trabajo principales para la adquisición de memoria e imágenes de disco. Una vez ejecutados los flujos de trabajo, acceden a la cuenta de miembro que tiene las instancias de Amazon EC2 involucradas en un incidente e inician un conjunto de funciones de Lambda que recopilarán un volcado de memoria o un volcado de disco. Luego, esos artefactos se almacenan en la cuenta de análisis forense.

La cuenta de análisis forense guardará los artefactos recopilados por el flujo de trabajo de Step Functions en el bucket de Amazon S3 de artefactos de análisis. La cuenta de análisis forense también tendrá una canalización del Generador de imágenes de Amazon EC2 que crea una imagen de máquina de Amazon (AMI) de una instancia de análisis forense. Actualmente, la imagen se basa en SANS SIFT Workstation.

El proceso de creación utiliza la VPC de mantenimiento, que tiene conectividad a Internet. La imagen se puede utilizar posteriormente para activar la instancia de Amazon EC2 para analizar los artefactos recopilados en la VPC de análisis.

La VPC de análisis no tiene conectividad a Internet. De forma predeterminada, el patrón crea tres subredes de análisis privadas. Puede crear hasta 200 subredes, que es la cuota para el número de subredes de una VPC, pero es necesario agregar esas subredes a los puntos finales de la VPC para automatizar la ejecución de comandos en ellos. AWS Systems Manager Session Manager

Desde el punto de vista de las prácticas recomendadas, se recomienda utilizar y hacer lo siguiente: AWS CloudTrail AWS Config

- Realice un seguimiento de los cambios realizados en su cuenta de análisis forense
- Supervise el acceso y la integridad de los artefactos que se almacenan y analizan

Flujo de trabajo

El siguiente diagrama muestra los pasos clave de un flujo de trabajo que incluye el proceso y el árbol de decisiones desde el momento en que una instancia se ve comprometida hasta que se analiza y contiene.

1. ¿Se ha establecido la etiqueta `SecurityIncidentStatus` con el valor Analizar? Si es así, haga lo siguiente:
   a. Adjunte los perfiles de IAM correctos para AWS Systems Manager Amazon S3.
   b. Envíe un mensaje de Amazon SNS a la cola de Amazon SNS de Slack.
   c. Envíe un mensaje de Amazon SNS a la cola `SecurityIncident`.
   d. Invoque el equipo de estado de adquisición de memoria y disco.
2. ¿Se han adquirido la memoria y el disco? Si la respuesta es no, se ha producido un error.
3. Etiquete la instancia de Amazon EC2 con la etiqueta `Contain`.
4. Adjunte el rol de IAM y el grupo de seguridad para aislar completamente la instancia.

Automatización y escala

La intención de este patrón es proporcionar una solución escalable para responder a los incidentes y realizar análisis forenses en varias cuentas de una sola organización. AWS Organizations

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y administrarlos a lo largo de su ciclo de vida en todas Cuentas de AWS las regiones.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto con la que puedes interactuar Servicios de AWS mediante comandos en tu consola de línea de comandos.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Security Hub CSPMproporciona una visión completa del estado de su seguridad en AWS. También le ayuda a comparar su AWS entorno con los estándares y las mejores prácticas del sector de la seguridad.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- AWS Step Functionses un servicio de organización sin servidor que le ayuda a combinar AWS Lambda funciones y otras Servicios de AWS para crear aplicaciones empresariales fundamentales.
- AWS Systems Manager lo ayuda a administrar las aplicaciones y la infraestructura que se ejecutan en la Nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo necesario para detectar y resolver problemas operativos y le ayuda a administrar sus recursos de forma segura y a escala. AWS

Código

Para obtener el código y las directrices específicas de implementación y uso, consulte el repositorio del Marco Forense y de Respuesta GitHub Automatizada a Incidentes.

Epics

Implemente las plantillas CloudFormation

Tarea	Descripción	Habilidades requeridas
Implemente CloudFormation plantillas.	Las CloudFormation plantillas están marcadas del 1 al 7 y la primera palabra del nombre del script indica en qué cuenta se debe implementar la plantilla. Tenga en cuenta que el orden de lanzamiento de las CloudFormation plantillas es importante. • `1-forensic-AnalysisVPCnS3Buckets.yaml` : se implementó en la cuenta de análisis forense. Crea los buckets de Amazon S3 y la VPC de análisis, y se activa. CloudTrail • `2-forensic-MaintenanceVPCnEC2ImageBuilderPipeline.yaml` : implementa la VPC de mantenimiento y la canalización del generador de imágenes basada en SANS SIFT. • `3-security_IR-Disk_Mem_automation.ya`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	`ml` : implementa las funciones en la cuenta de seguridad que permiten la adquisición de discos y memoria. • `4-security_LiME_Volatility_Factory.yaml` : inicia una función de compilación para empezar a crear los módulos de memoria en función de la AMI IDs dada. Tenga en cuenta que IDs las AMI son diferentes en todas partes Regiones de AWS. Siempre que necesite nuevos módulos de memoria, puede volver a ejecutar este script con la nueva AMI IDs. Considere la posibilidad de integrarlo con las canalizaciones de creación de AMI de Golden Image (si se utilizan en su entorno). • `5-member-IR-automation.yaml` : crea la función de automatización de respuesta a incidentes de los miembros, que inicia el proceso de respuesta a incidentes. Permite compartir los volúmenes de Amazon Elastic Block Store (Amazon EBS) entre	

Tarea	Descripción	Habilidades requeridas
	cuentas, publicar automáticamente en los canales de Slack durante el proceso de respuesta a incidentes, iniciar el proceso forense y aislar las instancias una vez finalizado el proceso. • `6-forensic-artifact-s3-policies.yaml` : una vez implementados todos los scripts, este script corrige los permisos necesarios para todas las interacciones entre cuentas. • `7-security-IR-vpc.yaml` : configura una VPC utilizada para el procesamiento del volumen de respuesta a incidentes. Para iniciar el marco de respuesta ante incidentes para una instancia de Amazon EC2 específica, cree una etiqueta con la clave `SecurityIncidentStatus` y el valor `Analyze`. Esto iniciará la función de Lambda de miembro que iniciará automáticamente el aislamiento y la memoria, así como la adquisición de discos.	

Tarea	Descripción	Habilidades requeridas
Opere el marco.	La función de Lambda también volverá a etiquetar el activo al final (o en caso de fallo) con `Contain`. Esto inicia la contención, que aísla completamente la instancia sin un grupo de INBOUND/OUTBOUND seguridad y con una función de IAM que impide todo acceso. Siga los pasos que se indican en el repositorio. GitHub	Administrador de AWS

Implemente acciones personalizadas de Security Hub (CSPM)

Tarea	Descripción	Habilidades requeridas
Implemente las acciones CSPM personalizadas de Security Hub mediante una CloudFormation plantilla.	Para crear una acción personalizada de forma que pueda usar la lista desplegable de Security Hub CSPM, implemente la plantilla. `Modules/SecurityHub Custom Actions/SecurityHubCustomActions.yaml` CloudFormation A continuación, modifique la función `IRAutomation` en cada una de las cuentas de los miembros para permitir que la función de Lambda que ejecuta la acción asuma la	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	función `IRAutomation` . Para obtener más información, consulte el repositorio. GitHub	

Recursos relacionados

- AWS Guía de respuesta a incidentes de seguridad

Información adicional

Al utilizar este entorno, un equipo del centro de operaciones de seguridad (SOC) puede mejorar su proceso de respuesta a los incidentes de seguridad de la siguiente manera:

- Tener la capacidad de realizar análisis forenses en un entorno dividido para evitar comprometer accidentalmente los recursos de producción
- Disponer de un proceso estandarizado, repetible y automatizado para la contención y el análisis.
- Ofrecer a cualquier propietario o administrador de una cuenta la posibilidad de iniciar el proceso de respuesta a los incidentes con un conocimiento mínimo de cómo usar las etiquetas
- Disponer de un entorno limpio y estandarizado para realizar análisis de incidentes y análisis forenses sin el ruido de un entorno más grande
- Tener la capacidad de crear múltiples entornos de análisis en paralelo
- Centrar los recursos del SOC en la respuesta a los incidentes en lugar de en el mantenimiento y la documentación de un entorno forense en la nube
- Pasar de un proceso manual a uno automatizado para lograr la escalabilidad
- Uso CloudFormation de plantillas para mantener la coherencia y evitar tareas repetitivas

Además, evita el uso de una infraestructura persistente y paga por los recursos cuando los necesita.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Audite automáticamente los grupos de AWS seguridad que permiten el acceso desde direcciones IP públicas

Eugene Shifer y Stephen DiCato, Amazon Web Services

Resumen

Como práctica recomendada de seguridad, es fundamental minimizar la exposición de los AWS recursos solo a lo que sea absolutamente necesario. Por ejemplo, los servidores web que sirven al público en general deben permitir el acceso entrante desde Internet, pero el acceso a otras cargas de trabajo debe restringirse a redes específicas para reducir la exposición innecesaria. Los grupos de seguridad de Amazon Virtual Private Cloud (Amazon VPC) son un control eficaz que lo ayudará a limitar el acceso a los recursos. Sin embargo, evaluar los grupos de seguridad puede ser una tarea engorrosa, especialmente en arquitecturas de varias cuentas. las reglas de AWS Config y los controles de AWS Security Hub CSPM pueden ayudarle a identificar los grupos de seguridad que permiten el acceso público de Internet (0.0.0.0/0) a protocolos de comunicación de red específicos, como Secure Shell (SSH), HTTP, HTTPS y el protocolo de escritorio remoto (RDP) de Windows. Sin embargo, estas reglas y controles no se aplican si los servicios se ejecutan en puertos no estándar o si el acceso está restringido a determinadas direcciones IP públicas. Por ejemplo, esto puede ocurrir cuando un servicio web está asociado al puerto TCP 8443 en lugar del puerto TCP 443 estándar. Esto también puede ocurrir cuando los desarrolladores tienen acceso al servidor desde sus redes domésticas, por ejemplo, con fines de prueba.

Para solucionar este problema, puede utilizar la solución de infraestructura como código (IaC) incluida en este patrón para identificar los grupos de seguridad que permiten el acceso desde cualquier dirección IP no privada (no conforme a la RFC 1918) a cualquier carga de trabajo de su organización. Cuenta de AWS AWS La AWS CloudFormationplantilla proporciona una AWS Config regla personalizada, una AWS Lambdafunción y los permisos necesarios. Puede implementarla como una pila en una sola cuenta o como un conjunto de pilas en toda la organización, gestionado de forma integral AWS Organizations.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Experiencia en el uso GitHub

- Si va a realizar la implementación en una sola Cuenta de AWS:
  - Permisos para crear CloudFormation pilas
  - AWS Config configurados en la cuenta de destino
  - (Opcional) Security Hub CSPM configurado en la cuenta de destino
- Si va a realizar un despliegue en una AWS organización:
  - Permisos para crear conjuntos de CloudFormation pilas
  - Security Hub (CSPM) configurado con integración AWS Organizations
  - AWS Config configúrelo en las cuentas en las que va a implementar esta solución
  - Designe Cuenta de AWS a un administrador delegado de un Security Hub (AWS Config CSPM)

Limitaciones

- Si va a realizar la implementación en una cuenta individual que no tiene activado el CSPM de Security Hub, puede utilizarla AWS Config para evaluar los resultados.
- Si va a realizar el despliegue en una organización que no tiene un administrador delegado para AWS Config el CSPM de Security Hub, debe iniciar sesión en las cuentas de los miembros individuales para ver los resultados.
- Si solía administrar y AWS Control Tower controlar las cuentas de su organización, implemente el IaC siguiendo este patrón mediante Customizations for (cFCT). AWS Control Tower El uso de la CloudFormation consola generaría desviaciones en la configuración y AWS Control Tower requeriría que volvieras a inscribir las unidades organizativas () o las cuentas gestionadas. OUs
- Algunas Servicios de AWS no están disponibles en todas las versiones. Regiones de AWS Para conocer la disponibilidad de las regiones, consulte Servicios de AWS by Region. Para los puntos de conexión específicos, consulte la página Service endpoints and quotas y elija el enlace del servicio.

Arquitectura

Desplegarse en un individuo Cuenta de AWS

El siguiente diagrama de arquitectura muestra el despliegue de los AWS recursos en una sola unidad Cuenta de AWS. Los recursos se aprovisionan mediante una CloudFormation plantilla directamente a través de la CloudFormation consola. Si el CSPM de Security Hub está activado, puede ver los resultados en el CSPM AWS Config o en el Security Hub. Si el CSPM de Security Hub no está activado, solo podrá ver los resultados en. AWS Config

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Usted crea una CloudFormation pila. Esto despliega una función Lambda y AWS Config una regla. Tanto la regla como la función se configuran con los permisos AWS Identity and Access Management (de IAM) necesarios para publicar las evaluaciones de los recursos en AWS Config los registros.
2. La AWS Config regla funciona en modo de evaluación detectivesca e invoca la función Lambda cada 24 horas.
3. La función Lambda evalúa los grupos de seguridad y envía las actualizaciones a. AWS Config
4. Security Hub CSPM recibe todos los AWS Config hallazgos.
5. Puede ver los resultados en Security Hub CSPM o en AWS Config, según los servicios que haya configurado en la cuenta.

Implementar en una organización AWS

El siguiente diagrama muestra la implementación del patrón en varias cuentas que se administran mediante AWS Organizations y AWS Control Tower. La CloudFormation plantilla se implementa a través de cFCT. Los resultados de la evaluación se centralizan en Security Hub CSPM en la cuenta de administrador delegado. La sección de AWS CodePipeline flujo de trabajo del diagrama muestra los pasos básicos que se producen durante la implementación de cFCT.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. En la cuenta de administración, cargUE un archivo comprimido (ZIP) de la plantilla de IaC a un bucket de Amazon Simple Storage Service (Amazon S3) que implementa CfCT.
2. La canalización cFCT descomprime el archivo, ejecuta las comprobaciones de cfn-nag (GitHub) y despliega la plantilla como un conjunto de pilas. CloudFormation
3. Según la configuración que especifiques en el archivo de manifiesto de cFCT, CloudFormation StackSets despliega las pilas en cuentas individuales o especificadas. OUs Esto despliega una función Lambda y AWS Config una regla en las cuentas de destino. Tanto la regla como la función se configuran con los permisos de IAM necesarios para publicar las evaluaciones de los recursos en AWS Config los registros.
4. La AWS Config regla funciona en modo de evaluación detectivesca e invoca la función Lambda cada 24 horas.

5. La función Lambda evalúa los grupos de seguridad y envía las actualizaciones a. AWS Config
6. AWS Config reenvía todos los resultados a Security Hub CSPM.
7. Los resultados del CSPM de Security Hub se agregan a la cuenta del administrador delegado.
8. Puede ver los resultados agregados en Security Hub CSPM en la cuenta de administrador delegado.

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todo el territorio y. Cuentas de AWS Regiones de AWS
- AWS Configproporciona una vista detallada de los recursos que tiene Cuenta de AWS y de cómo están configurados. Le ayuda a identificar cómo se relacionan los recursos entre sí y cómo han cambiado sus configuraciones a lo largo del tiempo. Una AWS Config regla define los parámetros de configuración ideales para un recurso y AWS Config puede evaluar si AWS los recursos cumplen las condiciones de la regla.
- AWS Control Towerle ayuda a configurar y administrar un entorno de AWS múltiples cuentas, siguiendo las prácticas recomendadas prescriptivas. Las personalizaciones de AWS Control Tower (cFCT) te ayudan a personalizar tu AWS Control Tower landing zone y a mantenerte alineado con las AWS mejores prácticas. Las personalizaciones de esta solución se implementan mediante CloudFormation plantillas y políticas de control AWS Organizations de servicios (). SCPs
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar múltiples cuentas Cuentas de AWS en una organización que puede crear y administrar de forma centralizada.
- AWS Security Hub CSPMproporciona una visión completa del estado de su seguridad en AWS. También le ayuda a comparar su AWS entorno con los estándares y las mejores prácticas del sector de la seguridad.

Otras herramientas

- Python es un lenguaje de programación informático de uso general.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub Detect vulnerable Security Groups.

Prácticas recomendadas

Le recomendamos que siga las prácticas recomendadas en los siguientes recursos:

- Prácticas recomendadas para unidades organizativas con AWS Organizations (blog sobre operaciones y migraciones en la AWS nube)
- Guía para establecer una base inicial mediante AWS Control Tower el uso de AWS (biblioteca de AWS soluciones)
- Guía para crear y modificar AWS Control Tower recursos (AWS Control Tower documentación)
- Consideraciones sobre el despliegue de CFCT (AWS Control Tower documentación)
- Aplicación de permisos con privilegios mínimos (documentación de IAM)

Epics

Revise la plantilla CloudFormation

Tarea	Descripción	Habilidades requeridas
Determine su estrategia de implementación.	Revise la solución y el código para determinar la estrategi a de implementación de su AWS entorno. Determine si va a realizar la implementación en una sola cuenta o en una AWS organización.	Propietario de la aplicación, AWS general
Clonar el repositorio.	Introduzca el siguiente comando para clonar el repositorio de Detección de grupos de seguridad vulnerabl es:	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	`git clone https://github.com/aws-samples/detect-public-security-groups.git`	
Valide la versión de Python.	1. Vaya al directorio de nivel superior del repositorio clonado: `cd detect-public-security-groups` 2. Abre Security-Group-Public-Assessment.yaml. 3. En el recurso de `SgPublicAccessCheckLambdaFunction`, confirme que la versión de Python es compatible con su objetivo de Regiones de AWS. De forma predeterminada, esta función usa Python 3.12. Para más información, consulte AWS Lambda adds support for Python 3.12. Si es necesario, actualice la versión de Python. 4. Guarde y cierre Security-Group-Public-Assessment.yaml.	Administrador de AWS, desarrollador de aplicaciones

Implemente la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla.	Implemente la CloudFormation plantilla en su AWS entorno. Realice una de las siguientes acciones: • Si va a realizar la implement ación en una sola Cuenta de AWS unidad, siga las instrucciones de Cómo crear una pila. • Si vas a realizar el despliegue en una organización que no está gestionada por AWS Control Tower, sigue las instrucci ones de Cómo crear un conjunto de pilas. • Si vas a realizar el despliegue en una organización gestionada por AWS Control Tower, consulta las instrucciones de la sección Crea tus propias personalizaciones.	Desarrollador de aplicaciones, administrador de AWS, AWS general
Comprobar la implementación.	En la CloudFormation consola, compruebe que la pila o el conjunto de pilas se hayan desplegado correctamente.	Administrador de AWS, propietario de la aplicación

Revisión de resultados

Tarea	Descripción	Habilidades requeridas
Vea los resultados de la AWS Config regla.	En Security Hub CSPM, haga lo siguiente para ver una lista de las conclusiones individua les: 1. Abra la consola CSPM de Security Hub. 2. En el panel de navegación, seleccione Resultados. 3. En el cuadro Agregar filtros, agregue los siguientes filtros: • El estado de conformidad es `FAILED` • El título es `SgPublicA ccessCheck` 4. Seleccione Aplicar. En Security Hub CSPM, haga lo siguiente para ver una lista del total de hallazgos agrupados por: Cuenta de AWS 1. Abra la consola CSPM de Security Hub. 2. En el panel de navegación, elija Hallazgos. 3. Seleccione Crear hallazgo.	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	4. Para seleccionar el atributo de agrupación para el conocimiento: a. Seleccione el cuadro de búsqueda para ver las opciones de filtro. b. Elija Group by (Agrupar por). c. Seleccione AwsAccountId. d. Seleccione Aplicar. 5. En el cuadro Agregar filtros, agregue los siguientes filtros: • El título es `SgPublicAccessCheck` • El estado de conformidad es `FAILED` 6. Seleccione Crear hallazgo. 7. Escriba un Nombre del hallazgo y elija Crear hallazgo. En AWS Config, para ver una lista de las conclusiones, siga las instrucciones que se indican en la documentación sobre la visualización de la información de conformidad y los resultados de la AWS Config evaluación.	

Resolución de problemas

Problema	Solución
Se produce un error al crear o eliminar el conjunto de CloudFormation pilas.	Cuando AWS Control Tower se despliega, impone las barreras de protección necesarias y asume el control de los AWS Config agregador es y las reglas. Esto incluye evitar cualquier alteración directa. CloudFormation Para implementar o eliminar correctamente esta CloudFormation plantilla, incluidos todos los recursos asociados, debe utilizar cFCT.
cFct no puede eliminar la CloudFormation plantilla.	Si la CloudFormation plantilla persiste incluso después de realizar los cambios necesario s en el archivo de manifiesto y eliminar los archivos de plantilla, confirme que el archivo de manifiesto contiene el `enable_st ack_set_deletion` parámetro y que el valor está establecido en. `false` Para más información, consulte Eliminación de un conjunto de pilas en la documentación de CfCT.

Recursos relacionados

- AWS Config Reglas personalizadas (AWS Config documentación)

Corrija automáticamente las instancias y los clústeres de bases de datos de Amazon RDS no cifrados

Ajay Rawat y Josh Joy, Amazon Web Services

Resumen

Este patrón describe cómo corregir automáticamente las instancias y clústeres de bases de datos no cifrados del Amazon Relational Database Service (Amazon RDS) en Amazon Web Services (AWS) mediante AWS Systems Manager runbooks y AWS Config claves (). AWS Key Management Service AWS KMS

Las instancias de base de datos RDS encriptadas proporcionan una capa adicional de protección de datos al proteger sus datos del acceso no autorizado al almacenamiento subyacente. Puede utilizar el cifrado de Amazon RDS para aumentar la protección de los datos de las aplicaciones implementadas en el sistema Nube de AWS y para cumplir con los requisitos de conformidad relativos al cifrado en reposo. Puede habilitar el cifrado para una instancia de base de datos de RDS cuando la cree, pero no después de haberla creado. Sin embargo, puede añadir cifrado a una instancia de base de datos RDS sin cifrar creando una instantánea de su instancia de base de datos y, a continuación, creando una copia cifrada de esa instantánea. A continuación, puede restaurar una instancia de base de datos a partir de la instantánea encriptada para obtener una copia encriptada de su instancia de base de datos original.

Este patrón se utiliza Reglas de AWS Config para evaluar las instancias y los clústeres de bases de datos de RDS. Aplica la corrección mediante AWS Systems Manager manuales de ejecución, que definen las acciones que se deben realizar en los recursos de Amazon RDS no conformes, AWS KMS y claves para cifrar las instantáneas de la base de datos. A continuación, aplica las políticas de control de servicios (SCPs) para evitar la creación de nuevas instancias de bases de datos y clústeres sin cifrado.

El código de este patrón se proporciona en GitHub.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Archivos del repositorio de código GitHub fuente de este patrón descargados a su ordenador

- Una instancia de base de datos de RDS o un clúster sin cifrar
- Una AWS KMS clave existente para cifrar instancias y clústeres de bases de datos de RDS
- Acceso para actualizar la política de recursos de claves de KMS
- AWS Config habilitada en su Cuenta de AWS (consulte Primeros pasos AWS Config en la AWS documentación)

Limitaciones

- Puede activar la encriptación para una instancia de base de datos RDS sólo cuando la cree, no después de haberla creado.
- No se puede tener una réplica de lectura cifrada de una instancia de base de datos sin cifrar ni una réplica de lectura sin cifrar de una instancia de base de datos cifrada.
- No se puede restaurar una copia de seguridad ni una instantánea sin cifrar en una instancia de base de datos cifrada.
- El cifrado de Amazon RDS está disponible para la mayoría de las clases de instancias de bases de datos. Para ver una lista de excepciones, consulte Cifrado de los recursos de Amazon RDS en la documentación de Amazon RDS.
- Para copiar una instantánea cifrada de una Región de AWS a otra, debe especificar la clave KMS en el destino Región de AWS. Esto se debe a que las claves de KMS son específicas del Región de AWS lugar en el que se crearon.
- La instantánea de origen permanece cifrada durante todo el proceso de copia. Amazon RDS utiliza el cifrado de sobre para proteger los datos durante el proceso de copia. Para obtener más información, consulte Cifrado de sobres en la AWS KMS documentación.
- No se puede descifrar una instancia de bases de datos cifrada. Sin embargo, puede exportar datos de una instancia de bases de datos cifrada e importar datos a una instancia de bases de datos sin cifrar.
- Debe eliminar una clave KMS solo cuando esté seguro de que ya no necesita usarla. Si no está seguro, considere la posibilidad de desactivar la clave KMS en lugar de eliminarla. Puede volver a habilitar una clave KMS deshabilitada si necesita volver a usarla más adelante, pero no puede recuperar una clave KMS eliminada.
- Si decide no conservar las copias de seguridad automatizadas, se eliminarán las copias de seguridad automatizadas que estén en la Región de AWS misma instancia de base de datos. No se pueden recuperar después de eliminar la instancia de base de datos.

- Las copias de seguridad automatizadas se retienen durante el período de retención establecido en la instancia de base de datos en el momento de eliminarla. Este período de retención establecido se produce independientemente de si decide crear o no una instantánea de base de datos final.
- Si la corrección automática está habilitada, esta solución cifra todas las bases de datos que tienen la misma clave de KMS.

Arquitectura

El siguiente diagrama ilustra la arquitectura de la CloudFormation implementación. Tenga en cuenta que también puede implementar este patrón mediante AWS Cloud Development Kit (AWS CDK).

Tools (Herramientas)

Herramientas

- CloudFormationle ayuda a configurar automáticamente sus recursos. AWS Le permite utilizar un archivo de plantilla para crear y eliminar una colección de recursos juntos como una sola unidad (una pila).
- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software para definir su infraestructura en la nube en código y aprovisionarla mediante lenguajes de programación conocidos.

Servicios y características de AWS

- AWS Configrealiza un seguimiento de la configuración de sus AWS recursos y de sus relaciones con los demás recursos. También puede evaluar el cumplimiento de esos AWS recursos. Este servicio utiliza reglas que se pueden configurar para evaluar AWS los recursos en función de las configuraciones deseadas. Puede usar un conjunto de reglas AWS Config administradas para escenarios de cumplimiento comunes o puede crear sus propias reglas para escenarios personalizados. Cuando se descubre que un AWS recurso no es conforme, puede especificar una acción correctiva mediante un AWS Systems Manager manual y, si lo desea, enviar una alerta a través de un tema de Amazon Simple Notification Service (Amazon SNS). En otras palabras, puede asociar las acciones de corrección a los recursos no conformes Reglas de AWS Config y optar por ejecutarlas automáticamente para hacer frente a los recursos no conformes sin intervención manual. Si un recurso sigue sin cumplir las normas tras la corrección automática, puede configurar la regla para que vuelva a intentar la corrección automática.

- Amazon Relational Database Service (Amazon RDS) facilita la configuración, la operación y el escalado de una base de datos relacional en la nube. El componente básico de Amazon RDS es la instancia de base de datos, que es un entorno de base de datos aislado en la Nube de AWS. Amazon RDS ofrece una selección de tipos de instancia optimizados para adaptarse a diferentes casos de uso de bases de datos relacionales. Los tipos de instancias tienen varios tipos de combinaciones de CPU, memoria, almacenamiento y capacidad de red. También, brindan la flexibilidad para elegir la combinación adecuada de recursos para las bases de datos. Cada tipo de instancia incluye varios tamaños de instancia, lo que permite escalar sus bases de datos según los requisitos de la carga de trabajo de destino.
- AWS Key Management Service (AWS KMS) es un servicio gestionado que facilita la creación AWS KMS keys, el control y el cifrado de los datos. Una clave KMS es una representación lógica de una clave raíz. La clave de KMS incluye metadatos, como el ID de clave, la fecha de creación, la descripción y el estado de la clave.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- Las políticas de control de servicios (SCPs) ofrecen un control central sobre los permisos máximos disponibles para todas las cuentas de la organización. SCPs le ayudan a garantizar que sus cuentas se ajusten a las directrices de control de acceso de su organización. SCPs no afectan a los usuarios ni a las funciones de la cuenta de administración. Afectan solo a las cuentas de miembro de su organización. Le recomendamos encarecidamente que no se vincule SCPs a la raíz de su organización sin comprobar exhaustivamente el impacto que la política tiene en las cuentas. En lugar de ello, cree una unidad organizativa (UO) en la que pueda mover sus cuentas de una en una, o al menos en incrementos pequeños, a fin de garantizar que no bloquee inadvertidamente a los usuarios de servicios clave.

Código

El código fuente y las plantillas de este patrón están disponibles en un GitHub repositorio. El patrón ofrece dos opciones de implementación: puede implementar una CloudFormation plantilla para crear la función de corrección que cifra las instancias y los clústeres de bases de datos de RDS, o puede utilizar la. AWS CDK El repositorio tiene carpetas independientes para estas dos opciones.

La sección Epics proporciona step-by-step instrucciones para implementar la plantilla. CloudFormation Si desea utilizarla AWS CDK, siga las instrucciones del `README.md` archivo del GitHub repositorio.

Prácticas recomendadas

- Habilite el cifrado de datos en reposo y en tránsito.
- Habilitar AWS Config en todas las cuentas y Regiones de AWS.
- Registre los cambios de configuración de todos los tipos de recursos.
- Rote con regularidad sus credenciales de IAM.
- Aproveche el etiquetado para AWS Config, lo que facilita la administración, la búsqueda y el filtrado de los recursos.

Epics

Creación del rol de corrección de IAM y el manual de procedimientos de Systems Manager

Tarea	Descripción	Habilidades requeridas
Descarga la CloudFormation plantilla.	Descarga el `unencrypted-to-encrypted-rds.template.json` archivo del GitHub repositorio.	DevOps ingeniero
Crea la CloudFormation pila.	1. Inicie sesión en la CloudFormation consola Consola de administración de AWS y ábrala. 2. Inicie la plantilla `unencrypted-to-encrypted-rds.template.json` para crear una nueva pila. Para más información sobre la implementación de plantillas, consulte la documentación de CloudFormation.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Revise CloudFormation los parámetros y valores.	1. Revise los detalles de la pila y actualice los valores en función de los requisitos de su entorno. 2. Elija Crear pila para implementar la plantilla.	DevOps ingeniero
Revise los recursos.	El estado cambia a CREATE_COMPLETE tras crear la pila. Revise los recursos creados (función de IAM, manual de ejecución de Systems Manager) en la CloudFormation consola.	DevOps ingeniero

Actualice la política AWS KMS clave

Tarea	Descripción	Habilidades requeridas
Actualice su política de claves de KMS.	1. Asegúrese de que el alias de la clave `alias/RDS EncryptionAtRestKMSAlias` exista. 2. La instrucción de la política de claves debe incluir el rol de corrección de IAM. (Comprueba los recursos creados por la CloudFormation plantilla que utilizaste en la epopeya anterior). 3. En la siguiente política de claves, actualice las partes que aparecen en negrita para que coincidan con su	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	cuenta y con el rol de IAM que se creó. `{ "Sid": "Allow access through RDS for all principals in the account that are authorized to use RDS", "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam:: <your-AWS-account-ID>":role/<your-IAM-remediation-role>" }, "Action": ["kms:Encrypt", "kms:Decrypt", "kms:ReEncrypt*", "kms:GenerateDataKey*", "kms:CreateGrant", "kms:ListGrants", "kms:DescribeKey"], "Resource": "*", "Condition": { "StringEquals": { "kms:ViaService": "rds.us-east-1.amazonaws.com",`	

Tarea	Descripción	Habilidades requeridas

	<pre>"kms:Call
	erAccount": "<your-AW
	S-account-ID>"
	}
	}
	}</pre>	

Encuentre y corrija los recursos que no cumplen con las normas

Tarea	Descripción	Habilidades requeridas
Vea los recursos que no cumplen con las normas.	1. Para ver una lista de recursos no conformes, abra la consola de AWS Config. 2. En el panel de navegación, elija Reglas y, a continuación, elija la regla `rds-storage-encrypted` . Los recursos no conformes que se muestran en la AWS Config consola serán instancias, no clústeres. La automatización de la corrección cifra las instancias y los clústeres y crea una instancia recién cifrada o un clúster recién creado. Sin embargo, asegúrese de no corregir simultáneamente varias instancias que pertenezcan al mismo clúster.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Antes de corregir cualquier instancia o volumen de base de datos de RDS, asegúrese de que la instancia de base de datos de RDS no esté en uso. Confirme que no se estén realizando operaciones de escritura mientras se crea la instantánea, para asegurarse de que la instantánea contiene los datos originales. Considere la posibilidad de establecer un período de mantenimiento durante el cual se ejecute la corrección.	

Tarea	Descripción	Habilidades requeridas
Resuelva los recursos no conformes.	1. Cuando esté listo y el período de mantenimiento esté activo, elija el recurso que desee corregir y, a continuación, elija Remediar. La columna Estado de la acción debería mostrar ahora la Ejecución de la acción en cola. 2. Vea el progreso y el estado de la corrección en Systems Manager. Abra la consola de Systems Manager. En el panel de navegación, elija Automatización y, a continuación, seleccione el ID de ejecución de la automatización correspondiente para ver más detalles.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Verificar que la instancia de base de datos de RDS esté disponible.	Cuando se complete la automatización, estará disponible la instancia de base de datos RDS recién cifrada. La instancia de base de datos de RDS cifrada tendrá el prefijo `encrypted` seguido del nombre original. Por ejemplo, si el nombre de la instancia de base de datos de RDS no cifrada fuera `database-1` , la instancia de base de datos de RDS recién cifrada sería `encrypted-database-1` .	DevOps ingeniero
Termine la instancia no cifrada.	Una vez completada la corrección y validado el recurso recién cifrado, puede terminar la instancia no cifrada. Asegúrese de confirmar que el recurso recién cifrado coincide con el recurso no cifrado antes de cancelar cualquier recurso.	DevOps ingeniero

Hacer cumplir SCPs

Tarea	Descripción	Habilidades requeridas
Hacer cumplir SCPs.	SCPs Exija su aplicació n para evitar que en el futuro se creen instancias y clústeres de bases de datos	Ingeniero de seguridad

Tarea	Descripción	Habilidades requeridas
	sin cifrado. Para ello, utilice el `rds_encrypted.json` archivo que se proporciona en el GitHub repositorio y siga las instrucciones de la AWS documentación.	

Recursos relacionados

Referencias

- Configuración AWS Config
- AWS Config reglas personalizadas
- AWS KMS conceptos
- AWS Systems Manager documentos
- Políticas de control de servicios

Herramientas

- CloudFormation
- AWS Cloud Development Kit (AWS CDK)

Guías y patrones

- Vuelva a habilitarlo automáticamente AWS CloudTrail mediante una regla de corrección personalizada en AWS Config

Información adicional

¿Cómo funciona? AWS Config

Cuando lo usas AWS Config, primero descubre los AWS recursos compatibles que existen en tu cuenta y genera un elemento de configuración para cada recurso. AWS Config también genera elementos de configuración cuando cambia la configuración de un recurso y mantiene

registros históricos de los elementos de configuración de los recursos desde el momento en que se inicia el registrador de configuración. De forma predeterminada, AWS Config crea elementos de configuración para todos los recursos admitidos en Región de AWS. Si no desea AWS Config crear elementos de configuración para todos los recursos compatibles, puede especificar los tipos de recursos de los que quiere que haga un seguimiento.

¿Cómo están AWS Config y Reglas de AWS Config con qué se relacionan AWS Security Hub CSPM?

AWS Security Hub CSPM es un servicio de seguridad y cumplimiento que proporciona la gestión de la postura de seguridad y cumplimiento como un servicio. Utiliza AWS Config y Reglas de AWS Config es su mecanismo principal para evaluar la configuración de AWS los recursos. Reglas de AWS Config también se puede utilizar para evaluar directamente la configuración de los recursos. Otros Servicios de AWS, como AWS Control Tower y AWS Firewall Manager, también se utilizan Reglas de AWS Config.

Valide e implemente automáticamente las políticas y funciones de IAM mediante CodePipeline IAM Access Analyzer y macros de AWS CloudFormation

Helton Ribeiro y Guilherme Simoes, Amazon Web Services

Resumen

Este patrón describe los pasos y proporciona código para crear un proceso de implementación que permita a sus equipos de desarrollo crear políticas y roles de AWS Identity and Access Management (IAM) en sus cuentas de Amazon Web Services (AWS). Este enfoque ayuda a su organización a reducir los gastos generales de sus equipos operativos y a acelerar el proceso de implementación. También ayuda a sus desarrolladores a crear roles y políticas de IAM que sean compatibles con sus controles de gobierno y seguridad actuales.

El enfoque de este patrón utiliza AWS Identity and Access Management Access Analyzer para validar las políticas de IAM que desea adjuntar a las funciones de IAM y utiliza AWS CloudFormation para implementar las funciones de IAM. Sin embargo, en lugar de editar directamente el archivo de CloudFormation plantilla de AWS, su equipo de desarrollo crea políticas y funciones de IAM con formato JSON. Una CloudFormation macro de AWS transforma estos archivos de políticas con formato JSON en tipos de recursos de AWS CloudFormation IAM antes de comenzar la implementación.

La canalización de implementación (`RolesPipeline`) tiene las etapas de origen, validación e implementación. Durante la fase de origen, su equipo de desarrollo envía los archivos JSON que contienen la definición de las funciones y políticas de IAM a un repositorio de AWS CodeCommit . CodeBuild A continuación, AWS ejecuta un script para validar esos archivos y los copia en un bucket de Amazon Simple Storage Service (Amazon S3). Como sus equipos de desarrollo no tienen acceso directo al archivo de CloudFormation plantilla de AWS almacenado en un depósito de S3 independiente, deben seguir el proceso de creación y validación de archivos JSON.

Por último, durante la fase de implementación, AWS CodeDeploy utiliza una CloudFormation pila de AWS para actualizar o eliminar las políticas y funciones de IAM de una cuenta.

> **Important**
>
> El flujo de trabajo de este patrón es una prueba de concepto (POC) y le recomendamos que solo lo utilice en un entorno de prueba. Si desea utilizar el enfoque de este patrón en

un entorno de producción, consulte las Prácticas recomendadas de seguridad en IAM en la documentación de IAM y realice los cambios necesarios en sus roles de IAM y en los servicios de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un bucket de S3 nuevo o existente para la canalización `RolesPipeline`. Asegúrese de que las credenciales de acceso que está utilizando tengan permisos para cargar objetos en este bucket.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada. Para obtener más información, consulte Instalar, actualizar y desinstalar la CLI de AWS en la documentación de la CLI de AWS.
- CLI de AWS Serverless Application Model (AWS SAM), instalada y configurada. Para obtener más información al respecto, consulte Instalación de la CLI de AWS SAM en la documentación de AWS SAM.
- Python 3, instalado en su máquina local. Para obtener más información, consulte la documentación de Python.
- Un cliente Git, Instalado y configurado.
- El GitHub `IAM roles pipeline` repositorio, clonado en su máquina local.
- Políticas y roles de IAM con formato JSON existentes. Para obtener más información al respecto, consulta el ReadMearchivo en el `IAM roles pipeline` repositorio de Github.
- Su equipo de desarrolladores no debe tener permisos para editar los CodeDeploy recursos de AWS CodePipeline y de esta solución. CodeBuild

Limitaciones

- El flujo de trabajo de este patrón es una prueba de concepto (POC) y le recomendamos que solo lo utilice en un entorno de prueba. Si desea utilizar el enfoque de este patrón en un entorno de producción, consulte las Prácticas recomendadas de seguridad en IAM en la documentación de IAM y realice los cambios necesarios en sus roles de IAM y en los servicios de AWS.

Arquitectura

En el siguiente diagrama, se muestra cómo validar e implementar automáticamente las funciones y políticas de IAM en una cuenta mediante el uso de CodePipeline macros de AWS y IAM Access Analyzer. CloudFormation

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un desarrollador escribe archivos JSON que contienen las definiciones de las políticas y los roles de IAM. El desarrollador envía el código a un CodeCommit repositorio y, a CodePipeline continuación, inicia la canalización. `RolesPipeline`
2. CodeBuild valida los archivos JSON mediante IAM Access Analyzer. Si se detecta algún problema de seguridad o relacionado con errores, se detiene el proceso de implementación.
3. Si no se detecta ningún problema de seguridad o relacionado con errores, los archivos JSON se envían al bucket de S3 `RolesBucket`.
4. A continuación, una CloudFormation macro de AWS implementada como una función de AWS Lambda lee los archivos JSON del `RolesBucket` bucket y los transforma en tipos de recursos de AWS CloudFormation IAM.
5. Una CloudFormation pila de AWS predefinida instala, actualiza o elimina las políticas y funciones de IAM de la cuenta.

Automatización y escala

CloudFormation Las plantillas de AWS que implementan automáticamente este patrón se proporcionan en el repositorio de canalización de roles de GitHub IAM.

Tools (Herramientas)

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- IAM Access Analyzer le ayuda a identificar los recursos de su organización y sus cuentas, como buckets de S3 o roles de IAM, que se comparten con una entidad externa. Esto le ayuda a identificar el acceso no deseado a sus recursos y datos.

- AWS Serverless Application Model (AWS SAM) es un marco de código abierto que permite crear aplicaciones sin servidor en la nube de AWS.

Código

El código fuente y las plantillas de este patrón están disponibles en el repositorio de la canalización de roles de GitHub IAM.

Epics

Clone el repositorio

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de muestra.	Clona el repositorio de canalización de roles de GitHub IAM en tu máquina local.	Desarrollador de aplicaciones, AWS general

Implemente la canalización RolesPipeline

Tarea	Descripción	Habilidades requeridas
Implemente la canalización.	1. Vaya al directorio que contiene el repositorio clonado. 2. **Important** Ejecute el comando `make deploy bucket=<bucket_name>` . Debe reemplazar `<bucket_name>` con el nombre de	Desarrollador de aplicaciones, AWS general

Tarea	Descripción	Habilidades requeridas
	bucket de su bucket de S3 existente. 3. Ejecute el comando `aws codepipeline get-pipeline –name RolesPipeline` para comprobar si la implement ación se ha realizado correctamente.	
Clone el repositorio de la canalización.	1. La CloudFormation pila de `RolesPipeline` AWS crea el `roles-pipeline-repo` CodeCommit repositorio. 2. Inicie sesión en la consola de administración de AWS, abra la CodeCommi t consola de AWS y, a continuación, copie la URL del CodeCommit repositorio para clonarlo en su máquina local. Para obtener más información al respecto, consulte Conectarse a un CodeCommit repositorio de AWS en la CodeCommit documentación de AWS.	Desarrollador de aplicaciones, AWS general

Pruebe la RolesPipeline canalización

Tarea	Descripción	Habilidades requeridas
Pruebe la RolesPipeline canalización con políticas y funciones de IAM válidas.	1. Cree archivos JSON para sus políticas y roles de IAM. Puede utilizar los ejemplos del `role-example` directorio del GitHub `IAM roles pipeline` repositorio. 2. **Important** Defina sus políticas y roles de IAM con las configuraciones requeridas. : Asegúrese de seguir el formato descrito en el `ReadMe` archivo del GitHub `IAM roles pipeline` repositorio. 3. Inserte las modificaciones en el `roles-pipeline-repo` CodeCommit repositorio. 4. Verifique la implementación de la canalización `RolesPipeline` . 5. Asegúrese de que las políticas y los roles de IAM estén implementados correctamente en la cuenta.	Desarrollador de aplicaciones, AWS general

Tarea	Descripción	Habilidades requeridas
	6. Valide si existe un límite de permisos asociado a las políticas o los roles de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la documentación de IAM.	
Pruebe la RolesPipeline canalización con políticas y funciones de IAM no válidas.	1. Modifique el `roles-pipeline-repo` CodeCommit repositorio e incluya funciones o políticas de IAM no válidas. Por ejemplo, puede utilizar una acción que no exista o una versión de la política de IAM no válida. 2. Verifique la implementación de la canalización. IAM Access Analyzer detiene la canalización durante la fase de validación si detecta políticas o roles de IAM no válidos.	Desarrollador de aplicaciones, AWS general

Eliminación de sus recursos

Tarea	Descripción	Habilidades requeridas
Prepárese para la limpieza.	Vacíe los buckets de S3 y, a continuación, ejecute el comando `destroy`.	Desarrollador de aplicaciones, AWS general

Tarea	Descripción	Habilidades requeridas
Elimine la RolesStack pila.	1. La `RolesPipeline` canalización crea una CloudFormation pila de `RolesStack` AWS que implementa las políticas y funciones de IAM. Debe eliminar esta pila antes de eliminar la canalización `RolesPipeline` . 2. Inicie sesión en la consola de administración de AWS, abra la CloudForm ation consola de AWS y, a continuación, elija la `RolesStack` pila y elija Eliminar.	Desarrollador de aplicaciones, AWS general
Elimine la RolesPipeline pila.	Para eliminar la CloudForm ation pila de `RolesPipe line` AWS, sigue las instrucciones del ReadMearchivo del `IAM roles pipeline` repositorio de Github.	Desarrollador de aplicaciones, AWS general

Recursos relacionados

- IAM Access Analyzer: validación de políticas (Blog de noticias de AWS)
- Uso de CloudFormation macros de AWS para realizar un procesamiento personalizado en plantillas (CloudFormation documentación de AWS)
- Creación de funciones Lambda con Python (documentación de AWS Lambda)

Integración bidireccional AWS Security Hub CSPM con el software de Jira

Joaquin Rinaudo, Amazon Web Services

Resumen

Esta solución admite una integración bidireccional entre Jira y Jira. AWS Security Hub CSPM Con esta solución, puedes crear y actualizar los tickets de Jira de forma automática y manual a partir de las conclusiones del CSPM de Security Hub. Los equipos de seguridad pueden usar esta integración para notificar a los equipos de desarrollo cualquier resultado grave en materia de seguridad que requiera la adopción de medidas.

La solución le permite:

- Selecciona qué controles de CSPM de Security Hub crean o actualizan automáticamente los tickets en Jira.
- En la consola CSPM de Security Hub, usa las acciones personalizadas de CSPM de Security Hub para escalar manualmente los tickets en Jira.
- Asigna automáticamente los tickets en Jira en función de las etiquetas definidas en. Cuenta de AWS AWS Organizations Si esta etiqueta no está definida, se asignan de forma predeterminada.
- Suprime automáticamente los hallazgos de CSPM de Security Hub que estén marcados como falsos positivos o riesgos aceptados en Jira.
- Cierra automáticamente un ticket de Jira cuando su hallazgo relacionado esté archivado en Security Hub CSPM.
- Vuelva a abrir los tickets de Jira cuando se repitan los hallazgos de CSPM de Security Hub.

Flujo de trabajo de Jira

La solución emplea un flujo de trabajo de Jira personalizado que permite a los desarrolladores gestionar y documentar los riesgos. A medida que el problema avanza en el flujo de trabajo, la integración bidireccional garantiza que el estado del ticket de Jira y la búsqueda de CSPM de Security Hub estén sincronizados en todos los flujos de trabajo de ambos servicios. Este flujo de trabajo es un derivado de SecDevOps Risk Workflow de Dinis Cruz, licenciado bajo la licencia Apache versión 2.0. Recomendamos añadir una condición de flujo de trabajo de Jira para que solo los miembros de su equipo de seguridad puedan cambiar el estado del ticket.

Para ver un ejemplo de ticket de Jira generado automáticamente por esta solución, consulte la sección de Información adicional de este patrón.

Requisitos previos y limitaciones

Requisitos previos

- Si desea implementar esta solución en un entorno de múltiples cuentas AWS :
  - Su entorno de múltiples cuentas está activo y gestionado por. AWS Organizations
  - El CSPM de Security Hub está activado en su. Cuentas de AWS
  - En AWS Organizations, ha designado una cuenta de administrador CSPM de Security Hub.
  - Tiene una función multicuenta AWS Identity and Access Management (IAM) que tiene `AWSOrganizationsReadOnlyAccess` permisos para acceder a la cuenta de administración. AWS Organizations
  - (Opcional) La has etiquetado con. Cuentas de AWS `SecurityContactID` Esta etiqueta se usa para asignar tickets de Jira a los contactos de seguridad definidos.
- Si desea implementar esta solución en una sola unidad Cuenta de AWS:
  - Usted tiene una Cuenta de AWS activa.
  - El CSPM de Security Hub está activado en su. Cuenta de AWS
- Una instancia del centro de datos de Jira

> **Important**
>
> Esta solución es compatible con el uso de Jira Cloud. Sin embargo, Jira Cloud no admite la importación de flujos de trabajo XML, por lo que deberá volver a crear el flujo de trabajo manualmente en Jira. Puede encontrar las transiciones y el estado en el GitHub repositorio.

- Permisos de administrador en Jira
- Uno de los siguientes tokens de Jira:
  - Para Jira Enterprise, un token de acceso personal (PAT). Para obtener más información, consulte Uso de tokens de acceso personal (soporte de Atlassian).
  - Para Jira Cloud, un token de la API de Jira. Para obtener más información, consulte Gestionar tokens de API (soporte de Atlassian).

Arquitectura

Esta sección ilustra la arquitectura de la solución en distintos escenarios, por ejemplo, cuando el desarrollador y el ingeniero de seguridad deciden aceptar el riesgo o deciden solucionar el problema.

Escenario 1: el desarrollador aborda el problema

1. Security Hub CSPM genera una conclusión contra un control de seguridad específico, como los del estándar AWS Foundational Security Best Practices.
2. Un CloudWatch evento de Amazon asociado al hallazgo y a la `CreateJIRA` acción inicia una AWS Lambda función.
3. La función de Lambda usa su archivo de configuración y el campo `GeneratorId` del resultado para evaluar el escalado del resultado.
4. La función Lambda determina que el hallazgo debe escalarse y obtiene la etiqueta de la `SecurityContactID` cuenta de administración AWS Organizations . AWS Esta ID está asociada al desarrollador y se usa como ID de asignación del ticket de Jira.
5. La función Lambda usa las credenciales almacenadas AWS Secrets Manager para crear un ticket en Jira. Jira notifica al desarrollador.
6. El desarrollador aborda el problema de seguridad subyacente en el resultado y, en Jira, cambia el estado del ticket a `TEST FIX`.
7. Security Hub CSPM actualiza el hallazgo a medida que `ARCHIVED` se genera un nuevo evento. Este evento hace que la función de Lambda cierre automáticamente el ticket de Jira.

Escenario 2: el desarrollador decide aceptar el riesgo

1. Security Hub CSPM genera una conclusión contra un control de seguridad específico, como los del estándar AWS Foundational Security Best Practices.
2. Un CloudWatch evento asociado al hallazgo y a la `CreateJIRA` acción inicia una función Lambda.
3. La función de Lambda usa su archivo de configuración y el campo `GeneratorId` del resultado para evaluar el escalado del resultado.
4. La función Lambda determina que el hallazgo debe escalarse y obtiene la etiqueta de la `SecurityContactID` cuenta de administración AWS Organizations . AWS Esta ID está asociada al desarrollador y se usa como ID de asignación del ticket de Jira.

5. La función de Lambda usa las credenciales almacenadas en AWS Secrets Manager para crear un ticket en Jira. Jira notifica al desarrollador.
6. El desarrollador decide aceptar el riesgo y, en Jira, cambia el estado del ticket a `AWAITING RISK ACCEPTANCE`.
7. El ingeniero de seguridad revisa la solicitud y considera que la justificación empresarial es adecuada. El ingeniero de seguridad cambia el estado del ticket de Jira a `ACCEPTED RISK`. El ticket de Jira se cierra.
8. Un evento CloudWatch diario inicia la función Lambda de actualización, que identifica los tickets de Jira cerrados y actualiza los hallazgos relacionados con el CSPM de Security Hub como. `SUPPRESSED`

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todas las regiones. Cuentas de AWS
- Amazon CloudWatch Events le ayuda a supervisar los eventos del sistema para sus AWS recursos mediante el uso de reglas para hacer coincidir los eventos y enrutarlos a funciones o transmisiones.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar múltiples cuentas Cuentas de AWS en una organización que usted crea y administra de forma centralizada.
- AWS Secrets Manager lo ayuda a reemplazar las credenciales codificadas en su código, incluidas contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- AWS Security Hub CSPMproporciona una visión completa del estado de su seguridad en AWS. También le ayuda a comparar su AWS entorno con los estándares y las mejores prácticas del sector de la seguridad.

Repositorio de código

El código de este patrón está disponible en GitHub el repositorio aws-securityhub-jira-software-integration. Incluye el código de muestra y el flujo de trabajo de Jira para esta solución.

Epics

Configure Jira

Tarea	Descripción	Habilidades requeridas
Importe el flujo de trabajo.	Como administrador de Jira, importe el archivo `issue-workflow.xml` a su instancia del centro de datos de Jira. Si utiliza Jira Cloud, debe crear el flujo de trabajo según los archivos `assets/jira-cloud-transitions.png` y `assets/jira-cloud-status.png` . Los archivos se encuentran en el repositorio aws-securityhub-jira-software-integration en. GitHub Para obtener más instrucciones, consulte Usar XML para crear un flujo de trabajo (documentación de Jira).	Administrador de Jira
Active y asigne el flujo de trabajo.	Los flujos de trabajo estarán inactivos hasta que los asigne a un esquema de flujo de trabajo. A continuación, asigne el esquema de flujo de trabajo a un proyecto.	Administrador de Jira

Tarea	Descripción	Habilidades requeridas
	1. En su proyecto, asegúrese de haber identificado un esquema de tipo de problema para el proyecto. Puede crear un nuevo tipo de problema o seleccionar uno existente, como Bug. 2. Asigne el flujo de trabajo importado a un esquema de flujo de trabajo siguiendo las instrucciones de Activar un flujo de trabajo (documentación de Jira). 3. Asigne el esquema de flujo de trabajo a un proyecto siguiendo las instrucciones de Asociar un esquema de flujo de trabajo a un proyecto (documentación de Jira).	

Configure los parámetros de la solución

Tarea	Descripción	Habilidades requeridas
Configure los parámetros de la solución.	1. En la carpeta conf, abra `params_prod.shfile` . 2. Proporcione valores para los siguientes parámetros: • `ORG_ACCOUNT_ID` — El ID de cuenta de tu cuenta AWS Organizations de administración. La	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	solución lee las etiquetas de las cuentas y asigna los tickets a los contactos de seguridad específicos definidos en esas Cuenta de AWS etiquetas. • `ORG_ROLE`— El nombre del rol de IAM utilizado para acceder a la cuenta de AWS Organizations administración. Este rol debe tener permisos de `OrganizationsReadOnlyAccess` . • `EXTERNAL_ID` – Un parámetro opcional si usa una ID externa para asumir el rol de IAM definido en `ORG_ROLE`. Para más información, consulte Cómo utilizar un ID externo (documentación de IAM). • `JIRA_DEFAULT_ASSIGNEE` : este es el ID de Jira a la que se asignan, de forma predeterminada, todos los problemas de seguridad. Esta asignación predeterminada se usa en caso de que la cuenta no esté etiquetada correctamente o no se pueda asumir el rol.	

Tarea	Descripción	Habilidades requeridas
	• `JIRA_INSTANCE` : la dirección HTTPS de su punto de conexión de Jira en el siguiente formato: `team-<team-id>.atlassian.net/` • `JIRA_PROJECT_KEY` – El nombre de la clave de proyecto de Jira empleada para crear los tickets, como `SEC` o `TEST`. Este proyecto ya debe existir en Jira. • `ISSUE_TYPE` – El nombre del esquema de tipo de problema asignado al proyecto en Jira, como `Bug` o `Security Issue`. • `REGIONS`— Lista de Región de AWS códigos en los que desea implementar esta solución, por ejemplo`eu-west-1` . 3. Guarde y cierre el archivo de parámetros de la solución.	

Tarea	Descripción	Habilidades requeridas
Identifique los resultados que desea automatizar.	1. Abra la consola CSPM de Security Hub. 2. En el panel de navegación del CSPM de Security Hub, elija Resultados. 3. Seleccione el título del resultado. 4. Seleccione el ID del resultado. Esto muestra el JSON completo del resultado. 5. En el JSON, copie la cadena del campo `GeneratorId` . Este valor está en formato de resultados de seguridad de AWS (ASFF). Por ejemplo, `aws-foundational-security-best-practices/v/1.0.0/S3.1` corresponde a los resultados del control de seguridad S3.1 S3 Block Public Access setting should be enabled. 6. Repita estos pasos hasta que haya copiado todos los valores `GeneratorID` de los resultados que desee automatizar.	

Tarea	Descripción	Habilidades requeridas
Agregue los resultados al archivo de configuración.	1. En src/code, abra el archivo `config.jsonconfig` . 2. Pegue los valores `GeneratorID` que recuperó anteriormente en el parámetro `default`, usando comas para separar cada ID. 3. Guarde y cierre el archivo de configuración. En el siguiente ejemplo de código se muestra la automatización de los resultados `aws-foundational-security-best-practices/v/1.0.0/SNS.1` y `aws-foundational-security-best-practices/v/1.0.0/S3.1` . `{ "Controls" : { "eu-west-1": [ "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.22" ], "default": [ aws-foundational-security-best-practices/v/1.0.0/SNS.1,`	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas

	<pre>aws-foundational-
	security-best-p
	ractices/v/1.0.0/S3.1
	]
	}
	}</pre>
	Note
	Puede optar por automatizar diferente s hallazgos para cada uno de ellos. Región de AWS Una práctica recomendada para evitar la duplicaci ón de resultados es seleccionar una sola región para automatiz ar la creación de controles relacionados con IAM.	

Implemente la integración

Tarea	Descripción	Habilidades requeridas
Implemente la integración.	En un terminal con línea de comandos, escriba el siguiente comando: <pre>./deploy.sh prod</pre>	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
Cargue las credenciales de Jira en Secrets Manager.	1. Abra la consola de Secrets Manager. 2. En Secrets (Secretos), elija Store a new secret (Almacenar un secreto nuevo). 3. En Secret type (Tipo de secreto), elija Other type of secret (Otro tipo de secreto). 4. Si usa Jira Enterprise, en los pares clave/valor, haga lo siguiente: • En la primera fila, introduzca `auth` en el cuadro de claves y, a continuación, introduzc a `token_auth` en el cuadro de valores. • Añada una segunda fila, introduzca `token` en el cuadro de claves y, a continuación, introduzc a su token de acceso personal en el cuadro de valores. Si usa la nube Jira Cloud, para los Pares de claves/va lores, haga lo siguiente: • En la primera fila, introduzca `auth` en el cuadro de claves y, a continuación, introduzc	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	a `basic_auth` en el cuadro de valores. • Añada una segunda fila, introduzca `token` en el cuadro de claves y, a continuación, introduzca su token de API en el cuadro de valores. • Añada una tercera fila, introduzca `email` en el cuadro de claves y, a continuación, escriba su dirección de correo electrónico en el cuadro de valores. 5. Elija Siguiente. 6. En Nombre del secreto, ingrese `Jira-Token` y, a continuación, en la parte inferior de la página, elija Siguiente. 7. En la página Secret rotation (Rotación del secreto), mantenga Disable automatic rotation (Desactivar rotación automática) y, a continuación, en la parte inferior de la página, elija Next (Siguiente). 8. En la página Review (Revisar), revise los detalles del secreto y,	

Tarea	Descripción	Habilidades requeridas
	luego, elija Store (Almacena r).	
Cree la acción personalizada CSPM de Security Hub.	1. Para cada uno de ellos Región de AWS, en AWS Command Line Interface (AWS CLI), utilice el create-action-targetcomando para crear una acción personalizada CSPM de Security Hub denominada. `CreateJiraIssue` `aws securityhub create-action-target --name "CreateJiraIssue" --description "Create ticket in JIRA" --id "CreateJiraIssue" --region $<aws-region>` 2. Abra la consola CSPM de Security Hub. 3. En el panel de navegación del CSPM de Security Hub, elija Resultados. 4. En la lista de resultados, seleccione aquellos que desee escalar. 5. En el menú Acciones, elija `CreateJiraIssue` .	Administrador de sistemas de AWS

Recursos relacionados

- AWS Conector de administración de servicios para Jira Service Management
- AWS Estándar fundamental de mejores prácticas de seguridad

Información adicional

Ejemplo de un ticket de Jira

Cuando se detecta un CSPM específico de Security Hub, esta solución crea automáticamente un ticket de Jira. El ticket contiene la información siguiente:

- Título: el título identifica el problema de seguridad en el siguiente formato:

```
AWS Security Issue :: <AWS account ID> :: <Security Hub finding title>
```

- Descripción: la sección de descripción del ticket describe el control de seguridad asociado al hallazgo, incluye un enlace al hallazgo en la consola CSPM de Security Hub y proporciona una breve descripción de cómo gestionar el problema de seguridad en el flujo de trabajo de Jira.

El siguiente es un ejemplo de ticket de Jira generado de manera automática.

Title	AWS Problema de seguridad:: 012345678 912:: Lambda.1 Las políticas de funciones de Lambda deberían prohibir el acceso público.
Descripción	¿Cuál es el problema? Hemos detectado un resultado de seguridad en la cuenta de Cuenta de AWS 012345678912 de la que es responsable. Este control comprueba si la política de AWS Lambda funciones adjunta al recurso de Lambda prohíbe el acceso público. Si la política de función de Lambda permite el acceso público, se produce un error en el control. <Link to Security Hub CSPM finding>

¿Qué debo hacer con el ticket?

- Acceda a la cuenta y verifique la configura ción. Confirme que está trabajando en el ticket moviéndolo a “Asignado para soluciona r”. Una vez solucionado el problema, páselo a la fase de solución de prueba para que el equipo de seguridad valide la resolución el problema.
- Si cree que se debe aceptar el riesgo, muévalo a “Esperando aceptación del riesgo”. Esto requerirá la revisión de un ingeniero de seguridad.
- Si cree que es un falso positivo, cámbielo a “Marcar como falso positivo”. Esto será revisado por un ingeniero de seguridad y reopened/closed en consecuencia.

Cree una canalización para imágenes de contenedores reforzadas con EC2 Image Builder y Terraform

Mike Saintcross y Andrew Ranes, Amazon Web Services

Resumen

Este patrón crea una canalización de EC2 Image Builder que produce una imagen de contenedor base de Amazon Linux 2 reforzada. Terraform es una herramienta de infraestructura como código (IaC) para configurar y aprovisionar la infraestructura que se usa para crear imágenes de contenedores reforzadas. Esta receta le ayuda a implementar una imagen de contenedor de Amazon Linux 2 basada en Docker y reforzada según Red Hat Enterprise Linux (RHEL) 7 STIG versión 3 lanzamiento 7 – Medium. (Consulte la STIG-Build-Linux-Medium versión 2022.2.1 en la sección de componentes de Linux STIG de la documentación de EC2 Image Builder). Esta imagen se conoce como imagen dorada de contenedor.

La versión incluye dos EventBridge reglas de Amazon. Una regla inicia el proceso de imágenes de contenedor cuando el resultado de Amazon Inspector es Alto o Crítico, con el fin de sustituir las imágenes no seguras. Esta regla requiere que se habilite el escaneo mejorado de Amazon Inspector y Amazon Elastic Container Registry (Amazon ECR). La otra regla envía las notificaciones a una cola de Amazon Simple Queue Service (Amazon SQS) tras una inserción correcta de las imágenes en el repositorio de Amazon ECR, con el fin de que use siempre las últimas imágenes del contenedor.

> **Note**
>
> Se acerca el fin de la compatibilidad de Amazon Linux 2. Para obtener más información, consulte Amazon Linux 2 FAQs.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS en la que pueda implementar la infraestructura.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada para configurar sus credenciales de AWS para la implementación local.
- Terraform descargado y configurado según las instrucciones de la documentación de Terraform.

- Git (si aprovisiona desde una máquina local).
- Un rol en la cuenta de AWS que pueda usar para crear recursos de AWS.
- Todas las variables definidas en el archivo .tfvars. También puede definir todas las variables al aplicar la configuración de Terraform.

Limitaciones

- Esta solución crea una infraestructura de Amazon Virtual Private Cloud (Amazon VPC) que incluye una puerta de enlace NAT y una puerta de enlace de Internet para la conectividad a Internet desde su subred privada. No puede usar puntos de enlace de VPC, ya que el proceso de arranque de AWS Task Orchestrator and Executor () AWSTOE instala la versión 2 de la CLI de AWS desde Internet.

Versiones de producto

- Amazon Linux 2
- Versión 1.1 o posterior de la CLI de AWS

Arquitectura

Pila de tecnología de destino

Este patrón crea 43 recursos, incluidos:

- Dos buckets de Amazon Simple Storage Service (Amazon S3): uno para los archivos de los componentes del proceso y otro para el acceso al servidor y los registros de flujo de Amazon VPC
- Un repositorio de Amazon ECR
- Una nube privada virtual (VPC) que contiene una subred pública, una subred privada, tablas de enrutamiento, una puerta de enlace NAT y una puerta de enlace de Internet
- Una canalización, una receta y componentes de EC2 Image Builder
- Una imagen de contenedor
- Una clave de AWS Key Management Service (AWS KMS) para el cifrado de imágenes
- Una cola de SQS
- Tres funciones: una para ejecutar la canalización de EC2 Image Builder, una para el perfil de instancia para EC2 Image Builder y otra para EventBridge las reglas

- Dos EventBridge reglas

Estructura del módulo Terraform

Para ver el código fuente, consulte el GitHub repositorio Terraform EC2 Image Builder Container Hardening Pipeline.

```
### components.tf
### config.tf
### dist-config.tf
### files
#   ###assumption-policy.json
### hardening-pipeline.tfvars
### image.tf
### infr-config.tf
### infra-network-config.tf
### kms-key.tf
### main.tf
### outputs.tf
### pipeline.tf
### recipes.tf
### roles.tf
### sec-groups.tf
### trigger-build.tf
### variables.tf
```

Detalles del módulo

- `components.tf` contiene un recurso de carga de Amazon S3 para cargar el contenido del directorio `/files`. También puede añadir aquí archivos YAML de componentes personalizados de forma modular.
- `/files` contiene los archivos `.yml` que definen los componentes usados en `components.tf`.
- `image.tf` contiene las definiciones del sistema operativo de la imagen base. Aquí es donde puede modificar las definiciones para crear un proceso de imagen base diferente.
- `infr-config.tf` y `dist-config.tf` contienen los recursos de la infraestructura de AWS mínima necesaria para crear y distribuir la imagen.
- `infra-network-config.tf` contiene la infraestructura de VPC mínima en la que implementar la imagen del contenedor.

- `hardening-pipeline.tfvars` contiene las variables de Terraform que se usarán en el momento de la aplicación.
- `pipeline.tf`crea y administra una canalización EC2 de Image Builder en Terraform.
- `recipes.tf` es donde puede especificar diferentes combinaciones de componentes para crear recetas de contenedores.
- `roles.tf`contiene las definiciones de la política de AWS Identity and Access Management (IAM) para el perfil de instancia y la función de implementación de canalización de Amazon Elastic Compute Cloud (Amazon EC2).
- `trigger-build.tf`contiene las EventBridge reglas y los recursos de colas de SQS.

Arquitectura de destino

El diagrama ilustra el flujo de trabajo siguiente:

1. EC2 Image Builder crea una imagen de contenedor mediante la receta definida, que instala las actualizaciones del sistema operativo y aplica el STIG de RHEL Medium a la imagen base de Amazon Linux 2.
2. La imagen reforzada se publica en un registro privado de Amazon ECR y una EventBridge regla envía un mensaje a una cola de SQS cuando la imagen se ha publicado correctamente.
3. Si Amazon Inspector está configurado para un escaneo mejorado, escanea el registro de Amazon ECR.
4. Si Amazon Inspector genera un resultado de gravedad crítica o alta para la imagen, una EventBridge regla activa la canalización de EC2 Image Builder para que se ejecute de nuevo y publique una imagen recién reforzada.

Automatizar y escalar

- Este patrón describe cómo aprovisionar la infraestructura y construir el proceso en su equipo. Sin embargo, está pensado para ser utilizado a escala. En lugar de implementar los módulos de Terraform de forma local, puede usarlos en un entorno multicuenta, como un entorno de AWS Control Tower con Account Factory para Terraform. En ese caso, deberá usar un bucket de S3 con estado de backend para administrar los archivos de estado de Terraform en lugar de gestionar el estado de configuración de forma local.

- Para un uso a gran escala, implemente la solución en una cuenta central, como una cuenta de Shared Services o Common Services, desde un modelo de cuenta de Control Tower o zona de aterrizaje, y conceda permiso a las cuentas de los consumidores para acceder al repositorio de Amazon ECR y a la clave de AWS KMS. Para obtener más información sobre la configuración, consulte el artículo de Re:post ¿Cómo puedo permitir que una cuenta secundaria inserte o extraiga imágenes de mi repositorio de imágenes de Amazon ECR? Por ejemplo, en una máquina expendedora de cuentas o en Account Factory para Terraform, añada permisos a cada línea base de cuenta o línea base de personalización de cuenta para proporcionar acceso a ese repositorio de Amazon ECR y a la clave de cifrado.
- Una vez desplegada la canalización de imágenes del contenedor, puede modificarla mediante las funciones de EC2 Image Builder, como los componentes, que le ayudan a empaquetar más componentes en la compilación de Docker.
- La clave de AWS KMS que se usa para cifrar la imagen del contenedor debe compartirse entre las cuentas en las que se va a usar la imagen.
- Puede añadir compatibilidad con otras imágenes duplicando todo el módulo Terraform y modificando los siguientes atributos `recipes.tf`:
  - Modifique `parent_image = "amazonlinux:latest"` a otro tipo de imagen.
  - Modifique `repository_name` para que apunte a un repositorio de Amazon ECR existente. Esto crea otro proceso que implementa un tipo de imagen principal diferente en su repositorio de Amazon ECR existente.

Tools (Herramientas)

Herramientas

- Terraform (aprovisionamiento de iAC)
- Git (si se aprovisiona localmente)
- CLI de AWS versión 1 o versión 2 (si se aprovisiona localmente)

Código

El código de este patrón se encuentra en el GitHub repositorio Terraform EC2 Image Builder Container Hardening Pipeline. Para usar el código de muestra, realice los pasos de la siguiente sección.

Epics

Aprovisione la infraestructura

Tarea	Descripción	Habilidades requeridas

Configure las credenciales locales.	Configure sus credenciales temporales de AWS.
	
	1. Compruebe si la CLI de AWS está instalada:
	
	`$ aws --version`
	`aws-cli/1.16.249`
	`Python/3.6.8...`
	
	• La versión de la CLI de AWS debe ser 1.1 o posterior.
	• Si no encuentra el comando, instale la CLI de AWS.
	2. Ejecute `aws configure` y proporcione los siguientes valores:
	
	`$ aws configure`
	`AWS Access Key ID`
	`[**********xxxx`
	`]: <Your AWS access`
	`key ID>`
	`AWS Secret Access Key`
	`[**********xxx`
	`x]: <Your AWS secret`
	`access key>`
	`Default region name:`
	`[us-east-1]: <Your`
	`desired Region for`
	`deployment>`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`Default output format [None]: <Your desired output format>`	

Clonar el repositorio.	1. Clonar el repositorio proporcionado con este patrón: Puede usar HTTPS o Secure Shell (SSH).
	
	HTTPS:
	
	`git clone https://github.com/aws-samples/terraform-ec2-image-builder-container-hardening-pipeline`
	
	SSH:
	
	`git clone git@github.com:aws-samples/terraform-ec2-image-builder-container-hardening-pipeline.git`
	2. Navegue hasta el directorio local que contiene esta solución:
	
	`cd terraform-ec2-image-builder-container-hardening-pipeline`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

Actualice variables.	Actualice las variables del archivo `hardening-pipeline.tfvars` para adecuarlas a su entorno y configuración. Debe proporcionar su `account_id`. También debe modificar el resto de las variables para adaptarlas a la implementación deseada. Todas las variables son obligatorias.
	
	`account_id = "<DEPLOYMENT-ACCOUNT-ID>"`
	`aws_region = "us-east-1"`
	`vpc_name = "example-hardening-pipeline-vpc"`
	`kms_key_alias = "image-builder-container-key"`
	`ec2_iam_role_name = "example-hardening-instance-role"`
	`hardening_pipeline_role_name = "example-hardening-pipeline-role"`
	`aws_s3_ami_resources_bucket = "example-hardening-ami-resources-bucket-0123"`
	`image_name = "example-hardening-al2-container-image"`
		AWS DevOps

Tarea	Descripción	Habilidades requeridas

	`ecr_name = "example-hardening-container-repo"`
	`recipe_version = "1.0.0"`
	`ebs_root_vol_size = 10`
	
	Aquí tiene una descripción de cada variable:
	
	• `account_id` – El número de cuenta de AWS en el que desea implementar la solución.
	• `aws_region` : la Región de AWS en la que desea implementar la solución.
	• `vpc_name` – El nombre de su infraestructura de VPC.
	• `kms_key_alias` – El nombre de la clave de AWS KMS que utilizará la configuración de la infraestructura de EC2 Image Builder.
	• `ec2_iam_role_name` – El nombre del rol que se utilizará como perfil de la EC2 instancia.
	• `hardening_pipeline_role_name` – El nombre del rol que se usará para implementar el proceso de refuerzo.	

Tarea	Descripción	Habilidades requeridas
	• `aws_s3_ami_resources_bucket` – El nombre del bucket de S3 que alojará todos los archivos necesarios para crear las imágenes del proceso y el contenedor. • `image_name` – El nombre de la imagen del contenedor. Este valor debe tener entre 3 y 50 caracteres, y solo puede contener caracteres alfanuméricos y guiones. • `ecr_name` – El nombre del registro de Amazon ECR en el que se almacenan las imágenes del contenedor. • `recipe_version` : la versión de la receta de la imagen. El valor predeterminado es 1.0.0. • `ebs_root_vol_size` – El tamaño (en gigabytes) del volumen raíz de Amazon Elastic Block Store (Amazon EBS). El valor predeterminado es 10 gigabytes.	

Tarea	Descripción	Habilidades requeridas
Inicialice Terraform.	Tras actualizar los valores de las variables, puede inicializar el directorio de configuración de Terraform. Al inicializar el directorio de configuración, se descarga e instala el proveedor de AWS definido en la configuración. `terraform init` Aparecerá un mensaje indicando que Terraform se ha inicializado correctamente e identificando la versión del proveedor instalada.	AWS DevOps
Implemente la infraestructura y cree una imagen de contenedor.	Use el siguiente comando para inicializar, validar y aplicar los módulos de Terraform al entorno mediante las variables definidas en su archivo `.tfvars`: `terraform init && terraform validate && terraform apply -var-file *.tfvars -auto-approve`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Personalice el contenedor.	Puede crear una nueva versión de una receta de contenedor después de que EC2 Image Builder haya implementado la canalización y la receta inicial. Puede añadir cualquiera de los más de 31 componentes disponibles en EC2 Image Builder para personalizar la construcción del contenedor. Para obtener más informaci ón, consulte la sección Componentes de Crear una nueva versión de una receta de contenedor en la documentación de EC2 Image Builder.	Administrador de AWS

Valide los recursos

Tarea	Descripción	Habilidades requeridas
Valide el aprovisionamiento de la infraestructura de AWS.	Una vez que haya completad o correctamente su primer comando `apply` de Terraform , si está aprovisionando localmente, debería ver este fragmento en la terminal de su máquina local:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`Apply complete! Resources: 43 added, 0 changed, 0 destroyed.`	
Valide los recursos individua les de la infraestructura de AWS.	Para validar los recursos individuales implementados, si aprovisiona de forma local, puede ejecutar el siguiente comando: `terraform state list` Este comando devuelve una lista de 43 recursos.	AWS DevOps

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Elimine la imagen de la infraestructura y el contenedo r.	Cuando haya terminado de trabajar con la configuración de Terraform, puede ejecutar el siguiente comando para eliminar los recursos: `terraform init && terraform validate && terraform destroy -var-file *.tfvars -auto-approve`	AWS DevOps

Resolución de problemas

Problema	Solución
Error al validar las credenciales del proveedor	Al ejecutar los comandos `apply` o `destroy` de Terraform desde su equipo local, es posible que se produzca un error similar al siguiente: `Error: configuring Terraform AWS Provider: error validating provider credentials: error calling sts:GetCallerIdentity: operation error STS: GetCallerIdentity, https response error StatusCode: 403, RequestID: 123456a9-fbc1-40ed-b8d8-513d0133ba7f, api error InvalidClientTokenId: The security token included in the request is invalid.` Este error se debe a la caducidad del token de seguridad de las credenciales usadas en la configuración de la máquina local. Para resolver el error, consulte Cómo establecer y ver ajustes de configuración en la documentación de la CLI de AWS.

Recursos relacionados

- Terraform EC2 Image Builder Container Hardening Pipeline (repositorio) GitHub
- EC2 Documentación de Image Builder
- Fábrica de cuentas de AWS Control Tower para Terraform (publicación del blog de AWS)
- Bucket de S3 de estado de backend (documentación de Terraform)
- Instalación o actualización de la versión más reciente de la CLI de AWS (documentación de la CLI de AWS)
- Descargar Terraform

Centralización de la administración de claves de acceso de IAM en AWS Organizations mediante Terraform

Pradip kumar Pandey y Pratap Kumar Nanda, Amazon Web Services

Resumen

Hacer cumplir las normas de seguridad para las claves y contraseñas es una tarea esencial para todas las organizaciones. Una regla importante es rotar las claves de AWS Identity and Access Management (IAM) a intervalos regulares para reforzar la seguridad. Por lo general, las claves de acceso de AWS se crean y configuran localmente cuando los equipos quieren acceder a AWS desde la interfaz de la línea de comandos de AWS (AWS CLI) o desde aplicaciones ajenas a AWS. Para mantener una seguridad sólida en toda la organización, las claves de seguridad antiguas deben cambiarse o eliminarse una vez que se haya cumplido el requisito o a intervalos regulares. El proceso de administrar la rotación de claves en varias cuentas de una organización lleva mucho tiempo y es tedioso. Este patrón lo ayudará a automatizar el proceso de rotación mediante Generador de cuentas para Terraform (AFT) y los servicios de AWS.

El patrón le ofrece las ventajas siguientes:

- Administra los ID de las claves de acceso y las claves de acceso secretas de todas las cuentas de la organización desde una ubicación central.
- Rota automáticamente las variables de entorno `AWS_ACCESS_KEY_ID` y `AWS_SECRET_ACCESS_KEY`.
- Exige la renovación de las credenciales de los usuarios si estas se ven comprometidas.

El patrón usa Terraform para implementar funciones de AWS Lambda, reglas de EventBridge Amazon y roles de IAM. Una EventBridge regla se ejecuta a intervalos regulares y llama a una función Lambda que enumera todas las claves de acceso de los usuarios en función del momento en que se crearon. Las funciones de Lambda adicionales crean un nuevo ID de clave de acceso y una clave de acceso secreta, si la clave antigua es anterior al período de rotación que se haya definido (por ejemplo, 45 días); a continuación, se notifica a un administrador de seguridad mediante Amazon Simple Notification Service (Amazon SNS) y Amazon Simple Email Service (Amazon SES). Los secretos se crean en AWS Secrets Manager para ese usuario, la clave de acceso secreta antigua se almacena en Secrets Manager y se configuran los permisos para acceder a la clave antigua. Para garantizar que la clave de acceso anterior ya no se utilice, se deshabilita después de un período de

inactividad (por ejemplo, 60 días; en nuestro ejemplo, serán 15 días después de rotar las claves). Tras un período de almacenamiento inactivo (en nuestro ejemplo, 90 días o 45 días después de rotar las claves), las claves de acceso antiguas se eliminan de AWS Secrets Manager. Para obtener información detallada sobre la arquitectura y el flujo de trabajo, consulte la sección Arquitectura.

Requisitos previos y limitaciones

- Una zona de aterrizaje para su organización creada mediante AWS Control Tower (versión 3.1 o posterior)
- Generador de cuentas para Terraform (AFT), configurado con tres cuentas:
  - La cuenta de administración de la organización administra toda la organización desde una ubicación central.
  - La cuenta de administración AFT aloja la canalización de Terraform e implementa la infraestructura en la cuenta de implementación.
  - La cuenta de implementación implementa esta solución completa y administra las claves de IAM desde una ubicación central.
- La versión 0.15.0 o posterior de Terraform para aprovisionar la infraestructura en la cuenta de implementación.
- Dirección de correo electrónico configurada en Amazon Simple Email Service (Amazon SES).
- (Recomendado) Para mejorar la seguridad, implemente esta solución en una subred privada (cuenta de implementación) dentro de una nube privada virtual (VPC). Puede proporcionar los detalles de la VPC y la subred al personalizar las variables (consulte Personalizar los parámetros de la canalización de código en la sección Epics).

Arquitectura

Repositorios de AFT

Este patrón utiliza el Generador de cuentas para Terraform (AFT) para crear todos los recursos de AWS necesarios y la canalización de código para implementar los recursos en una cuenta de implementación. La canalización de código se ejecuta en dos repositorios:

- La personalización global contiene el código de Terraform que se aplicará a todas las cuentas registradas en AFT.
- Las personalizaciones de la cuenta contienen el código de Terraform que se ejecutará en la cuenta de implementación.

Detalles del recurso

Los CodePipeline trabajos de AWS crean los siguientes recursos en la cuenta de implementación:

- EventBridge Regla de AWS y regla configurada
- Función de Lambda `account-inventory`
- Función de Lambda `IAM-access-key-rotation`
- Función de Lambda `Notification`
- Bucket de Amazon Simple Storage Service (Amazon S3) que contiene una plantilla de correo electrónico
- Política de IAM obligatoria

Arquitectura

En el siguiente diagrama se ilustra lo siguiente:

1. Una EventBridge regla llama a la función `account-inventory` Lambda cada 24 horas.
2. Esta función de Lambda `account-inventory` consulta a AWS Organizations para obtener una lista de todos los ID, nombres de cuenta y correos electrónicos de cuentas de AWS.
3. La función de Lambda `account-inventory` inicia una función de Lambda `IAM-access-key-auto-rotation` para cada cuenta de AWS y le pasa los metadatos para su procesamiento adicional.
4. La función de Lambda `IAM-access-key-auto-rotation` utiliza un rol de IAM asumido para acceder a la cuenta de AWS. El script de Lambda ejecuta una auditoría de todos los usuarios y sus claves de acceso de IAM en la cuenta.
5. El umbral de rotación de la clave de IAM (período de rotación) se configura como una variable de entorno cuando se implementa la función de Lambda `IAM-access-key-auto-rotation`. Si se modifica el período de rotación, la función de Lambda `IAM-access-key-auto-rotation` se vuelve a implementar con una variable de entorno actualizada. Puede configurar los parámetros para establecer el período de rotación, el período de inactividad de las claves antiguas y el búfer inactivo tras el cual se eliminarán las claves antiguas (consulte Personalización de los parámetros de la cadena de códigos en la sección Epics).
6. La función de Lambda `IAM-access-key-auto-rotation` valida la antigüedad de la clave de acceso en función de su configuración. Si la antigüedad de la clave de acceso de IAM no ha excedido el período de rotación definido, la función de Lambda no realiza ninguna otra acción.

7. Si la antigüedad de la clave de acceso de IAM ha superado el período de rotación que ha definido, la función de Lambda `IAM-access-key-auto-rotation` cree una clave nueva y rote la clave existente.
8. La función de Lambda guarda la clave anterior en Secrets Manager y limita los permisos al usuario cuyas claves de acceso no cumplan con los estándares de seguridad. La función de Lambda también crea una política basada en recursos que sólo permite a la entidad principal de IAM especificada acceder al secreto y recuperarlo.
9. La función de Lambda `IAM-access-key-rotation` llama a la función de Lambda `Notification`.
10. La función de Lambda `Notification` consulta el bucket de S3 en busca de una plantilla de correo electrónico y genera dinámicamente mensajes de correo electrónico con los metadatos de actividad relevantes.
11. La función de Lambda `Notification` solicita a Amazon SES que tome medidas adicionales.
12. Amazon SES envía un correo electrónico a la dirección de correo electrónico del propietario de la cuenta con la información pertinente.

Tools (Herramientas)

Servicios de AWS

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos. Este patrón requiere roles y permisos de IAM.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Secrets Manager le permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- Amazon Simple Email Service (Amazon SES) facilita poder enviar y recibir correos electrónicos a través de los dominios y direcciones de correo electrónico propios.

Otras herramientas

- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.

Repositorio de código

Las instrucciones y el código de este patrón están disponibles en el repositorio de rotación de claves de acceso de GitHub IAM. Puede implementar el código en la cuenta de implementación central de AWS Control Tower para administrar la rotación de claves desde una ubicación central.

Prácticas recomendadas

- Para más información de IAM, consulte Prácticas recomendadas de seguridad en la documentación de IAM.
- Para obtener información sobre la rotación de claves, consulte las pautas para actualizar las claves de acceso en la documentación de IAM.

Epics

Configuración de los archivos de origen

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	1. Clone el repositorio de rotación GitHub de claves de acceso de IAM: `$ git clone https://github.com/aws-samples/centralized-iam-key-management-aws-organizations-terraform.git` 2. Confirme que la copia local del repositorio contiene tres carpetas:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

	`$ cd Iam-Access-keys-Rotation`
	`$ ls`
	`org-account-customization`
	`global-account-customization`
	`account-customization`	

Configurar cuentas

Tarea	Descripción	Habilidades requeridas

Configure la cuenta de arranque.	Como parte del proceso de arranque de AFT, debe tener una carpeta llamada `aft-bootstrap` en su máquina local.
	1. Copie todos los archivos de Terraform manualmente de la carpeta GitHub org-account-customization local a su carpeta. `aft-bootstrap`
	2. Ejecute los comandos de Terraform para configurar el rol global entre cuentas en la cuenta de administración de AWS Control Tower:
	`$ cd aft-bootstrap`
	`$ terraform init`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`$ terraform apply –auto-approve`	

Configure las personalizaciones globales.	Como parte de la configuración de la carpeta AFT, debe tener una carpeta llamada `aft-global-customizations` en su máquina local.
	1. Copia manualmente todos los archivos de Terraform de tu carpeta local de GitHub personalización de cuentas globales a tu carpeta. `aft-global-customizations/terraform`
	2. Envía el código a AWS CodeCommit:
	`$ git add *`
	`$ git commit -m "message"`
	`$ git push`
		DevOps ingeniero

Tarea	Descripción	Habilidades requeridas

Configure las personalizaciones de cuentas.	Como parte de la configuración de la carpeta AFT, debe tener una carpeta llamada `aft-account-customizations` en su máquina local.
	1. Cree una carpeta con el número de cuenta vendida.
	2. Copia manualmente todos los archivos de Terraform de la carpeta de GitHub personalización de tu cuenta local a tu carpeta. `aft-account-customizations/<vended account>/terraform`
	3. Envía el código a AWS CodeCommit:
	`$ git add *`
	`$ git commit -m "message"`
	`$ git push`
		DevOps ingeniero

Personalización de los parámetros de la canalización del código

Tarea	Descripción	Habilidades requeridas
Personalice los parámetros de la canalización de códigos que no sean de Terraform para todas las cuentas.	Cree un archivo llamado `input.auto.tfvars` en la carpeta `aft-global-customizations/terraform/` y proporcione	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	los datos de entrada necesarios. Consulte el archivo del GitHub repositorio para ver los valores predeterminados.	

Tarea	Descripción	Habilidades requeridas
Personalice los parámetros de la canalización del código para la implementación de la cuenta.	Cree un archivo llamado `input.auto.tfvars` en la `aft-account-customizations/<AccountName>/terraform/` carpeta y envíe el código a AWS CodeCommit. Al enviar código a AWS, CodeCommit se inicia automáticamente la canalización del código. Especifique los valores de los parámetros en función de los requisitos de su organización, incluidos los siguientes (consulte el archivo del repositorio de Github para ver los valores predeterminados): • `s3_bucket_name` : un nombre de bucket exclusivo para la plantilla de correo electrónico. • `s3_bucket_prefix` : un nombre de carpeta en el bucket de S3. • `admin_email_address` : dirección de correo electrónico del administrador que debe recibir la notificación. • `org_list_account` : número de cuenta de la cuenta de administración.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• `rotation_period` : número de días después de los cuales una clave debe pasar de activa a inactiva. • `inactive_period` : número de días después de los cuales se deben desactivar las claves que han pasado la rotación. El valor de debe ser mayor que `rotation_period` . • `inactive_buffer` : período de gracia entre la rotación y la desactivación de una clave. • `recovery_grace_period` : período de gracia entre la desactivación y la eliminación de una clave. • `dry_run_flag` : establezca su valor en true si quiere enviar una notificación al administrador con fines de prueba, sin necesidad de rotar las claves. • `store_secrets_in_central_account` : establezca su valor en true si quiere almacenar el secreto en la cuenta de administración. Si la variable se establece en false (predeterminado), el	

Tarea	Descripción	Habilidades requeridas
	secreto se almacenará en la cuenta de miembro. • `credential_replication_region` : región de AWS en la que desea implementar la función de Lambda y los buckets de S3 para la plantilla de correo electrónico. • `run_lambda_in_vpc` : establezca su valor en true para ejecutar la función de Lambda en la VPC. • `vpc_id`: ID de la VPC de la cuenta de implementación, si quiere ejecutar la función de Lambda en la VPC. • `vpc_cidr`: rango CIDR de la cuenta de implementación. • `subnet_id` : ID de subred de la cuenta de implementación. • `create_smtp_endpoint` : establezca su valor en true si quiere habilitar el punto de conexión de correo electrónico.	

Validación de la rotación de claves

Tarea	Descripción	Habilidades requeridas
Valide la solución.	1. Desde la consola de administración de AWS, inicie sesión en la cuenta de implementación. 2. Abra la consola de IAM y compruebe si las credencia les de usuario (ID de clave de acceso y claves secretas) se rotan según lo especificado. 3. Tras rotar una clave de IAM, confirme lo siguiente: • El valor antiguo se guarda en AWS Secrets Manager. • El nombre del secreto tiene el formato `Account_<account ID>_User_<username>_AccessKey` . • El usuario que especific ó en el parámetro `admin_email_addres s` recibe una notificac ión por correo electróni co sobre la rotación de claves.	DevOps ingeniero

Ampliación de la solución

Tarea	Descripción	Habilidades requeridas
Personalice la fecha de notificación por correo electrónico.	Si desea enviar notificaciones por correo electrónico un día específico antes de deshabilitar la clave de acceso, puede actualizar la función de Lambda `IAM-access-key-auto-rotation` con esos cambios: 1. Defina una variable llamada `notify-period` . 2. Añada una condición `if` en `main.py` antes de desactivar la clave: `If (keyage>rotation-period-notify-period){ send_to_notifier(context, aws_account_id, account_name, resource_owner, resource_actions[resource_owner], dryrun, config.emailTemplateAudit) }`	DevOps ingeniero

Resolución de problemas

Problema	Solución
El trabajo de Lambda `account-inventory` devuelve un error con `AccessDenied` al enumerar las cuentas.	Si ve este problema, debe validar los permisos: 1. Inicia sesión en la cuenta recién vendida, abre la CloudWatch consola de Amazon y, a continuación, consulta el grupo `/aws/lambda/account-inventory-lambda` de CloudWatch registros. 2. En los CloudWatch registros más recientes, identifica el número de cuenta que está causando el problema de acceso denegado. 3. Inicie sesión en la cuenta de administración de AWS Control Tower y confirme que se creó el rol `allow-list-account`. 4. Si el rol no existe, vuelva a ejecutar el código de Terraform con el comando `terraform apply`. 5. Seleccione la pestaña Cuenta de confianza y compruebe que la misma cuenta es de confianza.

Recursos relacionados

- Prácticas recomendadas de Terraform (documentación de Terraform)
- Prácticas recomendadas de seguridad en IAM (documentación de IAM)
- Prácticas recomendadas para la rotación de claves (documentación de IAM)

Comprueba la versión de registro de acceso, HTTPS y TLS en una CloudFront distribución de Amazon

SaiJeevan Devireddy y Bijesh Bal, Amazon Web Services

Resumen

Este patrón comprueba una CloudFront distribución de Amazon para asegurarse de que utiliza HTTPS, utiliza la versión 1.2 o posterior de Transport Layer Security (TLS) y tiene habilitado el registro de acceso. CloudFront es un servicio ofrecido por Amazon Web Services (AWS) que acelera la distribución de su contenido web estático y dinámico, como .html, .css, .js y archivos de imagen, a sus usuarios. CloudFront entrega su contenido a través de una red mundial de centros de datos denominados ubicaciones perimetrales. Cuando un usuario solicita el contenido con el que estás publicando CloudFront, la solicitud se redirige a la ubicación perimetral que ofrezca la menor latencia (retraso de tiempo), de modo que el contenido se entregue con el mejor rendimiento posible.

Este patrón proporciona una función de AWS Lambda que se inicia cuando Amazon CloudWatch Events detecta la llamada a la CloudFront API CreateDistributionCreateDistributionWithTags, o. UpdateDistribution La lógica personalizada de la función Lambda evalúa todas CloudFront las distribuciones que se crearon o actualizaron en la cuenta de AWS. Envía una notificación de infracción mediante Amazon Simple Notification Service (Amazon SNS) si detecta las siguientes infracciones:

- Comprobaciones globales:
  - El certificado personalizado no usa TLS versión 1.2
  - El registro está deshabilitado para la distribución
- Comprobaciones de origen:
  - Origin no está configurado con TLS versión 1.2
  - La comunicación con Origin está permitida en un protocolo que no sea HTTPS
- Comprobaciones de comportamiento:
  - La comunicación de comportamiento predeterminada está permitida en un protocolo que no sea HTTPS
  - La comunicación por comportamiento personalizado está permitida en un protocolo que no sea HTTPS

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- La dirección de correo electrónico en la que desee recibir notificaciones de infracción

Limitaciones

- Este control de seguridad no comprueba las distribuciones de Cloudfront existentes, a menos que se haya realizado una actualización en la distribución.
- CloudFront se considera un servicio global y no está vinculado a una región de AWS específica. Sin embargo, el registro de las API de Amazon CloudWatch Logs y AWS Cloudtrail para los servicios globales se realiza en la región EE.UU. Este (Norte de Virginia) (`us-east-1`). Por lo tanto, esta forma de control de seguridad CloudFront debe implementarse y mantenerse en `us-east-1` ella. Esta implementación única monitorea todas las distribuciones para CloudFront. No implemente el control de seguridad en ninguna otra región de AWS. (La implementación en otras regiones provocará que no se inicien CloudWatch los eventos y la función Lambda, y no habrá notificaciones de SNS).
- Esta solución se ha sometido a pruebas exhaustivas con distribuciones de contenido CloudFront web. No cubre las distribuciones de streaming del protocolo de mensajería en tiempo real (RTMP).

Arquitectura

Pila de tecnología de destino

- Función de Lambda
- Tema de SNS
- EventBridge Regla de Amazon

Arquitectura de destino

Automatizar y escalar

- Si utiliza AWS Organizations, puede utilizar AWS Cloudformation StackSets para implementar la plantilla adjunta en varias cuentas que desee supervisar.

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormation: CloudFormation es un servicio que le ayuda a modelar y configurar los recursos de AWS mediante el uso de la infraestructura como código.
- Amazon EventBridge: EventBridge ofrece un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones de software como servicio (SaaS) y servicios de AWS, y dirige esos datos a objetivos como las funciones Lambda.
- AWS Lambda: Lambda admite la ejecución de código sin aprovisionar ni administrar servidores.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable que se puede utilizar para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.

Código

El código adjunto incluye:

- Un archivo .zip con el código de Lambda (index.py)
- Una CloudFormation plantilla (archivo.yml) que se ejecuta para implementar el código Lambda

Epics

Cargue el control de seguridad

Tarea	Descripción	Habilidades requeridas
Cree el bucket de S3 para el código de Lambda.	En la consola Amazon S3, cree un bucket de S3 con un nombre único que no contenga barras diagonale s iniciales. Un nombre de	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	bucket de S3 es globalmente único y todas las cuentas de AWS comparten el espacio de nombres. El bucket de S3 debe estar en la región en la que se planea implementar el código de Lambda.	
Cargue el código de Lambda en el bucket de S3.	Cargue el código de Lambda (archivo cloudfront_ssl_log _lambda.zip) que se proporcio na en la sección Adjuntos en el bucket de S3 que creó en el paso anterior.	Arquitecto de la nube

Implemente la plantilla CloudFormation

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla.	En la CloudFormation consola de AWS, en la misma región de AWS que el bucket de S3, implemente la CloudForm ation plantilla (cloudfront-ssl-lo gging.yml) que se proporciona en la sección de adjuntos.	Arquitecto de la nube
Especifique el nombre del bucket de S3.	En el parámetro de Bucket de S3, especifique el nombre del bucket de S3 que creó en la primera épica.	Arquitecto de la nube
Especifique el nombre de clave de Amazon S3 para el archivo Lambda.	Para el parámetro Clave de S3, especifique la ubicación en Amazon S3 del archivo .zip	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	de código de Lambda en su bucket de S3. No incluya barras diagonales iniciales (por ejemplo, puede escribir lambda.zip o controls/lambda.zip).	
Proporcione una dirección de correo electrónico para la notificación.	Para el parámetro Correo electrónico de notificación, proporcione una dirección de correo electrónico en la que le gustaría recibir las notificaciones de infracción.	Arquitecto de la nube
Defina el nivel de registro.	Para el parámetro Nivel de registro de Lambda, defina el nivel de registro de la función de Lambda. Elija uno de los valores siguientes: • INFO para recibir mensajes informativos detallados sobre el progreso de la aplicación. • ERROR para obtener información sobre los eventos de error que podrían seguir permitiendo que la aplicación siguiera ejecutándose. • ADVERTENCIA para obtener información sobre situaciones potencialmente peligrosas.	Arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la CloudFormation plantilla se haya implement ado correctamente, se creará un nuevo tema de SNS y se enviará un mensaje de suscripción a la dirección de correo electrónico que proporcionó. Debe confirmar esta suscripción de correo electrónico para recibir las notificaciones de infracciones.	Arquitecto de la nube

Recursos relacionados

- CloudFormation Información sobre AWS
- Creación de una pila en la CloudFormation consola de AWS (CloudFormation documentación)
- CloudFront registro (CloudFront documentación)
- Información sobre Amazon S3
- Información sobre AWS Lambda

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Elección de un flujo de autenticación de Amazon Cognito para aplicaciones empresariales

Michael Daehnert y Fabian Jahnke, Amazon Web Services

Resumen

Amazon Cognito ofrece autenticación, autorización y administración de usuarios para aplicaciones móviles y web. Ofrece características beneficiosas para la autenticación de identidades federadas. Para poner todo en marcha, los arquitectos técnicos deben decidir cómo quieren utilizar esas características.

Amazon Cognito admite varios flujos para las solicitudes de autenticación. Estos flujos definen la forma en que los usuarios pueden verificar su identidad. La decisión sobre qué flujo de autenticación utilizar depende de los requisitos específicos de la aplicación y puede resultar compleja. Este patrón le ayudará a decidir qué flujo de autenticación es el más adecuado para su aplicación empresarial. Asume que ya tiene conocimientos básicos de Amazon Cognito, OpenID Connect (OIDC) y la federación, y lo guiará a través de los detalles sobre los diferentes flujos de autenticación federada.

Esta solución está destinada a los responsables de la toma de decisiones técnicas. Le permitirá comprender los diferentes flujos de autenticación y le ayudará a adaptarlos a los requisitos de su aplicación. Los líderes técnicos deben recopilar la información necesaria para iniciar las integraciones de Amazon Cognito. Dado que las organizaciones empresariales se centran principalmente en la federación de SAML, este patrón incluye descripciones de los grupos de usuarios de Amazon Cognito con federación de SAML.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Roles de AWS Identity and Access Management (IAM) y permisos con acceso completo a Amazon Cognito
- (Opcional) Acceso a su proveedor de identidades (IdP), como Microsoft Entra ID, Active Directory Federation Service (AD FS) u Okta
- Un alto nivel de experiencia para su aplicación
- Conocimientos básicos de Amazon Cognito, OpenID Connect (OIDC) y federación

Limitaciones

- Este patrón se centra en los grupos de usuarios y proveedores de identidades de Amazon Cognito. Para obtener información sobre los grupos de identidades de Amazon Cognito, consulte la sección Información adicional.

Arquitectura

Utilice la siguiente tabla para elegir un flujo de autenticación. En esta sección se proporciona más información sobre cada flujo.

¿Necesita machine-to-machine autenticación?	¿Su aplicación se basa en la web y el frontend se representa en el servidor?	¿Su aplicación es de una sola página (SPA) o es una aplicación de frontend para dispositivos móviles?	¿Su aplicación requiere tokens de actualización para poder utilizar la característica Mantener la conexión?	¿El frontend ofrece un mecanismo de redireccionamiento basado en el navegador?	Flujo de Amazon Cognito recomendado
Sí	No	No	No	No	Flujo de credenciales del cliente
No	Sí	No	Sí	Sí	Flujo del código de autorización
No	No	Sí	Sí	Sí	Flujo del código de autorización con clave de prueba para el intercambio de códigos (PKCE)

No	No	No	No	No	Flujo de contraseñas del propietario del recurso*

* El flujo de contraseñas del propietario del recurso solo debe usarse si es absolutamente necesario. Para obtener más información, consulte la sección sobre el flujo de contraseñas del propietario del recurso en este patrón.

Flujo de credenciales del cliente

El flujo de credenciales de cliente es el más corto de los flujos de Amazon Cognito. Debe usarse si los sistemas o servicios se comunican entre sí sin la interacción del usuario. El sistema solicitante utiliza el ID y el secreto del cliente para recuperar un token de acceso. Como ambos sistemas funcionan sin la intervención del usuario, no se requiere ningún paso de consentimiento adicional.

En el siguiente diagrama se ilustra lo siguiente:

1. La aplicación 1 envía una solicitud de autenticación con el ID y el secreto del cliente al punto de conexión de Amazon Cognito y recupera un token de acceso.
2. La aplicación 1 usa este token de acceso en cada llamada posterior a la aplicación 2.
3. La aplicación 2 valida el token de acceso con Amazon Cognito.

Se debe usar este flujo:

- para las comunicaciones entre aplicaciones sin interacción con el usuario.

No se debe usar este flujo:

- para cualquier comunicación en la que sea posible la intervención del usuario.

Flujo del código de autorización

El flujo de códigos de autorización es para la autenticación clásica basada en la web. En este flujo, el backend gestiona todo el intercambio y el almacenamiento de los tokens. El cliente basado en

un navegador no ve los tokens reales. Esta solución se utiliza para aplicaciones escritas en marcos como .NET Core, Jakarta Faces o Jakarta Server Pages (JSP).

El flujo del código de autorización es un flujo basado en la redirección. El cliente debe ser capaz de interactuar con el navegador web o un cliente similar. El cliente se redirige a un servidor de autenticación y se autentica en este servidor. Si el cliente se autentica correctamente, se redirige de nuevo al servidor.

En el siguiente diagrama se ilustra lo siguiente:

1. El cliente envía una solicitud al servidor web.
2. El servidor web redirige al cliente a Amazon Cognito mediante un código de estado HTTP 302. El cliente sigue automáticamente esta redirección hasta el inicio de sesión del IdP configurado.
3. El IdP comprueba si hay una sesión de navegador existente en su lado. Si no existe ninguna, el usuario recibe una petición para autenticarse proporcionando su nombre de usuario y contraseña. El IdP responde con un token SAML a Amazon Cognito.
4. Amazon Cognito devuelve el éxito con un token web JSON (JWT); específicamente, un token de código. El servidor web llama a /oauth2/token para cambiar el token de código por un token de acceso. El servidor web envía el ID y el secreto de cliente a Amazon Cognito para su validación.
5. El token de acceso se utilizará en cada llamada posterior a otras aplicaciones.
6. Otras aplicaciones validarán el token de acceso con Amazon Cognito.

Se debe usar este flujo:

- si el usuario puede interactuar con el navegador web o el cliente. El código de la aplicación se ejecuta y representa en el servidor para garantizar que ningún secreto llegue al navegador.

No se debe usar este flujo:

- Para aplicaciones de una sola página (SPAs) o aplicaciones móviles, ya que se renderizan en el cliente y no deberían usar secretos del cliente.

Flujo de códigos de autorización con PKCE

El flujo de códigos de autorización con clave de prueba para el intercambio de códigos (PKCE) se debe utilizar en aplicaciones de una sola página y aplicaciones móviles. Es el sucesor del flujo

implícito y es más seguro porque utiliza PKCE. PKCE es una extensión de la concesión de códigos de autorización OAuth 2.0 para clientes públicos. Este tipo de autenticación evita que se canjeen códigos de autorización interceptados.

En el siguiente diagrama se ilustra lo siguiente:

1. La aplicación crea un verificador de código y un desafío de código. Se trata de valores únicos y bien definidos que se envían a Amazon Cognito para que pueda consultarlos en el futuro.
2. La aplicación llama al punto de conexión /oauth2/authorization de Amazon Cognito. A continuación, redirige automáticamente al usuario al inicio de sesión del IdP configurado.
3. El IdP comprueba si hay una sesión existente. Si no existe ninguna, el usuario recibe una petición para autenticarse proporcionando su nombre de usuario y contraseña. El IdP responde con un token SAML a Amazon Cognito.
4. Cuando Amazon Cognito devuelve el resultado correcto con un token de código, el servidor web llama a /oauth2/token para cambiar el token de código por un token de acceso.
5. El token de acceso se utilizará en cada llamada posterior a otras aplicaciones.
6. Las otras aplicaciones validarán el token de acceso con Amazon Cognito.

Se debe usar este flujo:

- Para SPAs nuestras aplicaciones móviles

No se debe usar este flujo:

- si el backend de la aplicación se encarga de la autenticación.

Flujo de contraseñas del propietario del recurso

El flujo de contraseñas del propietario del recurso está destinado a aplicaciones sin capacidades de redireccionamiento. Se compila mediante la creación de un formulario de inicio de sesión en su propia aplicación. El inicio de sesión se comprueba en Amazon Cognito mediante una llamada a la CLI o al SDK, en lugar de depender de los flujos de redireccionamiento. La federación no es posible en este flujo de autenticación porque esta requiere redireccionamientos basados en el navegador.

En el siguiente diagrama se ilustra lo siguiente:

1. El usuario introduce sus credenciales en un formulario de inicio de sesión que proporciona la aplicación.
2. La interfaz de línea de comandos de AWS (AWS CLI) realiza admin-initiated-authuna llamada a Amazon Cognito.

> **Note**
>
> Como alternativa, puede utilizar AWS SDKs en lugar de la CLI de AWS.

3. Amazon Cognito devuelve un token de acceso.
4. El token de acceso se utilizará en cada llamada posterior a otras aplicaciones.
5. Las otras aplicaciones validarán el token de acceso con Amazon Cognito.

Se debe usar este flujo:

- Al migrar los clientes existentes que utilizan una lógica de autenticación directa (como la autenticación de acceso básica o la autenticación de acceso implícita) a OAuth la conversión de las credenciales almacenadas en un token de acceso

No se debe usar este flujo:

- si desea utilizar identidades federadas.
- Si su aplicación admite redireccionamientos

Tools (Herramientas)

Servicios de AWS

- Amazon Cognito ofrece autenticación, autorización y administración de usuarios para aplicaciones móviles y web.

Otras herramientas

- El depurador del token web JSON (JWT) es una herramienta de validación de JWT basada en la web.

Epics

Evaluación de su aplicación

Tarea	Descripción	Habilidades requeridas
Defina los requisitos de autenticación.	Evalúe su aplicación de acuerdo con sus requisitos de autenticación específicos.	Desarrollador de aplicaciones, arquitecto de aplicaciones
Alinee los requisitos con los flujos de autenticación.	En la sección Arquitectura, utilice la tabla de decisiones y las explicaciones de cada flujo para elegir el flujo de autentica ción de Amazon Cognito.	Desarrollador de aplicaciones, AWS general, arquitecto de aplicaciones

Configuración de un grupo de usuarios de Amazon Cognito

Tarea	Descripción	Habilidades requeridas
Cree un grupo de usuarios.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon Cognito. 2. Cree un grupo de usuarios de Cognito. Para obtener instrucciones, consulte Grupos de usuarios de Amazon Cognito. 3. Actualice la configuración y los atributos del grupo de usuarios según sea necesario. Por ejemplo, establezca una política de contraseñas para el grupo de usuarios. No cree	AWS general

Tarea	Descripción	Habilidades requeridas
	clientes de aplicaciones todavía.	
(Opcional) Configure un proveedor de identidades.	1. Cree un proveedor de identidades de SAML en el grupo de usuarios de Amazon Cognito. Para obtener instrucciones, consulte Adición y administración de proveedores de identidades de SAML a un grupo de usuarios. 2. Configure su proveedor de identidades de SAML externo para que trabaje con la federación de los grupos de usuarios de Amazon Cognito. Para más información, consulte Configuración de un proveedor de identidades de SAML externo. Si utiliza AD FS, consulte Creación de una federación de AD FS para su aplicación web mediante grupos de usuarios de Amazon Cognito (entrada del blog de AWS).	AWS general, administrador de la federación

Tarea	Descripción	Habilidades requeridas
Cree un cliente de aplicación.	1. Cree un cliente de aplicación para el grupo de usuarios. Para obtener instrucciones, consulte Creación de un cliente de aplicación. Tenga en cuenta lo siguiente: • Cambie la configuración según sea necesario, como la caducidad de los tokens. • Si su flujo de autenticación no requiere un secreto de cliente, desactive la casilla Generar secreto de cliente. 2. Elija la configuración del cliente de aplicaciones para cambiar su integración a un inicio de sesión de grupo de usuarios (nombre de usuario y contraseña) o un inicio de sesión federado a través de un IdP basado en SAML. 3. Habilite su IdP definiendo URLs y definiendo OAuth flujos o ámbitos según sea necesario.	AWS general

Integración de la aplicación con Amazon Cognito

Tarea	Descripción	Habilidades requeridas
Intercambie detalles de la integración de Amazon Cognito.	En función del flujo de autenticación, comparta la información de Amazon Cognito con la aplicación, como el ID del grupo de usuarios y el ID del cliente de la aplicación.	Desarrollador de aplicaciones, AWS general
Implemente la autenticación de Amazon Cognito.	Esto depende del flujo de autenticación que elija, y del lenguaje de programación y de los marcos que utilice. Para ver algunos enlaces para empezar, consulte la sección Recursos relacionados.	Desarrollador de aplicaciones

Recursos relacionados

Documentación de AWS

- Flujo de autenticación de grupos de usuarios
- Verificación de un token web JSON
- Acceda a los servicios de AWS desde una aplicación ASP.NET Core mediante los grupos de identidades de Amazon Cognito
- Marcos y: SDKs
  - Autenticación de Amazon Amplify
  - Ejemplos de proveedores de identidad de Amazon Cognito (documentación de AWS SDK para Java 2.x)
  - Autenticación de usuarios con Amazon Cognito (documentación de AWS SDK para .NET)

Publicaciones del blog de AWS

- Uso de cookies por parte de Authorization @Edge: protege tu CloudFront contenido de Amazon para que no lo descarguen usuarios no autenticados
- Creación de una federación de AD FS para su aplicación web mediante grupos de usuarios de Amazon Cognito

Socios de implementación

- Socios de AWS para soluciones de autenticación

Información adicional

Preguntas frecuentes

¿Por qué está en desuso el flujo implícito?

Desde el lanzamiento del marco OAuth 2.1, el flujo implícito está marcado como obsoleto por motivos de seguridad. Como alternativa, use el flujo de códigos de autorización con PKCE que se describe en la sección Arquitectura.

¿Qué sucede si Amazon Cognito no ofrece alguna de las funciones que necesito?

Los socios de AWS ofrecen diferentes integraciones para las soluciones de autenticación y autorización. Para obtener más información, consulte Socios de AWS para soluciones de autenticación.

¿Qué pasa con los flujos del grupo de identidades de Amazon Cognito?

Los grupos de usuarios de Amazon Cognito y las identidades federadas se utilizan para la autenticación. Los grupos de identidades de Amazon Cognito se utilizan para autorizar el acceso a los recursos de AWS mediante la solicitud de credenciales de AWS temporales. En este patrón no se describe el intercambio de los tokens de ID y de acceso para los grupos de identidades. Para obtener más información, consulte Cuál es la diferencia entre los grupos de usuarios y los grupos de identidades de Amazon Cognito y Escenarios comunes de Amazon Cognito.

Pasos siguientes

Este patrón proporciona información general sobre los flujos de autenticación de Amazon Cognito. Como siguiente paso, es necesario elegir la implementación detallada del lenguaje de programación de la aplicación. Oferta SDKs y marcos de varios lenguajes, que puede usar con Amazon Cognito. Para obtener referencias útiles, consulte la sección Recursos relacionados.

Cree reglas AWS Config personalizadas mediante AWS CloudFormation Guard políticas

Andrew Lok, Nicole Brown, Kailash Havildar y Tanya Howell, Amazon Web Services

Resumen

AWS Configlas reglas le ayudan a evaluar sus AWS recursos y su estado de configuración objetivo. Hay dos tipos de AWS Config reglas: administradas y personalizadas. Puede crear reglas personalizadas con AWS Lambda funciones o con AWS CloudFormation Guard(GitHub), un policy-as-code idioma.

Las reglas creadas con Guard proporcionan un control más detallado que las reglas administradas y, por lo general, son más fáciles de configurar que las reglas de Lambda totalmente personalizadas. Este enfoque proporciona a los ingenieros y arquitectos la capacidad de crear reglas sin necesidad de conocer Python, Nodejs o Java, que son necesarios para implementar reglas personalizadas a través de Lambda.

Este patrón proporciona las plantillas, los ejemplos de código y los enfoques de implementación viables para ayudarle a adoptar reglas personalizadas con Guard. Al usar este patrón, un administrador puede usarlo AWS Config para crear reglas de cumplimiento personalizadas que tengan atributos de elementos de configuración. Por ejemplo, los desarrolladores pueden utilizar las políticas de Guard en relación con los elementos de AWS Config configuración para supervisar de forma continua el estado de los elementos desplegados AWS y no relacionados con AWS los recursos, detectar infracciones de las reglas e iniciar automáticamente las correcciones.

Objetivos

Después de leer este patrón, debería poder:

- Comprenda cómo el código de política de Guard interactúa con el AWS Config servicio.
- Implemente el escenario 1, que es una regla AWS Config personalizada que utiliza la sintaxis de Guard para validar el cumplimiento de los volúmenes cifrados. Esta regla verifica que la unidad esté en uso y que el tipo de unidad sea gp3.
- Implemente el escenario 2, que es una regla AWS Config personalizada que utiliza la sintaxis de Guard para validar el GuardDuty cumplimiento de Amazon. Esta regla verifica que las GuardDuty grabadoras tengan habilitadas las protecciones Amazon Simple Storage Service (Amazon S3) y Amazon Elastic Kubernetes Service (Amazon EKS).

Requisitos previos y limitaciones

Requisitos previos

- Una activa Cuenta de AWS
- AWS Config, configurado en su Cuenta de AWS

Limitaciones

- Las reglas personalizadas de Guard solo pueden consultar pares clave-valor en un registro JSON de un elemento de configuración de destino.

Arquitectura

La sintaxis de Guard se aplica a una AWS Config regla como una política personalizada. AWS Config captura el JSON jerárquico de cada uno de los recursos especificados. El JSON del elemento de AWS Config configuración contiene pares clave-valor. Estos atributos se utilizan en la sintaxis de Guard como variables que se asignan a su valor correspondiente.

La siguiente es una explicación de la sintaxis de Guard. Las variables del elemento de configuración JSON se utilizan y se anteponen con un carácter %.

```
# declare variable
let <variable name> = <'value'>

# create rule and assign condition and policy
    rule <rule name> when
        <CI json key> == <"CI json value"> {
            <top level CI json key>.<next level CI json key> == %<variable name>
        }
```

Escenario 1: volúmenes de Amazon EBS

El escenario 1 implementa una regla AWS Config personalizada que usa la sintaxis de Guard para validar el cumplimiento de los volúmenes cifrados. Esta regla verifica que la unidad esté en uso y que el tipo de unidad sea gp3.

El siguiente es un ejemplo de un elemento de AWS Config configuración para el escenario 1. Hay tres pares clave-valor en este elemento de configuración que se utilizan como variables en la

política de Guard: `volumestatusvolumeencryptionstatus`, y. `volumetype` Además, la clave `resourceType` se usa como filtro en la política de Guard.


```
{
  "version": "1.3",
  "accountId": "111111111111",
  "configurationItemCaptureTime": "2023-01-15T19:04:45.402Z",
  "configurationItemStatus": "ResourceDiscovered",
  "configurationStateId": "4444444444444",
  "configurationItemMD5Hash": "",
  "arn": "arn:aws:ec2:us-west-2:111111111111:volume/vol-222222222222",
  "resourceType": "AWS::EC2::Volume",
  "resourceId": "vol-222222222222",
  "awsRegion": "us-west-2",
  "availabilityZone": "us-west-2b",
  "resourceCreationTime": "2023-01-15T19:03:22.247Z",
  "tags": {},
  "relatedEvents": [],
  "relationships": [
    {
      "resourceType": "AWS::EC2::Instance",
      "resourceId": "i-33333333333333333",
      "relationshipName": "Is attached to Instance"
    }
  ],
  "configuration": {
    "attachments": [
      {
        "attachTime": "2023-01-15T19:03:22.000Z",
        "device": "/dev/xvda",
        "instanceId": "i-33333333333333333",
        "state": "attached",
        "volumeId": "vol-222222222222",
        "deleteOnTermination": true,
        "associatedResource": null,
        "instanceOwningService": null
      }
    ],
    "availabilityZone": "us-west-2b",
    "createTime": "2023-01-15T19:03:22.247Z",
    "encrypted": false,
    "kmsKeyId": null,
    "outpostArn": null,
```

```
    "size": 8,
    "snapshotId": "snap-55555555555555555",
    "state": "in-use",
    "volumeId": "vol-222222222222",
    "iops": 100,
    "tags": [],
    "volumeType": "gp2",
    "fastRestored": null,
    "multiAttachEnabled": false,
    "throughput": null,
    "sseType": null
  },
  "supplementaryConfiguration": {}
}
```

El siguiente es un ejemplo del uso de la sintaxis de Guard para definir las variables y las reglas en el escenario 1. En el siguiente ejemplo:

- Las tres primeras líneas definen las variables mediante el comando `let`. Se les asigna un nombre y un valor que se derivan de los atributos del elemento de configuración.
- El bloque de reglas `compliancecheck` añade una dependencia condicional "when" que busca un par de clave-valor `resourceType` que coincida con `AWS::EC2::Volume`. Si se encuentra una coincidencia, la regla pasa por el resto de los atributos de JSON y busca coincidencias en las tres condiciones siguientes: `state`, `encrypted` y `volumeType`.

```
let volumestatus = 'available'
let volumetype = 'gp3'
let volumeencryptionstatus = true

    rule compliancecheck when
        resourceType == "AWS::EC2::Volume" {
            configuration.state == %volumestatus
            configuration.encrypted == %volumeencryptionstatus
            configuration.volumeType == %volumetype
        }
```

Para ver la política personalizada completa de Guard que implementa esta regla personalizada, consulta awsconfig-guard-cft.yaml o awsconfig-guard-tf-ec2vol.json en el repositorio de código. GitHub Para ver el código de HashiCorp Terraform que implementa esta política personalizada en Guard, consulta .json en el repositorio de código. awsconfig-guard-tf-example

Escenario 2: cumplimiento GuardDuty

El escenario 2 implementa una regla AWS Config personalizada que usa la sintaxis de Guard para validar el GuardDuty cumplimiento de Amazon. Esta regla verifica que las GuardDuty grabadoras tengan habilitadas las protecciones Amazon S3 y Amazon EKS. También verifica que los GuardDuty resultados se publiquen cada 15 minutos. Este escenario podría implementarse en todos Cuentas de AWS y Regiones de AWS en una organización (en AWS Organizations).

El siguiente es un ejemplo de un elemento de AWS Config configuración para el escenario 2. Hay tres pares clave-valor en este elemento de configuración que se utilizan como variables en la política de Guard: `FindingPublishingFrequency`, `S3Logs` y `Kubernetes`. Además, la clave `resourceType` se usa como filtro en la política.

```
{
  "version": "1.3",
  "accountId": "111111111111",
  "configurationItemCaptureTime": "2023-11-27T13:34:28.888Z",
  "configurationItemStatus": "OK",
  "configurationStateId": "7777777777777",
  "configurationItemMD5Hash": "",
  "arn": "arn:aws:guardduty:us-
west-2:111111111111:detector/66666666666666666666666666666666",
  "resourceType": "AWS::GuardDuty::Detector",
  "resourceId": "66666666666666666666666666666666",
  "resourceName": "66666666666666666666666666666666",
  "awsRegion": "us-west-2",
  "availabilityZone": "Regional",
  "resourceCreationTime": "2020-02-17T02:48:04.511Z",
  "tags": {},
  "relatedEvents": [],
  "relationships": [],
  "configuration": {
    "Enable": true,
    "FindingPublishingFrequency": "FIFTEEN_MINUTES",
    "DataSources": {
      "S3Logs": {
        "Enable": true
      },
      "Kubernetes": {
        "AuditLogs": {
          "Enable": true
        }
```

```
      }
    },

    "Id": "66666666666666666666666666666666",
    "Tags": []
  },
  "supplementaryConfiguration": {
    "CreatedAt": "2020-02-17T02:48:04.511Z"
  }
}
```

El siguiente es un ejemplo del uso de la sintaxis de Guard para definir las variables y las reglas en el escenario 2. En el siguiente ejemplo:

- Las tres primeras líneas definen las variables mediante el comando `let`. Se les asigna un nombre y un valor que se derivan de los atributos del elemento de configuración.
- El bloque de reglas `compliancecheck` añade una dependencia condicional "when" que busca un par de clave-valor `resourceType` que coincida con `AWS::GuardDuty::Detector`. Si se encuentra una coincidencia, la regla pasa por el resto de los atributos de JSON y busca coincidencias en las tres condiciones siguientes: `S3Logs.Enable`, `Kubernetes.AuditLogs.Enable` y `FindingPublishingFrequency`.

```
let s3protection = true
let kubernetesprotection = true
let publishfrequency = 'FIFTEEN_MINUTES'

    rule compliancecheck when
        resourceType == "AWS::GuardDuty::Detector" {
            configuration.DataSources.S3Logs.Enable == %s3protection
            configuration.DataSources.Kubernetes.AuditLogs.Enable ==
 %kubernetesprotection
            configuration.FindingPublishingFrequency == %publishfrequency
        }
```

Para ver la política personalizada completa de Guard que implementa esta regla personalizada, consulta awsconfig-guard-cft-gd.yaml en el repositorio de GitHub código. Para ver el código de HashiCorp Terraform que implementa esta política personalizada en Guard, consulta awsconfig-guard-tf-gd.json en el repositorio de código.

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en Cuentas de AWS todas las regiones.
- AWS Configproporciona una vista detallada de sus recursos Cuenta de AWS y de cómo están configurados. Le ayuda a identificar cómo se relacionan los recursos entre sí y cómo han cambiado sus configuraciones a lo largo del tiempo.

Otras herramientas

- HashiCorp Terraform es una herramienta de infraestructura como código (IaC) que facilita usar el código para aprovisionar y administrar los recursos y la infraestructura en la nube.

Repositorio de código

El código de este patrón está disponible en el AWS CloudFormation Guard repositorio GitHub AWS Config with. Este repositorio de código contiene ejemplos de los dos escenarios descritos en este patrón.

Epics

Crear reglas AWS Config personalizadas

Tarea	Descripción	Habilidades requeridas
(Opcional) Seleccione pares clave-valor para la regla.	Complete estos pasos si va a definir una política de Guard personalizada. Si utiliza una de las políticas de ejemplo para el escenario 1 o 2, omita estos pasos. 1. Inicie sesión en la AWS Config consola Consola de administración de AWS y ábrala.	Administrador de AWS, ingeniero de seguridad

Tarea	Descripción	Habilidades requeridas
	2. En la página de navegación izquierda, seleccione Recursos. 3. En el inventario de recursos, elige el tipo de recurso para el que quieres crear una regla AWS Config personalizada. 4. Elija Ver detalles. 5. Seleccione Ver elemento de configuración (JSON). Esta sección se amplía para mostrar el elemento de configuración en formato JSON. 6. Identifique los pares clave-valor para los que desea crear una regla AWS Config personalizada.	
Cree la regla personalizada.	Utilice los pares clave-valor que identificó anteriormente o uno de los ejemplos de políticas de Guard proporcionados, siga las instrucciones de Creación de reglas de políticas AWS Config personalizadas para crear una regla personalizada.	Administrador de AWS, ingeniero de seguridad

Tarea	Descripción	Habilidades requeridas
Valide la regla personalizada.	Tome alguna de las siguiente s medidas para validar la regla personalizada de Guard: • Introduzca el siguiente comando en AWS Command Line Interface ()AWS CLI. `cfn-guard validate -r guard-s3.guard -d s3bucket-prod-pass.json` • Siga las instrucciones del modo Detective en Evaluación de sus recursos con AWS Config reglas para implementar la regla AWS Config. Confirme que la sintaxis de Guard coincide correctamente con los recursos correspondientes de la cuenta o el archivo de destino.	Administrador de AWS, ingeniero de seguridad

Resolución de problemas

Problema	Solución
Pon a prueba la política de guardia fuera de AWS Config	Las pruebas unitarias se pueden realizar en su dispositivo local o en un entorno de desarroll o integrado (IDE), como un AWS Cloud9 IDE. Para realizar las pruebas unitarias, haga lo siguiente:

Problema	Solución

	1. Instale la CLI de AWS CloudFormation Guard y sus dependencias.
	2. Guarde un ejemplo de CI con formato JSON en su estación de trabajo como archivo .json.
	3. Guarde la GuardDuty política en su estación de trabajo como un archivo.guard.
	4. En la CLI de Guard, introduzca el siguiente comando para validar el archivo JSON de muestra mediante la política de Guard.
	`cfn-guard validate \`
	`-r guard-s3.guard \`
	`-d s3bucket-prod-pass.json`

Depura una regla personalizada AWS Config	En su política de Guard, cambia el valor de `EnableDebugLogDelivery` a `true`. El valor predeterminado es `false`. Los mensajes de registro se almacenan en Amazon CloudWatch.

Recursos relacionados

AWS documentación

- Creación de reglas de políticas AWS Config personalizadas (AWS Config documentación)
- AWS CloudFormation Guard Reglas de redacción (documentación de Guard)

AWS publicaciones de blog y talleres

- Presentamos la AWS CloudFormation Guard versión 2.0 (AWS entrada de blog)

Otros recursos

- AWS CloudFormation Guard (GitHub)
- AWS CloudFormation Guard Documentación CLI (GitHub)

Cree un informe consolidado de los hallazgos de seguridad de Prowler a partir de múltiples Cuentas de AWS

Mike Virgilio, Jay Durga y Andrea Di Fabio, Amazon Web Services

Resumen

Prowler (GitHub) es una herramienta de línea de comandos de código abierto que puede ayudarle a evaluar, auditar y supervisar sus cuentas de Amazon Web Services (AWS) para comprobar si cumplen las mejores prácticas de seguridad. En este patrón, despliega Prowler de forma centralizada Cuenta de AWS en su organización, gestionada por Prowler y, a continuación AWS Organizations, utiliza Prowler para realizar una evaluación de seguridad de todas las cuentas de la organización.

Si bien existen muchos métodos para implementar y utilizar Prowler para realizar una evaluación, esta solución se ha diseñado para una implementación rápida, un análisis completo de todas las cuentas de la organización o de las cuentas objetivo definidas, y la elaboración de informes accesibles sobre los problemas de seguridad. En esta solución, cuando Prowler completa la evaluación de seguridad de todas las cuentas de la organización, consolida los resultados. También filtra cualquier mensaje de error esperado, como los errores relacionados con las restricciones que impiden a Prowler escanear los buckets de Amazon Simple Storage Service (Amazon S3) en las cuentas aprovisionadas a través de AWS Control Tower. Los resultados filtrados y consolidados se presentan en una plantilla de Microsoft Excel que se incluye con este patrón. Puede utilizar este informe para identificar posibles mejoras en los controles de seguridad de su organización.

Esta solución se diseñó teniendo en cuenta lo siguiente:

- Las AWS CloudFormation plantillas reducen el esfuerzo necesario para implementar los AWS recursos en este patrón.
- Puede ajustar los parámetros de las CloudFormation plantillas y del script prowler_scan.sh en el momento de la implementación para personalizar las plantillas para su entorno.
- Las velocidades de evaluación e informes de Prowler se optimizan mediante el procesamiento paralelo de los resultados agregados Cuentas de AWS, los informes consolidados con las soluciones recomendadas y las visualizaciones generadas automáticamente.
- El usuario no necesita monitorizar el progreso del escaneo. Cuando se completa la evaluación, se notifica al usuario a través de un tema de Amazon Simple Notification Service (Amazon SNS) para que pueda recuperar el informe.

- La plantilla de informe le ayuda a leer y evaluar solo los resultados relevantes para toda la organización.

Requisitos previos y limitaciones

Requisitos previos

- Y Cuenta de AWS para alojar servicios y herramientas de seguridad, gestionados como una cuenta de miembro de una organización en. AWS Organizations En este patrón, esta cuenta se denomina cuenta de seguridad.
- En la cuenta de seguridad, debe tener una subred privada con acceso saliente a Internet. Para obtener instrucciones, consulte VPC con servidores en subredes privadas y NAT en la documentación de Amazon Virtual Private Cloud (Amazon VPC). Puede establecer el acceso a Internet mediante una puerta de enlace NAT aprovisionada en una subred pública.
- Acceso a la cuenta AWS Organizations de administración o a una cuenta para la que se hayan delegado permisos de CloudFormation administrador. Para obtener instrucciones, consulte Registrar un administrador delegado en la CloudFormation documentación.
- Habilite el acceso confiable entre AWS Organizations y. CloudFormation Para obtener instrucciones, consulte Habilitar el acceso confiable con AWS Organizations en la CloudFormation documentación.

Limitaciones

- El objetivo Cuentas de AWS debe gestionarse como una organización en AWS Organizations. Si no la utiliza AWS Organizations, puede actualizar la CloudFormation plantilla IAM-ProwlerExecRole .yaml y el script prowler_scan.sh para su entorno. En su lugar, proporciona una lista de Cuenta de AWS IDs las regiones en las que desea ejecutar el script.
- La CloudFormation plantilla está diseñada para implementar la instancia de Amazon Elastic Compute Cloud (Amazon EC2) en una subred privada con acceso saliente a Internet. El AWS Systems Manager agente (agente SSM) requiere acceso saliente para llegar al punto final del AWS Systems Manager servicio, y usted necesita acceso saliente para clonar el repositorio de código e instalar las dependencias. Si quieres usar una subred pública, debes modificar la plantilla prowler-resources.yaml para asociar una dirección IP elástica a la instancia. EC2

Versiones de producto

- Prowler versión 4.0 o posterior

Arquitectura

El diagrama muestra el proceso siguiente:

1. Con el Administrador de sesiones, una función de AWS Systems Manager, el usuario se autentica en la EC2 instancia y ejecuta el script prowler_scan.sh. Este script del intérprete de comandos lleva a cabo los pasos del 2 al 8.
2. La EC2 instancia asume la función de `ProwlerEC2Role` IAM, que otorga permisos para acceder al bucket de S3 y para asumir las funciones de `ProwlerExecRole` IAM en las demás cuentas de la organización.
3. La EC2 instancia asume la función de `ProwlerExecRole` IAM en la cuenta de administración de la organización y genera una lista de las cuentas de la organización.
4. La EC2 instancia asume la función de `ProwlerExecRole` IAM en las cuentas de los miembros de la organización (denominadas cuentas de carga de trabajo en el diagrama de arquitectura) y realiza una evaluación de seguridad en cada cuenta. Los resultados se almacenan en archivos CSV y HTML en la EC2 instancia.

   > **Note**
   >
   > Los archivos HTML son el resultado de la evaluación de Prowler. Debido a la naturaleza del HTML, no se concatenan, procesan ni utilizan directamente en este patrón. Sin embargo, pueden resultar útiles para revisar los informes de cuentas individuales.

5. La EC2 instancia procesa todos los archivos CSV para eliminar los errores conocidos y esperados y consolida los hallazgos restantes en un solo archivo CSV.
6. La EC2 instancia empaqueta los resultados de las cuentas individuales y los resultados agregados en un archivo zip.
7. La EC2 instancia carga el archivo zip en el bucket de S3.
8. Una EventBridge regla detecta la carga del archivo y utiliza un tema de Amazon SNS para enviar un correo electrónico al usuario en el que se le notifica que la evaluación ha finalizado.
9. El usuario descarga el archivo zip del bucket de S3. El usuario importa los resultados a la plantilla de Excel y revisa los resultados.

Tools (Herramientas)

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática escalable en el Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, AWS Lambda funciones, puntos de enlace de invocación HTTP que utilizan destinos de API o buses de eventos en otros. Cuentas de AWS
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar múltiples cuentas Cuentas de AWS en una organización que usted crea y administra de forma centralizada.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Systems Manager lo ayuda a administrar las aplicaciones y la infraestructura que se ejecutan en la Nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo necesario para detectar y resolver problemas operativos y le ayuda a administrar sus AWS recursos de forma segura y a escala. Este patrón utiliza Session Manager, una capacidad de Systems Manager.

Otras herramientas

- Prowler es una herramienta de línea de comandos de código abierto que le ayuda a evaluar, auditar y supervisar sus cuentas para comprobar si cumplen las mejores prácticas de seguridad y otros marcos y AWS estándares de seguridad.

Repositorio de código

El código de este patrón está disponible en la evaluación de seguridad GitHub multicuenta del repositorio Prowler. El repositorio de código contiene los siguientes archivos:

- prowler_scan.sh: este script bash se utiliza para iniciar una evaluación de seguridad de Prowler de varios, Cuentas de AWS en paralelo. Como se define en Prowler-Resources.yaml CloudFormationtemplate, este script se implementa automáticamente en la carpeta de la instancia. `usr/local/prowler` EC2
- Prowler-Resources.yaml: usa esta plantilla para crear una pila en la cuenta de seguridad de la organización. CloudFormation Esta plantilla implementa todos los recursos necesarios para esta cuenta a fin de respaldar la solución. Esta pila debe implementarse antes que la plantilla IAM-.yaml. ProwlerExecRole No se recomienda implementar estos recursos en una cuenta que aloje cargas de trabajo de producción críticas.

> **Note**
>
> Si esta pila se elimina y se vuelve a implementar, debe volver a crear el conjunto de pilas `ProwlerExecRole` para recuperar las dependencias entre cuentas entre los roles de IAM.

- IAM- ProwlerExecRole .yaml: usa esta CloudFormation plantilla para crear un conjunto de pilas que despliegue la función de `ProwlerExecRole` IAM en todas las cuentas de la organización, incluida la cuenta de administración.
- prowler-report-template.xlsm: utilizas esta plantilla de Excel para procesar las conclusiones de Prowler. Las tablas dinámicas del informe proporcionan funciones de búsqueda, gráficos y resultados consolidados.

Epics

Preparación para la implementación

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código.	1. En una interfaz de la línea de comandos, cambie el directorio de trabajo a la ubicación en la que desee almacenar los archivos de muestra. 2. Introduzca el siguiente comando:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`git clone https://github.com/aws-samples/multi-account-security-assessment-via-prowler.git`	
Revise las plantillas.	1. En el repositorio clonado, abra los archivos Prowler-Resources.yaml e IAM- .yaml. ProwlerEx ecRole 2. Revise los recursos creados por estas plantillas y ajuste las plantillas según sea necesario para su entorno. Para obtener más información, consulta Cómo trabajar con plantillas en la documentación. CloudFormation 3. Guarde y cierre los archivos Prowler-Resources.yaml e IAM- .yaml. ProwlerEx ecRole	AWS DevOps

Crea las CloudFormation pilas

Tarea	Descripción	Habilidades requeridas
Aprovisione recursos en la cuenta de seguridad.	Con la plantilla prowler-resources.yaml, se crea una CloudFormation pila que despliega todos los recursos	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	necesarios en la cuenta de seguridad. Para obtener instrucciones, consulta Cómo crear una pila en la documentación. CloudFormation Tenga en cuenta lo siguiente al implementar esta plantilla: 1. En la página Especificar plantilla, seleccione Plantilla lista y, a continuación, cargue el archivo prowler-resources.yaml. 2. En la página Especificar detalles de pila, en Nombre de la pila, introduzca `Prowler-Resources` . 3. En la sección Parámetros, introduzca lo siguiente: • `VPCId`: seleccione una VPC en la cuenta. • `SubnetId`: seleccione una subred privada que tenga acceso a Internet. Nota: Si seleccionas una subred pública, a la EC2 instancia no se le asignará una dirección IP pública porque la CloudFormation plantilla, de forma predeterminada, no aprovisiona ni adjunta una dirección IP elástica.	

Tarea	Descripción	Habilidades requeridas

	• `InstanceType` : seleccione un tamaño de instancia en función del número de evaluaciones paralelas:
	  • Para 10, elija `r6i.large` .
	  • Para 12, elija `r6i.xlarge` .
	  • Para 14 a 18 años, elija `r6i.2xlarge` .
	• `InstanceImageId` : deje el valor predeterm inado para Amazon Linux.
	• `KeyPairName` : si utiliza SSH para acceder, especifique el nombre de un par de claves existente.
	• `PermittedSSHInboun d` : si utiliza SSH para el acceso, especifiq ue un bloque CIDR permitido. Si no utiliza SSH, mantenga el valor predeterminado de `127.0.0.1` .
	• `BucketName` : El valor predeterminado es `prowler-output- <accountID>- <region>` . Puede	

Tarea	Descripción	Habilidades requeridas
	modificarlo según sea necesario. Si especifica un valor personalizado, el ID de cuenta y la región se añaden automátic amente al valor especific ado. • `EmailAddress` : especifique una dirección de correo electrónico para una notificación de Amazon SNS cuando Prowler complete la evaluación y cargue el archivo .zip en el bucket de S3. Nota: La configuración de la suscripción a SNS debe confirmarse antes de que Prowler complete la evaluación o no se enviará ninguna notificac ión. • `IAMProwlerEC2Role` -: mantenga el nombre predeterminado a menos que sus convenciones de nomenclatura requieran un nombre diferente para este rol de IAM. • `IAMProwlerExecRole` — Mantenga el valor predeterminado a menos	

Tarea	Descripción	Habilidades requeridas
	que se utilice otro nombre al implementar el archivo ProwlerExecRoleIAM -.yaml. • `Parallelism` : especifique el número de evaluaciones paralelas que se van a realizar. Asegúrese de que el valor del parámetro `InstanceType` admite este número de evaluaciones paralelas. • `FindingOutput` : si desea excluir los resultados de los pases, seleccione `FailOnly`. Esto reduce significativamente el tamaño de la salida y se centra en las comprobaciones que podrían necesitar ser resueltas. Si desea incluir los resultados de las aprobaciones, seleccione `FailAndPass` . 4. En la página de revisión, seleccione Los siguientes recursos requieren capacidades: [AWS::IAM::Role] y, a continuación, elija Create Stack. 5. Una vez que la pila se haya creado correctamente, en	

Tarea	Descripción	Habilidades requeridas
	la CloudFormation consola, en la pestaña Outputs, copia el `ProwlerEC 2Role` Amazon Resource Name (ARN). Este ARN se utiliza más adelante al implementar el archivo IAM-ProwlerExecRole .yaml.	

Tarea	Descripción	Habilidades requeridas
Facilitar el rol de IAM en las cuentas de los miembros.	En la cuenta AWS Organizations de administración o en una cuenta con permisos de administrador delegados CloudFormation, utilice la plantilla ProwlerExecRoleIAM-.yaml para crear un conjunto de pilas. CloudFormation El conjunto de pilas implementa el rol de IAM de `ProwlerExecRole` para todas las cuentas de miembros de la organización. Para obtener instrucciones, consulta Cómo crear un conjunto de pilas con permisos administrados por el servicio en la documentación. CloudFormation Tenga en cuenta lo siguiente al implementar esta plantilla: 1. En Preparar plantilla, selecciona La plantilla está lista y, a continuación, carga el archivo ProwlerExecRoleIAM-.yaml. 2. En la página Especificar StackSet detalles, asigne un nombre al conjunto de pilas. `IAM-ProwlerExecRole` 3. En la sección Parámetros, introduzca lo siguiente:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• `AuthorizedARN` : introduzca el ARN de `ProwlerEC2Role` que copió al crear la pila de `Prowler-Resources` . • `ProwlerExecRoleNam e` : mantenga el valor predeterminado de `ProwlerExecRole` a menos que se haya utilizado otro nombre al implementar el archivo Prowler-Resources.yaml. 4. En Permisos, seleccione Permisos administrados por servicios. 5. En la página Cómo establecer opciones de implementación, en Destinos de implement ación, seleccione Implementación en organización y acepte todos los valores predeterm inados. Nota: Si quiere que las pilas se desplieguen en todas las cuentas de los miembros de forma simultánea, establece el número Máximo de cuentas simultáneas y la Tolerancia a errores en un valor alto, por ejemplo `100`.	

Tarea	Descripción	Habilidades requeridas
	6. En Regiones de despliegue, selecciona el Región de AWS lugar en el que se despliega la EC2 instancia de Prowler. Como los recursos de IAM son globales y no regionales, se implementa el rol de IAM en todas las regiones activas. 7. En la página de revisión, seleccione Acepto que AWS CloudFormation podría crear recursos de IAM con nombres personalizados y, a continuación, elija Crear. StackSet 8. Supervise la pestaña Instancias de pila (para ver el estado de las cuentas individuales) y la pestaña Operaciones (para ver el estado general) para determinar cuándo se ha completado la implementación.	

Tarea	Descripción	Habilidades requeridas
Facilite el rol de IAM en la cuenta de administración.	Con la plantilla ProwlerExecRoleIAM-.yaml, se crea una CloudFormation pila que implementa la función de `ProwlerExecRole` IAM en la cuenta de administración de la organización. El conjunto de pilas que creó anteriormente no implementa el rol de IAM en la cuenta de administración. Para obtener instrucciones, consulta Cómo crear una pila en la documentación. CloudFormation Tenga en cuenta lo siguiente al implementar esta plantilla: 1. En la página Especificar plantilla, elija La plantilla está lista y, a continuación, cargue el archivo ProwlerExecRoleIAM-.yaml. 2. En la página Especificar detalles de pila, en Nombre de la pila, introduzca `IAM-ProwlerExecRole` . 3. En la sección Parámetros, introduzca lo siguiente: • `AuthorizedARN` : introduzca el ARN de `ProwlerEC2Role` que copió al crear la pila de `Prowler-Resources` .	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• `ProwlerExecRoleNam e` : mantenga el valor predeterminado de `ProwlerExecRole` a menos que se haya utilizado otro nombre al implementar el archivo Prowler-Resources.yaml. 4. En la página de revisión, seleccione Los siguiente s recursos requieren capacidades: [AWS::IAM ::Role] y, a continuación, elija Create Stack.	

Realice la evaluación de seguridad de Prowler

Tarea	Descripción	Habilidades requeridas
Ejecute el escaneo.	1. Inicie sesión en la cuenta de seguridad de la organización. 2. Con el administrador de sesiones, conéctese a la EC2 instancia de Prowler que aprovisionó anteriorm ente. Para obtener instrucci ones, consulte Conexión a la instancia de Linux mediante Session Manager. Si no puede conectars e, consulte la sección de solución de problemas de este patrón.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	3. Navegue hasta `usr/local/prowler` , y luego abra el archivo prowler_scan.sh. 4. Revise y modifique los parámetros y variables ajustables de este script según sea necesario para su entorno. Para obtener más informaci ón sobre las opciones de personalización, consulte los comentarios al principio del script. Por ejemplo, en lugar de obtener una lista de todas las cuentas de los miembros de la organización a partir de la cuenta de administr ación, puede modificar el Cuenta de AWS IDs script para especificar qué cuentas desea escanear o puede hacer referencia a un archivo externo que contenga estos parámetros. Regiones de AWS 5. Guarde y cierre el archivo prowler_scan.sh. 6. Introduzca los comandos siguientes. Esto ejecuta el script prowler_scan.sh. `sudo -i`	

Tarea	Descripción	Habilidades requeridas

	`screen`
	`cd /usr/local/prowler`
	`./prowler_scan.sh`
	
	Tenga en cuenta lo siguiente:
	• El comando screen permite que el script continúe ejecutándose en caso de que se agote el tiempo de espera de la conexión o se pierda el acceso a la consola.
	• Cuando comience el escaneo, puede forzar la separación de la pantalla pulsando Ctrl +A D. La pantalla se separa y puede cerrar la conexión de la instancia y permitir que la evaluación continúe.
	• Para reanudar una sesión separada, conéctese a la instancia, introduzca `sudo -i` y, a continuación, introduzca `screen -r`.
	• Para supervisar el progreso de las evaluaciones de las cuentas individuales, puede navegar hasta el directori	

Tarea	Descripción	Habilidades requeridas
	o de `usr/local/prowler` e introducir el comando `tail -f output/stdout-<account-id>` . 7. Espera a que Prowler complete los escaneos en todas las cuentas. El script evalúa varias cuentas al mismo tiempo. Cuando se complete la evaluación en todas las cuentas, recibirá una notificación si especificó una dirección de correo electrónico al implementar el archivo Prowler-Resources.yaml.	

Tarea	Descripción	Habilidades requeridas
Recupera los resultados de Prowler.	1. Descargue el archivo `prowler-output-<assessDate>.zip` del bucket `prowler-output-<accountID>-<region>` . Para obtener instrucciones, consulte Descargar un objeto en la documentación de Amazon S3. 2. Elimine todos los objetos del bucket, incluido el archivo que ha descargado. Esta es una práctica recomendada para optimizar los costes y garantizar que se puede eliminar la `Prowler-Resources` CloudFormation pila en cualquier momento. Para obtener instrucciones, consulte Eliminar objetos en la documentación de Amazon S3.	AWS general
Detenga la EC2 instancia.	Para evitar la facturación mientras la instancia está inactiva, detiene la EC2 instancia que ejecuta Prowler. Para obtener instrucciones, consulte Detener e iniciar las instancias en la EC2 documentación de Amazon.	AWS DevOps

Creación de un informe de los resultados

Tarea	Descripción	Habilidades requeridas
Importe los resultados.	1. En Excel, abra el prowler-report-templatearchivo.xlsx y, a continuación, elija la hoja de trabajo CSV de Prowler. 2. Elimine todos los datos de la muestra, incluida la fila del encabezado. Si se le pregunta si desea eliminar la consulta asociada a los datos que se van a eliminar, elija No. La eliminación de la consulta puede afectar a la funcionalidad de las tablas dinámicas de la plantilla de Excel. 3. Extraiga el contenido del archivo .zip que ha descargado del bucket de S3. 4. En Excel, abra el archivo.txt. prowler-fullorgresults-accessdeniedfiltered Le recomendamos que utilice este archivo porque ya se han eliminado los errores más comunes y no procesables, como los `Access Denied` errores relacionados con los intentos de escaneo de recursos. AWS Control	AWS general

Tarea	Descripción	Habilidades requeridas
	Tower Si desea obtener los resultados sin filtrar, abra en su lugar el archivo prowler-fullorgresults.txt. 5. Seleccione la columna A. 6. Si usas Windows, escriba Ctrl+C, o si usa macOS, escriba Cmd+C. Esto copia todos los datos al portapapeles. 7. En la plantilla de informe de Excel, en la hoja de trabajo CSV de Prowler, seleccione la celda A1. 8. Si usas Windows, escriba Ctrl+V, o si usa macOS, escriba Cmd+V. De este modo, se pegan los resultados en el informe. 9. Confirme que estén seleccionadas todas las celdas que contienen los datos pegados. Si no es así, seleccione la columna A. 10. En la pestaña Datos, seleccione Texto a columnas. 11. En el panel, haga lo siguiente: • Para el paso 1, seleccione Delimitado.	

Tarea	Descripción	Habilidades requeridas
	• En el paso 2, para Delimitadores, elija punto y coma. En el panel Vista previa de datos, confirme que los datos se están separando en columnas. • Para el paso 3, elija Finalizar. 12. Confirme que los datos de texto estén delimitados en varias columnas. 13. Guarde el informe de Excel con un nuevo nombre. 14. Busque y elimine cualquier error `Access Denied` en los resultados. Para obtener instrucciones sobre cómo eliminarlos mediante programación, consulte Eliminar errores mediante programación en la sección Información adicional.	

Tarea	Descripción	Habilidades requeridas
Finalice el informe.	1. Elija la hoja de trabajo Resultados y, a continuación, seleccione la celda A17. Esta celda es el encabezado de la tabla dinámica. 2. En la cinta, en PivotTable Herramientas, elija Analizar y, a continuación, en Actualizar, elija Actualizar todo. Esto actualiza las tablas dinámicas con el nuevo conjunto de datos. 3. De forma predeterminada, Excel no muestra Cuenta de AWS los números correctamente. Para corregir el formato de los números, haga lo siguiente: • En la hoja de trabajo de Resultados, abra el menú contextual (haga clic con el botón derecho) de la columna A y, a continuación, elija Formatear celdas. • Elija Número y, en decimales, introduzca `0`. • Seleccione Aceptar. Nota: Si un Cuenta de AWS número comienza con uno o más ceros, Excel los elimina automáticamente.	AWS general

Tarea	Descripción	Habilidades requeridas
	Si ve un número de cuenta que tiene menos de 12 dígitos en el informe, los dígitos que faltan son ceros al principio del número. 4. (Opcional) Puede contraer los campos para facilitar la lectura de los resultados. Haga lo siguiente: • En la hoja de trabajo Resultados, si mueve el cursor a la línea entre las filas 18 y 19 (el espacio entre el encabezad o crítico y el primer hallazgo), el icono del cursor cambia a una pequeña flecha que apunta hacia abajo. • Haga clic para seleccion er todos los campos de búsqueda. • Abra el menú contextua l (haga clic con el botón derecho), busque Expandir/Contraer y, a continuación, elija Contraer. 5. Para obtener más informaci ón sobre la evaluació n, consulte las hojas de trabajo sobre los Resultados, la Gravedad	

Tarea	Descripción	Habilidades requeridas
	y la Aprobación de la evaluación.	

(Opcional) Actualizar Prowler o los recursos del repositorio de código

Tarea	Descripción	Habilidades requeridas

Actualice Prowler.	Si desea actualizar Prowler a la versión más reciente, haga lo siguiente:
	1. Conéctese a la EC2 instancia de Prowler mediante el Administrador de sesiones. Para obtener instrucciones, consulte Conexión a la instancia de Linux mediante Session Manager.
	2. Introduzca el siguiente comando.
	`sudo -i`
	`pip3 install --upgrade prowler`
		AWS general

Actualice el script prowler_scan.sh.	Si quiere actualizar el script prowler_scan.sh a la última versión del repositorio, haga lo siguiente: 1. Conéctese a la EC2 instancia de Prowler mediante el Administrador de sesiones. Para obtener	AWS general

Tarea	Descripción	Habilidades requeridas

	instrucciones, consulte Conexión a la instancia de Linux mediante Session Manager.
	2. Introduzca el siguiente comando.
	`sudo -i`
	3. Desplácese hasta el directorio de scripts de Prowler.
	`cd /usr/local/prowler`
	4. Introduzca el siguiente comando para guardar el script local de forma que pueda combinar los cambios personalizados en la versión más reciente.
	`git stash`
	5. Introduzca el siguiente comando para obtener la versión más reciente del script.
	`git pull`
	6. Introduzca el siguiente comando para combinar el script personalizado con la versión más reciente del script.	

Tarea	Descripción	Habilidades requeridas
	`git stash pop` **Note** Es posible que recibas advertencias relacionadas con cualquier archivo generado localmente que no esté en el GitHub repositorio, como la búsqueda de informes. Puede ignorarlos siempre que el archivo prowler_scan.sh muestre que los cambios guardados localmente se han vuelto a combinar.	

(Opcional) Limpieza

Tarea	Descripción	Habilidades requeridas
Elimine todos los recursos implementados.	Puede dejar los recursos implementados en las cuentas. Si cierra la EC2 instancia cuando no está en uso y mantiene el depósito de S3 vacío, se reducen los costes de mantenimiento	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	de los recursos para futuros escaneos. Si desea desaprovisionar todos los recursos, haga lo siguiente: 1. Elimine la pila `IAM-ProwlerExecRole` aprovisionada en la cuenta de administración. Para obtener instrucciones, consulte Eliminar una pila en la CloudFormation documentación. 2. Elimine el conjunto de pilas `IAM-ProwlerExecRole` aprovisionado en la cuenta de administración de la organización o en la cuenta de administrador delegado. Para obtener instrucciones, consulte Eliminar un conjunto de pilas en la CloudFormation documentación. 3. Elimine todos los objetos del bucket de S3 `prowler-output` . Para obtener instrucciones, consulte Eliminar objetos en la documentación de Amazon S3. 4. Elimine la pila `Prowler-Resources` aprovisionada	

Tarea	Descripción	Habilidades requeridas
	en la cuenta de seguridad . Para obtener instrucciones, consulte Eliminar una pila en la CloudFormation documentación.	

Resolución de problemas

Problema	Solución
No se puede conectar a la EC2 instancia mediante el administrador de sesiones.	El agente SSM debe poder comunicarse con el punto de conexión de Systems Manager. Haga lo siguiente: 1. Valide que la subred en la que se implement a la EC2 instancia tenga acceso a Internet. 2. Reinicia la EC2 instancia.
Al implementar el conjunto de pilas, la CloudFormation consola te solicitará que lo hagas. `Enable trusted access with AWS Organizations to use service-managed permissions`	Esto indica que no se ha habilitado el acceso de confianza entre AWS Organizations y CloudFormation. Se requiere acceso de confianza para implementar el conjunto de pilas gestionado por servicios. Seleccione el botón para activar el acceso de confianza. Para obtener más información, consulte Habilitar el acceso confiable en la CloudFormation documentación.

Recursos relacionados

AWS documentación

- Implementación de controles de seguridad en AWS (Guía AWS prescriptiva)

Otros recursos

- Merodeador () GitHub

Información adicional

Eliminar errores mediante programación

Si los resultados contienen errores de `Access Denied`, debe eliminarlos de los resultados. Por lo general, estos errores se deben a una influencia externa en los permisos que impiden que Prowler evalúe un recurso en particular. Por ejemplo, algunas comprobaciones fallan al revisar los depósitos de S3 aprovisionados a través de ellos. AWS Control Tower Puede extraer estos resultados mediante programación y guardar los resultados filtrados como un archivo nuevo.

Los siguientes comandos eliminan las filas que contienen una sola cadena de texto (un patrón) y, a continuación, envían los resultados a un archivo nuevo.

- Para Linux o macOS (Grep)

```
grep -v -i "Access Denied getting bucket" myoutput.csv > myoutput_modified.csv
```

- Para Windows () PowerShell

```
Select-String -Path myoutput.csv -Pattern 'Access Denied getting bucket' -NotMatch >
 myoutput_modified.csv
```

Los siguientes comandos eliminan las filas que coinciden con más de una cadena de texto y, a continuación, envían los resultados a un archivo nuevo.

- Para Linux o macOS (utiliza un tubo de escape entre las cadenas)

```
grep -v -i 'Access Denied getting bucket\|Access Denied Trying to Get' myoutput.csv >
 myoutput_modified.csv
```

- Para Windows (usa una coma entre las cadenas)

```
Select-String -Path myoutput.csv -Pattern 'Access Denied getting bucket', 'Access
 Denied Trying to Get' -NotMatch > myoutput_modified.csv
```

Ejemplos de informes

La siguiente imagen es un ejemplo de la hoja de trabajo sobre los resultados del informe sobre los resultados consolidados de Prowler.

La siguiente imagen es un ejemplo de la hoja de trabajo Pasar Fallar del informe sobre los resultados consolidados de Prowler. (De forma predeterminada, los resultados de las aprobaciones se excluyen de la salida).

La siguiente imagen es un ejemplo de la hoja de trabajo sobre la Gravedad del informe sobre los resultados consolidados de Prowler.

Implemente y gestione AWS Control Tower los controles mediante el uso AWS CDK y CloudFormation

Iker Reina Fuente e Ivan Girardi, Amazon Web Services

Resumen

Este patrón describe cómo usar, implementar AWS CloudFormation y AWS Cloud Development Kit (AWS CDK) administrar los AWS Control Tower controles preventivos, de detección y proactivos en forma de infraestructura como código (IaC). Un control (también conocido como barrera de protección) es una regla de alto nivel que proporciona un control continuo del entorno general. AWS Control Tower Por ejemplo, puede usar controles para exigir el registro Cuentas de AWS y, a continuación, configurar las notificaciones automáticas si se producen eventos específicos relacionados con la seguridad.

AWS Control Tower le ayuda a implementar controles preventivos, de detección y proactivos que rigen sus AWS recursos y supervisan el cumplimiento en varios de ellos. Cuentas de AWS Cada control aplica una única regla. En este patrón, debe utilizar la plantilla de IaC proporcionada para especificar qué controles desea implementar en su entorno.

AWS Control Tower los controles se aplican a toda una unidad organizativa (OU) y el control afecta a todos los Cuenta de AWS miembros de la OU. Por lo tanto, cuando los usuarios realicen cualquier acción en cualquier cuenta de su zona de aterrizaje, la acción queda sujeta a los controles que rigen la OU.

La implementación de AWS Control Tower controles ayuda a establecer una base de seguridad sólida para tu AWS landing zone. Al utilizar este patrón para desplegar los controles a lo largo CloudFormation y ancho de la IAC AWS CDK, puedes estandarizar los controles en tu landing zone y desplegarlos y gestionarlos de forma más eficiente. Esta solución usa cdk_nag para escanear la aplicación durante la implementación. AWS CDK Esta herramienta comprueba si la aplicación cumple con las mejores prácticas. AWS

Para implementar AWS Control Tower controles como iAC, también puedes usar HashiCorp Terraform en lugar de. AWS CDK Para obtener más información, consulte Implementar y administrar AWS Control Tower controles mediante Terraform.

Destinatarios previstos

Este patrón se recomienda para los usuarios que tienen experiencia con AWS Control Tower, CloudFormation AWS CDK, y AWS Organizations.

Requisitos previos y limitaciones

Requisitos previos

- Activa Cuentas de AWS gestionada como una organización en AWS Organizations y una AWS Control Tower landing zone. Para obtener instrucciones, consulte Primeros pasos en la AWS Control Tower documentación.
- AWS Command Line Interface (AWS CLI), instalado y configurado.
- Administrador de paquetes de nodos (npm), instalado y configurado para AWS CDK.
- Requisitos previos para. AWS CDK
- Permisos para asumir un rol existente AWS Identity and Access Management (IAM) en una cuenta de implementación.
- Permisos para asumir una función de IAM en la cuenta de administración de la organización que se pueden utilizar para arrancar. AWS CDK El rol debe tener permisos para modificar e implementar CloudFormation los recursos. Para obtener más información, consulte Bootstrapping en la documentación. AWS CDK
- Permisos para crear roles y políticas de IAM en la cuenta de administración de la organización. Para obtener más información, consulte Permisos necesarios para acceder a los recursos de IAM en la documentación de IAM.

Limitaciones

- Este patrón proporciona instrucciones para implementar esta solución en todas las cuentas Cuentas de AWS, desde una cuenta de implementación hasta la cuenta de administración de la organización. Para realizar pruebas, puede implementar esta solución directamente en la cuenta de administración, pero las instrucciones para esta configuración no se proporcionan de forma explícita.
- En el caso de AWS Control Tower los controles, este patrón requiere el uso de identificadores globales con el siguiente formato:

```
arn:<PARTITION>:controlcatalog:::control/<CONTROL_CATALOG_OPAQUE_ID>
```

Las versiones anteriores de este patrón utilizaban identificadores regionales que ya no son compatibles. Se recomienda que migre de los identificadores regionales a los globales. Los identificadores globales lo ayudan a administrar los controles y a ampliar la cantidad de controles que puede usar.

> **Note**
>
> En la mayoría de los casos, el valor de `<PARTITION>` es `aws`.

Versiones de producto

- AWS Control Tower versión 3.2 o posterior
- Python, versión 3.9 o posterior
- npm versión 8.9.0 o posterior

Arquitectura

En esta sección se ofrece información general sobre esta solución y la arquitectura establecida en el código de ejemplo. El siguiente diagrama muestra los controles implementados en las distintas cuentas de la OU.

AWS Control Tower los controles se clasifican según su comportamiento y su orientación.

Existen tres tipos principales de comportamientos de control:

1. Los controles preventivos están diseñados para evitar que se produzcan acciones. Se implementan con las políticas de control de servicios (SCPs) o las políticas de control de recursos (RCPs) en AWS Organizations. El estado de una medida de seguridad preventiva es uno de los siguientes: aplicado o no habilitado. Los controles preventivos están respaldados en todos Regiones de AWS.
2. Los controles de detección están diseñados para detectar eventos específicos cuando se producen y registrar la acción en AWS CloudTrail. Se implementan con reglas de AWS Config. El estado de una medida de seguridad de detección es uno de los siguientes: limpio, infracción o no habilitado. Los controles de Detective se aplican solo a los Regiones de AWS compatibles con AWS Control Tower.

3. Los controles proactivos analizan los recursos que aprovisionaría AWS CloudFormation y comprueban si cumplen con las políticas y los objetivos de su empresa. Los recursos que no sean conformes no se aprovisionarán. Estos se implementan con enlaces de AWS CloudFormation. El estado de un control proactivo es PASS, FAIL o SKIP.

La guía de control se refiere a la práctica recomendada sobre cómo aplicar cada control a su OUs caso. AWS Control Tower proporciona tres categorías de orientación: obligatoria, muy recomendable y optativa. La directriz de un control es independiente de su comportamiento. Para obtener más información, consulte Directrices y comportamiento de control.

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir y aprovisionar la Nube de AWS infraestructura en código. El AWS CDK kit de herramientas es la herramienta principal para interactuar con la AWS CDK aplicación.
- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todo el mundo Cuentas de AWS . Regiones de AWS
- AWS Configproporciona una vista detallada de sus recursos Cuenta de AWS y de cómo están configurados. Le ayuda a identificar cómo se relacionan los recursos entre sí y cómo han cambiado sus configuraciones a lo largo del tiempo.
- AWS Control Towerle ayuda a configurar y administrar un entorno de AWS múltiples cuentas, siguiendo las prácticas recomendadas prescriptivas.
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar varias cuentas Cuentas de AWS en una organización que puede crear y administrar de forma centralizada.

Otras herramientas

- cdk_nag es una herramienta de código abierto que utiliza una combinación de paquetes de reglas para comprobar si AWS CDK las solicitudes cumplen las mejores prácticas.
- npm es un registro de software que se ejecuta en un entorno Node.js y se utiliza para compartir o tomar prestados paquetes y administrar la implementación de paquetes privados.
- Python es un lenguaje de programación informático de uso general.

Repositorio de código

El código de este patrón está disponible en el repositorio Deploy controls using. GitHub AWS Control TowerAWS CDK Se usa el archivo cdk.json para interactuar con la AWS CDK aplicación y se usa el archivo package.json para instalar los paquetes npm.

Prácticas recomendadas

- Siga el principio del privilegio mínimo (documentación de IAM). Los ejemplos de política de IAM y política de confianza que se proporcionan en este patrón incluyen los permisos mínimos necesarios, y las AWS CDK pilas creadas en la cuenta de gestión están restringidas por estos permisos.
- Siga las prácticas recomendadas para AWS Control Tower los administradores (AWS Control Tower documentación).
- Siga las prácticas recomendadas para desarrollar e implementar una infraestructura de nube con la AWS CDK (AWS CDK documentación).
- Al iniciarlo AWS CDK, personalice la plantilla de arranque para definir las políticas y las cuentas de confianza que deberían poder leer y escribir en cualquier recurso de la cuenta de administración. Para obtener más información, consulte Personalización del proceso de arranque.
- Utilice herramientas de análisis de código, como cfn_nag, para escanear las plantillas generadas. CloudFormation La herramienta cfn-nag busca patrones en las CloudFormation plantillas que puedan indicar que la infraestructura no es segura. También puedes usar cdk-nag para comprobar tus CloudFormation plantillas mediante el módulo cloudformation-include.

Epics

Preparación para habilitar los controles

Tarea	Descripción	Habilidades requeridas
Crear el rol de IAM en la cuenta de administración.	1. Cree una política de IAM en la cuenta de administración con los permisos definidos en la Política de IAM, en la sección Información adicional. Para obtener	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas

	más información, consulte Creación de políticas de IAM en la documentación de IAM. Tome nota del nombre de recurso de Amazon (ARN) de la política. A continuación se muestra un ejemplo de ARN.
	
	`arn:aws:iam::<MANAGEMENT-ACCOUNT-ID>:policy/<POLICY-NAME>`
	
	2. Cree un rol de IAM en la cuenta de administración, adjunte la política de permisos de IAM que ha creado en el paso anterior y adjunte la política de confianza personalizada de la Política de confianza en la sección Información adicional. Para obtener instrucciones, consulte Creación de un rol mediante políticas de confianza personalizadas en la documentación de IAM. A continuación se muestra un ejemplo de ARN para el nuevo rol.
	
	`arn:aws:iam::<MANAGEMENT-ACCOUN`	

Tarea	Descripción	Habilidades requeridas
	`T-ID>:role/<ROLE-NAME>`	

Tarea	Descripción	Habilidades requeridas
Bootstrap. AWS CDK	1. En la cuenta de administración, asuma un rol que tenga permisos para AWS CDK arrancar. 2. Introduzca el siguiente comando, reemplazando lo siguiente: • `<MANAGEMENT-ACCOUNT-ID>` es el ID de la cuenta de administración de la organización. • `<AWS-CONTROL-TOWER-REGION>` es el Región de AWS lugar donde AWS Control Tower se despliega . Para obtener la lista completa de códigos de región, consulte Puntos de conexión regionales en la Referencia general de AWS . • `<DEPLOYMENT-ACCOUNT-ID>` es el ID de la cuenta de implementación. • `<DEPLOYMENT-ROLE-NAME>` es el nombre del rol de IAM que está utilizando en la cuenta de implementación. • `<POLICY-NAME>` es el nombre de la política que	DevOps ingeniero, AWS general, Python

Tarea	Descripción	Habilidades requeridas
	ha creado en la cuenta de administración. `$ npx cdk bootstrap aws://<MANAGEMENT-ACCOUNT-ID>/<AWS-CONTROL-TOWER-REGION> \ --trust arn:aws:iam::<DEPLOYMENT-ACCOUNT-ID>:role/<DEPLOYMENT-ROLE-NAME> \ --cloudformation-execution-policies arn:aws:iam::<MANAGEMENT-ACCOUNT-ID>:policy/<POLICY-NAME>`	
Clonar el repositorio.	En un intérprete de comandos de bash, ingrese el siguiente comando. Esto clona los AWS Control Tower controles de Deploy utilizando el AWS CDK repositorio de GitHub. `git clone https://github.com/aws-samples/aws-control-tower-controls-cdk.git`	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas
Edite el archivo AWS CDK de configuración.	1. En el repositorio clonado, abra el archivo constants.py. 2. En el parámetro `ACCOUNT_ID`, introduzca el ID de su cuenta de administración. 3. En el `<AWS-CONTROL-TOWER-REGION>` parámetro, introduzca el Región de AWS lugar donde AWS Control Tower se despliega. 4. En el parámetro `ROLE_ARN`, introduzca el ARN del rol que ha creado en la cuenta de administración. 5. Abra todos los identificadores globales de la AWS Control Tower documentación. 6. En la lista con formato JSON, busque el control que desee implementar y, a continuación, copie su identificador global (también conocido como valor {CONTROL_CATALOG_OPAQUE_ID}). Por ejemplo, el identificador global del control AWS-GR_AUDIT_BUCKET_ENCRYPTION_ENABL	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas
	ED es `k4izcjxhu kijhajp6ks5mjxk` . 7. En la sección `GUARDRAILS_CONFIGURATION` , en el parámetro `Enable-Control` , introduzca el identificador global que ha copiado. Introduzca el identificador entre comillas dobles y separe los diversos identificadores con comas. 8. En la sección `GUARDRAILS_CONFIGURATION` , en el parámetro `OrganizationalUnitIds` , introduzca el ID de la unidad organizativa en la que quiere habilitar el control, por ejemplo `ou-1111-11111111` . Introduzca el ID entre comillas dobles y separe los números múltiples IDs con comas. Para obtener más información sobre cómo recuperar una unidad organizativa IDs, consulte Visualización de los detalles de una unidad organizativa. 9. Guarde y cierre el archivo constants.py. Para ver un ejemplo de un archivo constants.py actualiza	

Tarea	Descripción	Habilidades requeridas
	do, consulte la sección Información adicional de este patrón.	

Página de administración de cuentas en la consola de

Tarea	Descripción	Habilidades requeridas
Asumir el rol de IAM en la cuenta de implementación.	En la cuenta de implement ación, asuma la función de IAM que tiene permisos para implementar las AWS CDK pilas en la cuenta de administración. Para obtener más información sobre cómo asumir una función de IAM en la AWS CLI, consulte Usar una función de IAM en la. AWS CLI	DevOps ingeniero, AWS general
Activar el entorno.	Si utiliza Linux o MacOS: 1. Especifique el siguiente comando para crear un entorno virtual. `$ python3 -m venv .venv` 2. Una vez creado el entorno virtual, introduzca el siguiente comando para activarlo.	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas

	`$ source .venv/bin/activate`
	
	Si utiliza Windows:
	
	1. Especifique el siguiente comando para activar un entorno virtual.
	
	`% .venv\Scripts\activate.bat`	

Instalar las dependencias.	Una vez activado el entorno virtual, introduzca el siguiente comando para ejecutar el script install_deps.sh. Este script instala las dependencias requeridas. `$ ./scripts/install_deps.sh`	DevOps ingeniero, AWS general, Python

Implemente la pila.	Introduzca los siguientes comandos para sintetizar e implementar la CloudFormation pila.
	
	`$ npx cdk synth`
	`$ npx cdk deploy`
		DevOps ingeniero, AWS general, Python

Recursos relacionados

AWS documentación

- Acerca de los controles (AWS Control Tower documentación)
- Biblioteca de controles (AWS Control Tower documentación)
- AWS CDK Comandos del kit de herramientas (AWS CDK documentación)
- Implemente y gestione AWS Control Tower los controles mediante Terraform (guíaAWS prescriptiva)

Otros recursos

- Python

Información adicional

Ejemplo de archivo constants.py

El siguiente es un ejemplo de un archivo constants.py. Este ejemplo habilita el control AWS-GR_DISALLOW_CROSS_REGION_NETWORKING (ID global: `dvuaav61i5cnfazfelmvn9m6k`) y el control AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED (ID global: `50z1ot237wl8u1lv5ufau6qqo`). Para obtener una lista de los identificadores globales IDs, consulte Todos los identificadores globales en la documentación. AWS Control Tower

```
ACCOUNT_ID = 111122223333
AWS_CONTROL_TOWER_REGION = us-east-2
ROLE_ARN = "arn:aws:iam::111122223333:role/CT-Controls-Role"
GUARDRAILS_CONFIGURATION = [
    {
        "Enable-Control": {
            "dvuaav61i5cnfazfelmvn9m6k": {  # AWS-GR_DISALLOW_CROSS_REGION_NETWORKING
                "Parameters": {
                    "ExemptedPrincipalArns": ["arn:aws:iam::111122223333:role/
RoleName"]
                },
                "Tags": [{"key": "Environment", "value": "Production"}]
            },
            ...
        },
        "OrganizationalUnitIds": ["ou-1111-11111111", "ou-2222-22222222"...],
    },
    {
        "Enable-Control": {
```

```
            "50z1ot237wl8u1lv5ufau6qqo",  # AWS-
GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED
            ...
        },
        "OrganizationalUnitIds": ["ou-2222-22222222"...],
    },
]
```

Política de IAM

El siguiente ejemplo de política permite realizar las acciones mínimas necesarias para habilitar o deshabilitar AWS Control Tower los controles al implementar AWS CDK pilas desde una cuenta de implementación a la cuenta de administración.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:EnableControl",
                "controltower:DisableControl",
                "controltower:GetControlOperation",
                "controltower:ListEnabledControls",
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DetachPolicy",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:UpdatePolicy",
                "ssm:GetParameters"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Política de confianza

La siguiente política de confianza personalizada permite que un rol de IAM específico en la cuenta de implementación asuma el rol de IAM en la cuenta de administración. Sustituya lo siguiente:

- <DEPLOYMENT-ACCOUNT-ID> es el ID de la cuenta de implementación
- <DEPLOYMENT-ROLE-NAME> es el nombre del rol en la cuenta de implementación que tiene permitido asumir el rol en la cuenta de administración

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<DEPLOYMENT-ACCOUNT-ID>:role/<DEPLOYMENT-ROLE-
NAME>"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

Implemente y gestione AWS Control Tower controles mediante Terraform

Iker Reina Fuente e Ivan Girardi, Amazon Web Services

Resumen

Este patrón describe cómo usar AWS Control Tower los controles, HashiCorp Terraform y la infraestructura como código (IaC) para implementar y administrar controles de seguridad preventivos, de detección y proactivos. Un control (también conocido como barrera de protección) es una regla de alto nivel que proporciona un control continuo del entorno general. AWS Control Tower Por ejemplo, puede usar controles para exigir el registro Cuentas de AWS y, a continuación, configurar las notificaciones automáticas si se producen eventos específicos relacionados con la seguridad.

AWS Control Tower le ayuda a implementar controles preventivos, de detección y proactivos que rigen sus AWS recursos y supervisan el cumplimiento en varios de ellos. Cuentas de AWS Cada control aplica una única regla. En este patrón, debe utilizar la plantilla de IaC proporcionada para especificar qué controles desea implementar en su entorno.

AWS Control Tower los controles se aplican a toda una unidad organizativa (OU) y el control afecta a todos los Cuenta de AWS miembros de la OU. Por lo tanto, cuando los usuarios realicen cualquier acción en cualquier cuenta de su zona de aterrizaje, la acción queda sujeta a los controles que rigen la OU.

La implementación de AWS Control Tower controles ayuda a establecer una base de seguridad sólida para tu AWS landing zone. Al usar este patrón para implementar los controles como IaC a través de Terraform, puede estandarizar los controles en su zona de aterrizaje e implementarlos y administrarlos de manera más eficiente.

Para implementar AWS Control Tower controles como iAC, también puedes usarlos AWS Cloud Development Kit (AWS CDK) en lugar de Terraform. Para obtener más información, consulte Implementar y administrar AWS Control Tower controles mediante AWS CDK y. AWS CloudFormation

Destinatarios previstos

Este patrón se recomienda para los usuarios que tengan experiencia con AWS Control Tower Terraform y AWS Organizations.

Requisitos previos y limitaciones

Requisitos previos

- Activa Cuentas de AWS gestionada como una organización en AWS Organizations y una AWS Control Tower landing zone. Para obtener instrucciones, consulte Primeros pasos en la AWS Control Tower documentación.
- AWS Command Line Interface (AWS CLI), instalado y configurado.
- Un rol AWS Identity and Access Management (IAM) en la cuenta de administración que tiene permisos para implementar este patrón. Para obtener más información sobre los permisos necesarios y un ejemplo de política, consulte Permisos con privilegios mínimos para el rol de IAM en la sección de Información adicional de este patrón.
- Permisos para asumir el rol de IAM en la cuenta de administración.
- Terraform CLI, instalada (documentación de Terraform).
- Terraform AWS Provider, configurado (documentación de Terraform).
- Backend de Terraform, configurado (documentación de Terraform).

Limitaciones

- Para AWS Control Tower los controles, este patrón requiere el uso de identificadores globales con el siguiente formato:

```
arn:<PARTITION>:controlcatalog:::control/<CONTROL_CATALOG_OPAQUE_ID>
```

  Las versiones anteriores de este patrón utilizaban identificadores regionales que ya no son compatibles. Se recomienda que migre de los identificadores regionales a los globales. Los identificadores globales lo ayudan a administrar los controles y a ampliar la cantidad de controles que puede usar.

> **Note**
>
> En la mayoría de los casos, el valor de `<PARTITION>` es `aws`.

Versiones de producto

- AWS Control Tower versión 3.2 o posterior
- Terraform versión 1.5 o posterior
- Terraform AWS Provider versión 4.67 o posterior

Arquitectura

En esta sección se ofrece información general sobre esta solución y la arquitectura establecida en el código de ejemplo. El siguiente diagrama muestra los controles implementados en las distintas cuentas de la OU.

AWS Control Tower los controles se clasifican según su comportamiento y su orientación.

Existen tres tipos principales de comportamientos de control:

1. Los controles preventivos están diseñados para evitar que se produzcan acciones. Se implementan con las políticas de control de servicios (SCPs) o las políticas de control de recursos (RCPs) en AWS Organizations. El estado de una medida de seguridad preventiva es uno de los siguientes: aplicado o no habilitado. Los controles preventivos están respaldados en todos Regiones de AWS.
2. Los controles de detección están diseñados para detectar eventos específicos cuando se producen y registrar la acción en AWS CloudTrail. Se implementan con reglas de AWS Config. El estado de una medida de seguridad de detección es uno de los siguientes: limpio, infraccióno no habilitado. Los controles de Detective se aplican solo a los Regiones de AWS compatibles con AWS Control Tower.
3. Los controles proactivos analizan los recursos que aprovisionaría AWS CloudFormation y comprueban si cumplen con las políticas y los objetivos de su empresa. Los recursos que no sean conformes no se aprovisionarán. Estos se implementan con enlaces de AWS CloudFormation. El estado de un control proactivo es PASS, FAIL o SKIP.

La guía de control es la práctica recomendada sobre cómo aplicar cada control a su OUs cuerpo. AWS Control Tower proporciona tres categorías de orientación: obligatoria, muy recomendable y optativa. La directriz de un control es independiente de su comportamiento. Para obtener más información, consulte Directrices y comportamiento de control.

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y administrarlos a lo largo de su ciclo de vida en todas Cuentas de AWS las regiones.
- AWS Configproporciona una vista detallada de sus recursos Cuenta de AWS y de cómo están configurados. Le ayuda a identificar cómo se relacionan los recursos entre sí y cómo han cambiado sus configuraciones a lo largo del tiempo.
- AWS Control Towerle ayuda a configurar y administrar un entorno de AWS múltiples cuentas, siguiendo las prácticas recomendadas prescriptivas.
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar varias cuentas Cuentas de AWS en una organización que puede crear y administrar de forma centralizada.

Otras herramientas

- HashiCorp Terraform es una herramienta de infraestructura como código (IaC) que facilita usar el código para aprovisionar y administrar los recursos y la infraestructura en la nube.

Repositorio de código

El código de este patrón está disponible en el repositorio de Terraform para GitHub implementar y administrar AWS Control Tower controles.

Prácticas recomendadas

- Los roles de IAM usados para implementar esta solución deben cumplir con el principio de privilegio mínimo (documentación de IAM).
- Siga las mejores prácticas para AWS Control Tower administradores (AWS Control Tower documentación).

Epics

Página de administración de cuentas en la consola de

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	En un intérprete de comandos de bash, ingrese el siguiente comando. Esto clona los AWS Control Tower controles de implementación y administración mediante el repositorio Terraform de GitHub. `git clone https://github.com/aws-samples/aws-control-tower-controls-terraform.git`	DevOps ingeniero
Edite el archivo de configuración del backend de Terraform.	1. En el repositorio clonado, abra el archivo backend.tf. 2. Edite el archivo para establecer la configuración del backend de Terraform. La configuración que defina en este archivo depende de su entorno. Para obtener más información, consulte la sección Configuración del backend (documentación de Terraform). 3. Guarde y cierre el archivo backend.tf.	DevOps ingeniero, Terraform

Tarea	Descripción	Habilidades requeridas
Edite el archivo de configuración del proveedor de Terraform.	1. En el repositorio clonado, abra el archivo provider.tf. 2. Edite el archivo para establecer la configuración del proveedor de Terraform. Para obtener más información, consulte Configuración del proveedor (documentación de Terraform). Establece Región de AWS la región en la que está disponible la AWS Control Tower API. 3. Guarde y cierre el archivo provider.tf.	DevOps ingeniero, Terraform

Tarea	Descripción	Habilidades requeridas
Edite el archivo de configuración.	1. En el repositorio clonado, abra el archivo variables.tfvars. 2. Abra todos los identificadores globales de la AWS Control Tower documentación. 3. En la lista con formato JSON, busque el control que desee implementar y, a continuación, copie su identificador global (también conocido como valor {CONTROL_CATALOG_OPAQUE_ID}). Por ejemplo, el identificador global del control AWS-GR_AUDIT_BUCKET_ENCRYPTION_ENABLED es `k4izcjxhu kijhajp6ks5mjxk` . 4. En la sección `controls`, en el parámetro `control_names` , introduzca el identificador global que ha copiado. 5. En la sección `controls`, en el parámetro `organizational_unit_ids` , introduzca el ID de la unidad organizativa en la que quiere habilitar el control, por ejemplo `ou-1111-11111111` .	DevOps ingeniero, AWS general, Terraform

Tarea	Descripción	Habilidades requeridas
	Introduzca el ID entre comillas dobles y separe los números múltiples IDs con comas. Para obtener más información sobre cómo recuperar una unidad organizativa IDs, consulte Visualización de los detalles de una unidad organizativa. 6. Guarde y cierre el archivo variables.tfvars. Para ver un ejemplo de un archivo variables.tfvars actualizado, consulte la sección de información adicional de este patrón.	
Asuma el rol de IAM de la cuenta de administración	En la cuenta de administración, asuma el rol de IAM que tiene permisos para implementar el archivo de configuración de Terraform. Para obtener más información sobre los permisos necesarios y un ejemplo de política, consulte Permisos con privilegios mínimos para el rol de IAM en la sección de Información adicional. Para obtener más información sobre cómo asumir un rol de IAM en el AWS CLI, consulte Usar un rol de IAM en el. AWS CLI	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas

Implementación del archivo de configuración	1. Ingrese el comando siguiente para inicializar Terraform.
	`$ terraform init -upgrade`
	2. Introduzca el comando siguiente para obtener una vista previa de los cambios en comparación con el estado actual.
	`$ terraform plan -var-file="variables.tfvars"`
	3. Revise los cambios de configuración en el plan de Terraform y confirme que desea implementar estos cambios en la organización.
	4. Ingrese el comando siguiente para implementar los recursos.
	`$ terraform apply -var-file="variables.tfvars"`
		DevOps ingeniero, AWS general, Terraform

(Opcional) Deshabilite los controles en la cuenta AWS Control Tower de administración

Tarea	Descripción	Habilidades requeridas
Ejecute el comando `destroy`.	Ingrese el comando siguiente para eliminar los recursos implementados por este patrón. `$ terraform destroy -var-file="variables.tfvars"`	DevOps ingeniero, AWS general, Terraform

Resolución de problemas

Problema	Solución
Error `Error: creating ControlTower Control ValidationException: Guardrail <control ID> is already enabled on organizational unit <OU ID>`	El control que intenta activar ya está activado en la unidad organizativa de destino. Este error puede producirse si un usuario habilitó manualmente el control a través de Consola de administración de AWS, mediante AWS Control Tower o mediante AWS Organizations. Para implementar el archivo de configuración de Terraform, puede usar cualquiera de las siguientes opciones. Opción 1: actualizar el archivo de estado actual de Terraform Puede importar el recurso al archivo de estado actual de Terraform. Al volver a ejecutar el comando `apply`, Terraform omitirá este recurso. Haga lo siguiente para importar el recurso al estado actual de Terraform:

Problema	Solución

	1. En la cuenta AWS Control Tower de administración, introduce el siguiente comando para recuperar una lista de los nombres de recursos de Amazon (ARNs) para OUs, donde `<root-ID>` está la raíz de la organización. Para obtener más información sobre cómo recuperar este ID, consulte Visualización de los detalles de la raíz.
	`aws organizations list-organizational-units-for-parent --parent-id <root-ID>`
	2. Para cada unidad organizativa devuelta en el paso anterior, introduzca el siguiente comando, donde `<OU-ARN>` es el ARN de la unidad organizativa.
	`aws controltower list-enabled-controls --target-identifier <OU-ARN>`
	3. Copie ARNs y realice la importación de Terraform en el módulo correspondiente para que se incluya en el estado de Terraform. Para obtener instrucciones, consulte Importación (documentación de Terraform).
	4. Repita los pasos de Implementar la configuración en la sección Epics..
	
	Opción 2: deshabilitar el control
	
	Si trabaja en un entorno que no es de producción, puede deshabilitar el control en la consola. Vuelva a habilitarlo al repetir los

Problema	Solución
	pasos de Implementar la configuración en la sección Epics. Este enfoque no se recomiend a para entornos de producción porque hay un período de tiempo en el que el control estará deshabilitado. Si desea utilizar esta opción en un entorno de producción, puede implement ar controles temporales, como la aplicación temporal de un SCP en AWS Organizations.

Recursos relacionados

AWS documentación

- Acerca de los controles (AWS Control Tower documentación)
- Biblioteca de controles (AWS Control Tower documentación)
- Implemente y gestione AWS Control Tower los controles mediante el uso de AWS CDK y AWS CloudFormation (Guía AWS prescriptiva)

Otros recursos

- Terraform
- Documentación de Terraform CLI

Información adicional

Ejemplo de archivo variables.tfvars

A continuación se muestra un ejemplo de un archivo variables.tfvars actualizado. Este ejemplo habilita el control AWS-GR_ENCRYPTED_VOLUMES (ID global: `503uicglhjkokaajywfpt6ros`) y el control AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED (ID global: `50z1ot237wl8u1lv5ufau6qqo`). Para obtener una lista de los identificadores globales IDs, consulte Todos los identificadores globales en la AWS Control Tower documentación.

El siguiente ejemplo también habilita los controles que tienen parámetros como CT.S3.PV.5 (IDglobal: `7mo7a2h2ebsq71l8k6uzr96ou`) y CT.SECRETSMANAGER.PV.1 (ID global:

dvhe47fxg5o6lryqrq9g6sxg4). Para obtener una lista de controles con parámetros, consulte Controles con parámetros en la AWS Control Tower documentación.

```
controls = [
    {
        control_names = [
            "503uicglhjkokaajywfpt6ros", # AWS-GR_ENCRYPTED_VOLUMES
            ...
        ],
        organizational_unit_ids = ["ou-1111-11111111", "ou-2222-22222222"...],
    },
    {
        control_names = [
            "50z1ot237wl8u1lv5ufau6qqo", # AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED
            ...
        ],
        organizational_unit_ids = ["ou-1111-11111111"...],
    },
]

controls_with_params = [
  {
    control_names = [
      { "7mo7a2h2ebsq71l8k6uzr96ou" = { # CT.S3.PV.5
        parameters = {
          "ExemptedPrincipalArns" : ["arn:aws:iam::*:role/RoleName"],
          "ExemptedResourceArns" : [],
        }
      } },
      { "dvhe47fxg5o6lryqrq9g6sxg4" = { # CT.SECRETSMANAGER.PV.1
        parameters = {
          "ExemptedPrincipalArns" : ["arn:aws:iam::*:role/RoleName"],
        }
      } },
      ...
    ],
    organizational_unit_ids = ["ou-1111-11111111"...]
  },
  {
    control_names = [
      { "dvuaav61i5cnfazfelmvn9m6k" = { # AWS-GR_DISALLOW_CROSS_REGION_NETWORKING
        parameters = {
          "ExemptedPrincipalArns" : ["arn:aws:iam::*:role/RoleName"],
```

```
        }
      } },
      { "41ngl8m5c4eb1myoz0t707n7h" = { # AWS-GR_DISALLOW_VPC_INTERNET_ACCESS
        parameters = {
          "ExemptedPrincipalArns" : ["arn:aws:iam::*:role/RoleName"],
        }
      } },
      ...
    ],
    organizational_unit_ids = ["ou-2222-22222222"...]
  }
]
```

Permisos con privilegios mínimos para el rol de IAM

Este patrón requiere que asuma un rol de IAM en la cuenta de administración. La práctica recomendada es asumir un rol con permisos temporales y limitar los permisos según el principio del privilegio mínimo. El siguiente ejemplo de política permite realizar las acciones mínimas necesarias para activar o desactivar AWS Control Tower los controles.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:EnableControl",
                "controltower:DisableControl",
                "controltower:GetControlOperation",
                "controltower:ListEnabledControls",
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeOrganization",
                "organizations:DetachPolicy",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:UpdatePolicy"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

Implemente las automatizaciones de seguridad para la AWS WAF solución mediante Terraform

Dr. Rahul Sharad Gaikwad y Tamilselvan P, Amazon Web Services

Resumen

AWS WAF es un firewall de aplicaciones web que ayuda a proteger las aplicaciones de los ataques más comunes mediante reglas personalizables, que se definen e implementan en listas de control de acceso web (). ACLs Configurar AWS WAF las reglas puede resultar complicado, especialmente para las organizaciones que no cuentan con equipos de seguridad especializados. Para simplificar este proceso, Amazon Web Services (AWS) ofrece la AWS WAF solución Security Automations for, que implementa automáticamente una única ACL web con un conjunto de AWS WAF reglas que filtra los ataques basados en la web. Durante la implementación de Terraform, puede especificar qué características de protección desea incluir. Tras implementar esta solución, AWS WAF inspecciona las solicitudes web a las CloudFront distribuciones de Amazon o a los balanceadores de carga de aplicaciones existentes y bloquea las solicitudes que no cumplan con las reglas.

La AWS WAF solución Security Automations for se puede implementar AWS CloudFormation siguiendo las instrucciones de la Guía de automatización de seguridad para la implementación. AWS WAF Este patrón proporciona una opción de implementación alternativa para las organizaciones que utilizan HashiCorp Terraform como su herramienta preferida de infraestructura como código (IaC) para aprovisionar y administrar su infraestructura de nube. Al implementar esta solución, Terraform aplica automáticamente los cambios en la nube e implementa y configura los ajustes y las AWS WAF funciones de protección.

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- AWS Command Line Interface (AWS CLI) versión 2.4.25 o posterior, instalada y configurada con los permisos necesarios. Para obtener más información, consulte Primeros pasos (AWS CLI documentación).
- La versión 1.1.9 o posterior de Terraform instalada y configurada. Para obtener más información, consulte Instalar Terraform (documentación de Terraform).

Arquitectura

Arquitectura de destino

Este patrón implementa las automatizaciones de seguridad para AWS WAF la solución. Para obtener más información sobre la arquitectura de destino, consulte la descripción general de la arquitectura en la Guía de automatización de seguridad para AWS WAF la implementación. Para obtener más información sobre AWS Lambda las automatizaciones de esta implementación, el analizador de registros de aplicaciones, el analizador de AWS WAF registros, el analizador de listas de IP y el controlador de acceso, consulte los detalles de los componentes en la Guía de automatización de seguridad para la implementación. AWS WAF

Implementación de Terraform

Cuando ejecuta `terraform apply`, Terraform hace lo siguiente:

1. Terraform crea roles AWS Identity and Access Management (IAM) y funciones Lambda en función de las entradas del archivo testing.tfvars.
2. Terraform crea reglas de AWS WAF ACL y conjuntos de IP en función de las entradas del archivo testing.tfvars.
3. Terraform crea los depósitos del Amazon Simple Storage Service (Amazon S3), las reglas AWS Glue de Amazon EventBridge , las tablas de bases de datos y los grupos de trabajo de Amazon Athena en función de las entradas del archivo testing.tfvars.
4. Terraform despliega la pila para aprovisionar los recursos personalizados. AWS CloudFormation
5. Terraform crea los recursos de Amazon API Gateway en función de las entradas proporcionadas del archivo testing.tfvars.

Automatización y escala

Puede usar este patrón para crear AWS WAF reglas para múltiples soluciones Cuentas de AWS e Regiones de AWS implementar la AWS WAF solución Security Automations for en todo su entorno. Nube de AWS

Tools (Herramientas)

Servicios de AWS

- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar Servicios de AWS mediante los comandos de su consola de línea de comandos.

- AWS WAF es un firewall de aplicación web que lo ayuda a supervisar las solicitudes HTTP y HTTPS que se reenvían a los recursos de su aplicación web protegida.

Otros servicios

- Git es un sistema de control de versiones distribuido y de código abierto.
- HashiCorp Terraform es una aplicación de interfaz de línea de comandos que le ayuda a usar código para aprovisionar y administrar la infraestructura y los recursos de la nube.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub AWS WAF Automation Using Terraform.

Prácticas recomendadas

- Coloque los archivos estáticos en buckets de Amazon S3 separados.
- Evite codificar variables de forma rígida.
- Limite el uso de scripts personalizados.
- Adopte una convención de nomenclatura.

Epics

Configure su equipo de trabajo local

Tarea	Descripción	Habilidades requeridas
Instale Git	Siga las instrucciones de Primeros pasos (sitio web de Git) para instalar Git en su estación de trabajo local.	DevOps ingeniero
Clonar el repositorio.	En la estación de trabajo local, introduzca el siguiente comando para clonar el repositorio de código:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`git clone https://github.com/aws-samples/aws-waf-automation-terraform-samples.git`	
Actualice las variables.	1. Para navegar al directorio clonado, introduzca el siguiente comando: `cd terraform-aws-waf-automation` 2. En cualquier editor de texto, abra el archivo testing.tfvars. 3. Actualice los valores de las variables en el archivo testing.tfvars. 4. Guarde y cierre el archivo.	DevOps ingeniero

Aprovisionar la arquitectura de destino mediante Terraform

Tarea	Descripción	Habilidades requeridas
Inicialice la configuración de Terraform.	Introduzca el siguiente comando para inicializar el directorio de trabajo que contiene los archivos de configuración de Terraform: `terraform init`	DevOps ingeniero
Obtenga una vista previa del plan Terraform.	Escriba el siguiente comando. Terraform evalúa los archivos	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	de configuración para determinar el estado objetivo de los recursos declarados. A continuación, compara el estado objetivo con el estado actual y crea un plan: `terraform plan -var-file ="testing.tfvars"`	
Verifique el plan.	Revise el plan y confirme que configura la arquitectura requerida en su Cuenta de AWS de destino.	DevOps ingeniero
Implemente la solución.	1. Introduzca el siguiente comando para aplicar el plan: `terraform apply -var-file="testing .tfvars"` 2. Escriba `yes` para confirmar . Terraform crea, actualiza o destruye la infraestructura para alcanzar el estado objetivo declarado en los archivos de configuración. Para obtener más informaci ón sobre la secuencia, consulte el implementación de Terraform en la sección Arquitectura de este patrón.	DevOps ingeniero

Validar y limpiar

Tarea	Descripción	Habilidades requeridas
Verifique los cambios.	1. En la consola de Terraform , compruebe que las salidas coincidan con los resultado s esperados. 2. Inicie sesión en Consola de administración de AWS. 3. Compruebe que las salidas de la consola de Terraform se hayan implementado correctamente en su Cuenta de AWS.	DevOps ingeniero
(Opcional) Limpieza de la infraestructura.	Si desea eliminar todos los cambios de configuración y recursos realizados por esta solución, haga lo siguiente: 1. En la consola de Terraform , introduzca el siguiente comando: `terraform destroy -var-file="testing .tfvars"` 2. Escriba `yes` para confirmar.	DevOps ingeniero

Resolución de problemas

Problema	Solución
Error `WAFV2 IPSet: WAFOptimisticLockException`	Si recibe este error al ejecutar el comando `terraform destroy`, debe eliminar

Problema	Solución
	manualmente los conjuntos de IP. Para obtener instrucciones, consulte Eliminar un conjunto de direcciones IP (AWS WAF documentación).

Recursos relacionados

AWS referencias

- Guía de automatización de seguridad para AWS WAF la implementación
- Automatizaciones de seguridad para AWS WAF(biblioteca de AWS soluciones)
- Preguntas frecuentes sobre las automatizaciones de seguridad para AWS WAF

Referencias de Terraform

- Terraform backend configuration
- Terraform AWS Provider: documentación y uso
- Terraform AWS Provider (repositorio) GitHub

Implementación de una canalización que detecte simultáneamente los problemas de seguridad en varios entregables de código

Benjamin Morris, Tim Hahn, Sapeksh Madan, Dina Odum y Isaiah Schisler, Amazon Web Services

Resumen

La canalización simple de análisis de código (SCSP) permite crear con dos clics una canalización de análisis de código que ejecuta en paralelo las herramientas de seguridad de código abierto estándares del sector. Esto permite a los desarrolladores comprobar la calidad y la seguridad de su código sin tener que instalar herramientas ni siquiera saber cómo ejecutarlas. Esto lo ayuda a reducir las vulnerabilidades y los errores de configuración en los entregables de código. También reduce la cantidad de tiempo que su organización dedica a instalar, investigar y configurar las herramientas de seguridad.

Antes del SCSP, el análisis de código con este conjunto particular de herramientas requería que los desarrolladores localizaran, instalaran y configuraran manualmente las herramientas de análisis de software. Incluso si se instalan localmente, all-in-one las herramientas, como Automated Security Helper (ASH), requieren configurar un contenedor Docker para poder ejecutarse. Sin embargo, con SCSP, un conjunto de herramientas de análisis de código estándar del sector se ejecuta automáticamente en la Nube de AWS. Con esta solución, utilizas Git para impulsar las entregas de código y, a continuación, recibes un resultado visual con at-a-glance información sobre los errores en las comprobaciones de seguridad.

Requisitos previos y limitaciones

- Un activo Cuenta de AWS
- Uno o más entregables de código que desee analizar para detectar problemas de seguridad
- AWS Command Line Interface (AWS CLI), instalado y configurado
- La versión 3.0 o posterior de Python o la versión 9.0.3 o posterior de pip instaladas
- Git, instalado
- Instálelo git-remote-codecommiten su estación de trabajo local

Arquitectura

Pila de tecnología de destino

- AWS CodeCommit repositorio
- AWS CodeBuild proyecto
- AWS CodePipeline oleoducto
- Bucket de Amazon Simple Storage Service (Amazon S3)
- AWS CloudFormation plantilla

Arquitectura de destino

El SCSP para el análisis de código estático es un DevOps proyecto diseñado para proporcionar información de seguridad sobre el código entregable.

1. En el Consola de administración de AWS, inicia sesión en el objetivo. Cuenta de AWS Confirme que se encuentra en el Región de AWS lugar donde desea implementar la canalización.
2. Utilice la CloudFormation plantilla del repositorio de código para implementar la pila SCSP. Esto crea un CodeCommit repositorio y un CodeBuild proyecto nuevos.

> **Note**
>
> Como opción de implementación alternativa, puedes usar un CodeCommit repositorio existente proporcionando el nombre de recurso de Amazon (ARN) del repositorio como parámetro durante el despliegue de la pila.

3. Clone el repositorio en su estación de trabajo local y, a continuación, añada los archivos a sus respectivas carpetas del repositorio clonado.
4. Usa Git para añadir, confirmar y enviar los archivos al CodeCommit repositorio.
5. Al empujarlos al CodeCommit repositorio, se inicia un CodeBuild trabajo. El CodeBuild proyecto utiliza las herramientas de seguridad para escanear los entregables de código.
6. Revise el resultado de la canalización. Las herramientas de seguridad que detecten problemas de nivel de error provocarán acciones fallidas en la canalización. Corrija estos errores o elimínelos como falsos positivos. Revisa los detalles del resultado de la herramienta en los detalles de la acción en el bucket S3 de la canalización CodePipeline o en él.

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y administrarlos a lo largo de su ciclo de vida en todas Cuentas de AWS las regiones.
- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- AWS CodeCommit es un servicio de control de versiones que permite almacenar y administrar repositorios de Git de forma privada, sin necesidad de administrar su propio sistema de control de origen.

Otras herramientas

Para obtener una lista completa de las herramientas que SCSP utiliza para escanear los entregables de código, consulte el léame del SCSP. GitHub

Repositorio de código

El código de este patrón está disponible en el repositorio Simple Code Scanning Pipeline (SCSP) de. GitHub

Epics

Implementación de SCSP

Tarea	Descripción	Habilidades requeridas
Crea la CloudFormation pila.	1. Inicie sesión en la Consola de administración de AWS. 2. En la consola, confirme que se encuentra en la región de destino en la que desea implementar la solución. Para obtener más informaci ón, consulte Selección de una región. 3. Elija el enlace siguiente. Esto abre el asistente de	AWS DevOps, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	creación rápida de pilas CloudFormation. https://console.aws.amazon.com/cloudformation/¿casa? #/ -Pipeline-stack.template.json&stackName= stacks/create/review?templateURL=https://proservetools.s3.amazonaws.com/cft/scsp SimpleCodeScanPipeline 4. En el asistente de creación rápida de pilas, revise la configuración de los parámetros de la pila y realice las modificaciones necesarias según su caso de uso. 5. Seleccione Acepto que AWS CloudFormation podría crear recursos de IAM y, a continuación, elija Create stack. Esto crea un CodeCommit repositorio, una CodePipeline canalización, varias definiciones de CodeBuild trabajos y un bucket de S3. Las ejecuciones de compilación y los resultados del análisis se copian en este bucket. Una	

Tarea	Descripción	Habilidades requeridas
	vez que la CloudFormation pila se haya desplegado por completo, SCSP estará listo para su uso.	

Uso de la canalización

Tarea	Descripción	Habilidades requeridas
Examine los resultados del análisis.	1. En la consola de Amazon S3, en Buckets, elija el bucket simplecodescanpipeline-deleteresourcespipelinereso. 2. Elija el directorio scan_results y, a continuación, elija la carpeta con la fecha de análisis más reciente. 3. Revise los archivos de registro de esta carpeta para revisar cualquier problema detectado por las herramientas de seguridad utilizadas en la canalización. Las herramientas de seguridad que detecten problemas de nivel de error provocarán acciones `failed` en la canalización. Si se trata de falsos positivos, es necesario corregirlos o suprimirlos.	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Note También puede ver los detalles del resultado de la herramienta (tanto para los escaneos aprobados como para los que no) en la CodePipeline consola, en la sección de detalles de las acciones.	

Resolución de problemas

Problema	Solución
HashiCorp No se están escaneando Terraform ni sus AWS CloudFormation archivos.	Asegúrese de que los archivos Terraform (.tf) y CloudFormation (.yml, .yaml o .json) estén ubicados en las carpetas correspondientes del repositorio clonado. CodeCommit
El comando `git clone` está fallando.	Asegúrese de haber instalado `git-remote-codecommit` y de que su CLI tenga acceso a AWS las credenciales que tienen permisos para leer el CodeCommit repositorio.
Un error de simultaneidad, como `Project-level concurrent build limit cannot exceed the account-level concurrent build limit of 1 .`	Vuelva a ejecutar la canalización pulsando el botón Release Change de la CodePipeline consola. Se trata de un problema conocido que parece ser más común las primeras veces que se ejecuta la canalización.

Recursos relacionados

Proporcione comentarios sobre el proyecto de SCSP.

Información adicional

Preguntas frecuentes

¿El proyecto de SCSP es igual al de Automated Security Helper (ASH)?

No. Use ASH cuando desee una herramienta de CLI que ejecute herramientas de análisis de código mediante contenedores. Automated Security Helper (ASH) es una herramienta diseñada para reducir la probabilidad de que se produzca una infracción de seguridad en la nueva configuración de código, infraestructura o recursos de IAM. ASH es una utilidad de línea de comandos que se puede ejecutar de forma local. El uso local requiere que un entorno de contenedores esté instalado y operativo en el sistema.

Utilice SCSP cuando desee una canalización de configuración más sencilla que la de ASH. SCSP no requiere instalaciones locales. SCSP está diseñado para ejecutar comprobaciones de forma individual en una canalización y mostrar los resultados por herramienta. SCSP también evita gran parte de la sobrecarga que supone la configuración de Docker y es independiente del sistema operativo (SO).

¿SCSP es solo para equipos de seguridad?

No, cualquiera puede implementar la canalización para determinar qué partes de su código no superan los controles de seguridad. Por ejemplo, los usuarios que no son usuarios de seguridad pueden usar SCSP para comprobar su código antes de revisarlo con sus equipos de seguridad.

¿Puedo usar SCSP si estoy trabajando con otro tipo de repositorio, como GitLab GitHub, o Bitbucket?

Puede configurar un repositorio git local para que apunte a dos repositorios remotos diferentes. Por ejemplo, puedes clonar un GitLab repositorio existente, crear una instancia de SCSP (especificando CloudFormation las carpetas Terraform y AWS Config Rules Development Kit (AWS RDK), si fuera necesario) y, a continuación, utilizarla `git remote add upstream <SCSPGitLink>` para apuntar también el repositorio local al repositorio de SCSP. CodeCommit Esto permite que los cambios de código se envíen primero a SCSP, se validen y, después, después de realizar cualquier actualización adicional para corregir los hallazgos, se envíen al repositorio o a Bitbucket

GitLab. GitHub Para obtener más información sobre varios controles remotos, consulta Enviar confirmaciones a un repositorio de Git adicional (entrada AWS del blog).

> **Note**
>
> Tenga cuidado con las desviaciones, por ejemplo, evite hacer cambios a través de las interfaces web.

Contribución y adición de sus propias acciones

La configuración de SCSP se mantiene como un GitHub proyecto, que contiene el código fuente de la aplicación AWS Cloud Development Kit (AWS CDK) SCSP. Para añadir comprobaciones adicionales a la canalización, es necesario actualizar la AWS CDK aplicación y, a continuación, sintetizarla o desplegarla en el destino en el que Cuenta de AWS se ejecutará la canalización. Para ello, comience por clonar el GitHub proyecto SCSP y, a continuación, busque el archivo de definición de la pila en la `lib` carpeta.

Si quieres añadir una marca adicional, la `StandardizedCodeBuildProject` clase del AWS CDK código facilita la adición de acciones. Proporciona el nombre, la descripción `install` o los `build` comandos. AWS CDK crea el CodeBuild proyecto utilizando valores predeterminados razonables. Además de crear el proyecto de construcción, es necesario añadirlo a las CodePipeline acciones de la fase de construcción. Al diseñar una nueva comprobación, la acción debería `FAIL` si la herramienta de análisis detecta problemas o no se ejecuta. La acción debería `PASS` si la herramienta de análisis no detecta ningún problema. Para ver un ejemplo de configuración de una herramienta, revise el código de la acción `Bandit`.

Para obtener más información acerca de las entradas y salidas esperadas, consulte la documentación del repositorio.

Si agrega acciones personalizadas, debe implementar SCSP mediante `cdk deploy` o `cdk synth + CloudFormation deploy`. Esto se debe a que los propietarios del repositorio mantienen la CloudFormation plantilla de pila Quick Create.

Implemente controles de acceso basados en atributos de detección para subredes públicas mediante AWS Config

Alberto Menéndez, Amazon Web Services

Resumen

Las arquitecturas de redes perimetrales distribuidas se basan en la seguridad perimetral de la red que se ejecuta junto con las cargas de trabajo de sus nubes privadas virtuales (). VPCs Esto proporciona una escalabilidad sin precedentes en comparación con el enfoque centralizado más común. Si bien la implementación de subredes públicas en las cuentas de carga de trabajo puede ofrecer beneficios, también presenta nuevos riesgos de seguridad porque aumenta la superficie expuesta a ataques. Le recomendamos que implemente solo los recursos de Elastic Load Balancing, como los balanceadores de carga de aplicaciones o las puertas de enlace NAT, en las subredes públicas de estos. VPCs El uso de equilibradores de carga y puertas de enlace NAT en subredes públicas dedicadas lo ayuda a implementar un control detallado del tráfico entrante y saliente.

Le recomendamos que implemente controles preventivos y de detección para limitar los tipos de recursos que se pueden implementar en las subredes públicas. Para obtener más información sobre el uso del control de acceso basado en atributos (ABAC) para implementar controles preventivos en las subredes públicas, consulte Implementación de controles de acceso preventivos basados en atributos para las subredes públicas. Si bien son eficaces en la mayoría de las situaciones, es posible que estos controles preventivos no aborden todos los casos de uso posibles. Por lo tanto, este patrón se basa en el enfoque ABAC y lo ayuda a configurar alertas sobre los recursos no conformes que se despliegan en las subredes públicas. La solución comprueba si las interfaces de red elásticas pertenecen a un recurso que no está permitido en las subredes públicas.

Para lograrlo, este patrón utiliza reglas de AWS Config personalizadas y ABAC. La regla personalizada procesa la configuración de una interfaz de red elástica cada vez que se crea o modifica. En un nivel superior, esta regla realiza dos acciones para determinar si la interfaz de red es compatible:

1. Para determinar si la interfaz de red está dentro del ámbito de aplicación de la regla, la regla comprueba si la subred tiene etiquetas de AWS específicas que indican que es una subred pública. Por ejemplo, esta etiqueta podría ser `IsPublicFacing=True`.
2. Si la interfaz de red se implementa en una subred pública, la regla comprueba quién creó este recurso. Servicio de AWS Si el recurso no es un recurso de Elastic Load Balancing o una puerta de enlace de NAT, lo marca como no conforme.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- AWS Configconfigurado en la cuenta de carga de trabajo
- Permisos para implementar los recursos necesarios en la cuenta de carga de trabajo
- Una VPC con subredes públicas
- Etiquetas aplicadas correctamente para identificar las subredes públicas de destino
- (Opcional) Una organización en AWS Organizations
- (Opcional) Una cuenta de seguridad central que es la administradora delegada de AWS Config y AWS Security Hub CSPM

Arquitectura

Arquitectura de destino

En el siguiente diagrama se ilustra lo siguiente:

1. Cuando se implementa o modifica un recurso de interface de red elástica (`AWS::EC2::NetworkInterface`), AWS Config captura el evento y la configuración.
2. AWS Config compara este evento con la regla personalizada utilizada para evaluar la configuración.
3. Se invoca la AWS Lambda función asociada a esta regla personalizada. La función evalúa el recurso y aplica la lógica especificada para determinar si la configuración del recurso es `COMPLIANT`, `NON_COMPLIANT` o `NOT_APPLICABLE`.
4. Si se determina que un recurso lo es`NON_COMPLIANT`, AWS Config envía una alerta a través de Amazon Simple Notification Service (Amazon SNS).

> Nota: Si esta cuenta es una cuenta de miembro AWS Organizations, puede enviar los datos de conformidad a una cuenta de seguridad central a través de AWS Config o AWS Security Hub CSPM.

Lógica de evaluación de funciones de Lambda

El siguiente diagrama muestra la lógica aplicada por la función de Lambda para evaluar la conformidad de la interfaz de red elástica.

Automatización y escala

Este patrón es una solución detectivesca. También puede complementarlo con una regla de corrección para resolver automáticamente cualquier recurso que no cumpla con las normas. Para obtener más información, consulte Remediar recursos no conformes con AWS Config reglas.

Puede escalar esta solución de la siguiente manera:

- Exigir la aplicación de las AWS etiquetas correspondientes que establezca para identificar las subredes públicas. Para obtener más información, consulte las políticas de etiquetas en la documentación. AWS Organizations
- Configurar una cuenta de seguridad central que aplique la regla AWS Config personalizada a todas las cuentas de carga de trabajo de la organización. Para obtener más información, consulte Automatizar el cumplimiento de la configuración a gran escala AWS (entrada del AWS blog).
- Integrarse AWS Config con AWS Security Hub CSPM para capturar, centralizar y notificar a escala. Para obtener más información, consulte Configuración AWS Config en la AWS Security Hub CSPM documentación.

Tools (Herramientas)

- AWS Configproporciona una vista detallada de los recursos que tiene Cuenta de AWS y de cómo están configurados. Le ayuda a identificar cómo se relacionan los recursos entre sí y cómo han cambiado sus configuraciones a lo largo del tiempo.
- Elastic Load Balancing permite distribuir el tráfico entrante de las aplicaciones o de la red entre varios destinos. Por ejemplo, puede distribuir el tráfico entre instancias, contenedores y direcciones IP de Amazon Elastic Compute Cloud (Amazon EC2) en una o más zonas de disponibilidad.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.

- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Prácticas recomendadas

Para obtener más ejemplos y prácticas recomendadas para desarrollar AWS Config reglas personalizadas, consulte el repositorio de AWS Config reglas oficial en GitHub.

Epics

Implementar la solución

Tarea	Descripción	Habilidades requeridas
Crear la función de Lambda.	1. Inicie sesión en la AWS Lambda consola y Consola de administración de AWS, a continuación, ábrala. 2. En la página Functions (Funciones), seleccione Create function (Crear función). 3. Seleccione Crear desde cero. 4. En el panel de Información básica, para el Nombre de la función introduzca un nombre. 5. En Tiempo de ejecución, seleccione Python 3.12. 6. Deje la arquitectura establecida en x86_64. 7. Seleccione Creación de función. 8. Elija la pestaña Código.	AWS general

Tarea	Descripción	Habilidades requeridas
	9. En el explorador de archivos, elija lambda_function.py. 10. Pegue el código de ejemplo que se proporciona en la sección Información adicional en este patrón en la pestaña lambda_function.py. Personalice el código de ejemplo para identificar cualquier lógica de evaluación personalizada de la función `evaluate_change_notification_compliance` . 11. Elija Implementar.	

Tarea	Descripción	Habilidades requeridas
Todos estos permisos se agregan al rol de ejecución de la función de Lambda.	1. Seleccione Funciones en el panel de navegación. 2. Elegir la función que acaba de crear. 3. Elija Configuration (Configuración) y, a continuación, seleccione Permissions (Permisos). 4. Elija el nombre del rol para abrirlo en la consola AWS Identity and Access Management (IAM). 5. En la pestaña Políticas de permisos, elija Agregar permisos y después Crear política insertada. 6. Elija JSON. 7. Pegue la siguiente política en el editor de políticas . Esto permite a las funciones de Lambda: • Obtener los detalles de las etiquetas de subred. • Envíe el resultado de la conformidad a AWS Config. `{ "Version": "2012-10-17", "Statement": [ {`	AWS general

Tarea	Descripción	Habilidades requeridas

	<pre>"Action":
	[
	"config:PutEvaluations",
	"ec2:DescribeSubnets"
	],
	"Resource": "*",
	"Effect":
	"Allow"
	}
	]
	}</pre>
	8. Elija Siguiente.
	9. Escriba un nombre para la política y elija Create policy (Crear política).	

Recuperar el nombre de recurso de Amazon (ARN) de la función de Lambda.	1. Abra la consola de Lambda. 2. Seleccione Funciones en el panel de navegación. 3. Elegir la función que acaba de crear. 4. En la sección Información general de la función, en ARN de la función, copie el valor.	AWS general

Tarea	Descripción	Habilidades requeridas
Cree la regla AWS Config personalizada.	1. Abra la consola de AWS Config. 2. En la página Rules (Reglas), seleccione Add rule (Añadir regla). 3. En la página Especificar tipo de regla, elija Cree una regla personalizada de Lambda y, a continuación, elija Siguiente. 4. En la página Configurar regla, haga lo siguiente: a. Introduzca un nombre y una descripción. b. En ARN de la función AWS Lambda , pegue el ARN que copió anteriormente. c. Para Tipo de desencadenador, elija Cuando cambia la configuración. d. En Ámbito de cambios, elija Recursos. e. En Tipo de recurso, elija AWS EC2 NetworkInterface. f. Elija Siguiente. 5. En la página Revisar y crear, revise la configuración de su regla y, a continuación, seleccione Guardar.	AWS general

Tarea	Descripción	Habilidades requeridas
Configure las notificaciones.	1. Siga las instrucciones de Creación de un tema de Amazon SNS para crear un tema de Amazon SNS. 2. Siga las instrucciones de Suscripción a un tema de Amazon SNS para configurar un punto de conexión que reciba notificaciones del tema Amazon SNS. 3. Sigue las instrucciones de Cómo puedo recibir una notificación cuando un AWS recurso no cumple con las normas AWS Config para configurar una EventBridge regla de Amazon personali zada para tus recursos no conformes.	AWS general

Pruebe la solución

Tarea	Descripción	Habilidades requeridas
Cree un recurso compatible.	1. Siga las instrucciones siguientes para crear uno de los recursos compatibles en una subred pública: • Cree una puerta de enlace NAT • Getting started with Network Load Balancers	AWS general

Tarea	Descripción	Habilidades requeridas
	• Creación de un equilibrador de carga de aplicación 2. Una vez creado el recurso, la regla AWS Config personalizada evalúa las interfaces de red elásticas asociadas al recurso. Marca estas interfaces de red como `COMPLIANT` . AWS Config Para ver los recursos en él, sigue estos pasos: a. Abra la consola de AWS Config. b. En la página Reglas, seleccione su regla. c. En la página de detalles de la regla, vaya al final de la página. d. En Recursos incluidos en el ámbito de aplicación, seleccione Conforme. Confirme que ve las interfaces IDs de red que se crearon. e. Para obtener más información sobre la configuración de la interfaz de red, elija el ID del recurso.	

Tarea	Descripción	Habilidades requeridas
Cree un recurso no conforme.	1. Siga las instrucciones siguientes para crear un recurso no conforme en una subred pública: • Lanza una EC2 instancia de Amazon • Creación de una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) • Crear un punto final de VPC 2. Una vez creado el recurso, la regla AWS Config personalizada evalúa las interfaces de red elásticas asociadas al recurso. Marca estas interfaces de red como `NON_COMPLIANT` . AWS Config Para ver los recursos en él, sigue estos pasos: a. Abra la consola de AWS Config. b. En la página Reglas, seleccione su regla. c. En la página de detalles de la regla, vaya al final de la página. d. En Recursos incluidos en el ámbito, selecciona NonCompliant. Confirme	AWS general

Tarea	Descripción	Habilidades requeridas
	que ve las interfaces IDs de red que se crearon. e. Para obtener más información sobre la configuración de la interfaz de red, elija el ID del recurso. 3. Confirme que recibe la notificación en el punto de conexión que configuró en Amazon SNS.	
Cree un recurso que no sea aplicable.	1. En una subred privada, cree cualquier recurso que requiera una interfaz de red elástica. 2. Una vez creado el recurso, la regla AWS Config personalizada evalúa las interfaces de red elásticas asociadas al recurso. Marca estas interfaces de red como `NOT_APPLICABLE` . Estos recursos no se muestran en la AWS Config consola.	AWS general

Recursos relacionados

AWS documentación

- Configuración AWS Config
- AWS Config reglas personalizadas
- ABAC para AWS

- Implementación de controles de acceso preventivos basados en atributos para las subredes públicas

Otros recursos AWS

- Automatice el cumplimiento de la configuración a gran escala AWS
- Arquitecturas de inspección distribuida con el Equilibrador de carga de puerta de enlace

Información adicional

El siguiente es un ejemplo de una función de Lambda que se proporciona con fines de demostración.

```
import boto3
import json
import os

# Init clients
config_client = boto3.client('config')
ec2_client = boto3.client('ec2')

def lambda_handler(event, context):

    # Init values
    compliance_value = 'NOT_APPLICABLE'
    invoking_event = json.loads(event['invokingEvent'])
    configuration_item = invoking_event['configurationItem']

    status = configuration_item['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']

    # First check if the event configuration applies. Ex. resource event is not delete
    if (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope:
        compliance_value = evaluate_change_notification_compliance(configuration_item)


    config_client.put_evaluations(
       Evaluations=[
           {
               'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
```

```
                'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
                'ComplianceType': compliance_value,
                'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
            },
        ],
        ResultToken=event['resultToken'])

# Function with the logs to evaluate the resource
def evaluate_change_notification_compliance(configuration_item):
    is_in_scope = is_in_scope_subnet(configuration_item['configuration']['subnetId'])

    if (configuration_item['resourceType'] != 'AWS::EC2::NetworkInterface') or not
 is_in_scope:
        return 'NOT_APPLICABLE'

    else:
        alb_condition = configuration_item['configuration']['requesterId'] in ['amazon-
elb']
        nlb_condition = configuration_item['configuration']['interfaceType'] in
 ['network_load_balancer']
        nat_gateway_condition = configuration_item['configuration']['interfaceType'] in
 ['nat_gateway']

        if alb_condition or nlb_condition or nat_gateway_condition:
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

# Function to check if elastic network interface is in public subnet
def is_in_scope_subnet(eni_subnet):

    subnet_description = ec2_client.describe_subnets(
        SubnetIds=[eni_subnet]
    )

    for subnet in subnet_description['Subnets']:
        for tag in subnet['Tags']:
            if tag['Key'] == os.environ.get('TAG_KEY') and tag['Value'] ==
 os.environ.get('TAG_VALUE'):
                return True

    return False
```

Implementación de controles de acceso preventivos basados en atributos para las subredes públicas

Joel Alfredo Nunez Gonzalez y Samuel Ortega Sancho, Amazon Web Services

Resumen

En las arquitecturas de red centralizadas, las nubes privadas virtuales de inspección y periferia (VPCs) concentran todo el tráfico entrante y saliente, como el tráfico hacia y desde Internet. Sin embargo, esto puede crear cuellos de botella o provocar que se alcancen los límites de las Service quotas de AWS. La implementación de la seguridad perimetral de la red junto con las cargas de trabajo VPCs proporciona una escalabilidad sin precedentes en comparación con el enfoque centralizado más común. Esto se denomina arquitectura de periferia distribuida.

Si bien la implementación de subredes públicas en las cuentas de carga de trabajo puede ofrecer beneficios, también presenta nuevos riesgos de seguridad porque aumenta la superficie expuesta a ataques. Se recomienda implementar solo los recursos de Elastic Load Balancing (ELB), como los balanceadores de carga de aplicaciones o las puertas de enlace NAT, en las subredes públicas de estos. VPCs El uso de equilibradores de carga y puertas de enlace NAT en subredes públicas dedicadas lo ayuda a implementar un control detallado del tráfico entrante y saliente.

El control de acceso basado en atributos (ABAC) es la práctica de crear permisos detallados basados en los atributos del usuario, como el departamento, el puesto de trabajo y el nombre del equipo. Para obtener más información, consulte ABAC para AWS. ABAC puede proporcionar barreras para las subredes públicas en las cuentas de carga de trabajo. Esto ayuda a los equipos de aplicaciones a ser ágiles, sin comprometer la seguridad de la infraestructura.

Este patrón describe cómo ayudar a proteger las subredes públicas mediante la implementación de ABAC mediante una política de control de servicios (SCP) en AWS Organizations y políticas en AWS Identity and Access Management (IAM). El SCP se aplica a una cuenta de miembro de una organización o a una unidad organizativa (OU). Estas políticas de ABAC permiten a los usuarios implementar pasarelas NAT en las subredes de destino e impiden que desplieguen otros recursos de Amazon Elastic Compute Cloud (Amazon EC2), como EC2 instancias e interfaces de red elásticas.

Requisitos previos y limitaciones

Requisitos previos

- Una organización en AWS Organizations

- Acceso administrativo a la cuenta raíz de AWS Organizations
- En la organización, una cuenta de miembro activa o una unidad organizativa para probar el SCP

Limitaciones

- El SCP de esta solución no impide que los servicios de AWS que utilizan un rol vinculado a un servicio implementen recursos en las subredes de destino. Algunos ejemplos de estos servicios son Elastic Load Balancing (ELB), Amazon Elastic Container Service (Amazon ECS) y Amazon Relational Database Service (Amazon RDS). Para obtener más información, consulte Efectos de SCP en los permisos en la documentación de AWS Organizations. Implemente controles de seguridad para detectar estas excepciones.

Arquitectura

Pila de tecnología de destino

- SCP aplicado a una cuenta o unidad organizativa de AWS en AWS Organizations
- Las siguientes roles de IAM:
  - `AutomationAdminRole`: Se utiliza para modificar las etiquetas de subred y crear recursos de VPC después de implementar el SCP
  - `TestAdminRole`: Se utiliza para comprobar si el SCP impide que otros responsables de IAM, incluidos los que tienen acceso administrativo, realicen las acciones reservadas para `AutomationAdminRole`

Arquitectura de destino

1. El rol de IAM de `AutomationAdminRole` se crea en la cuenta de destino. Este rol tiene permisos para administrar los recursos de red. Tenga en cuenta los siguientes permisos que son exclusivos de este rol:
   - Esta función puede crear VPCs y publicar subredes.
   - Este rol puede modificar las asignaciones de etiquetas para las subredes de destino.
   - Este rol puede administrar sus propios permisos.
2. En AWS Organizations, se aplica el SCP a la cuenta o unidad organizativa de AWS de destino. Para ver un ejemplo de política, consulte Información adicional en este patrón.

3. Un usuario o una herramienta de la CI/CD canalización pueden asumir la `AutomationAdminRole` función de aplicar la `SubnetType` etiqueta a las subredes de destino.
4. Al asumir otros roles de IAM, los directores de IAM autorizados de su organización pueden administrar las puertas de enlace NAT en las subredes de destino y otros recursos de red permitidos en la cuenta de AWS, como las tablas de enrutamiento. Utilice políticas de IAM para conceder esos permisos. Para obtener más información, consulte Administración de identidad y acceso para Amazon VPC.

Automatizar y escalar

Para ayudar a proteger las subredes públicas, se deben aplicar las etiquetas de AWS correspondientes. Tras aplicar el SCP, las pasarelas NAT son el único tipo de EC2 recurso de Amazon que los usuarios autorizados pueden crear en las subredes que tienen la etiqueta. `SubnetType:IFA` (se `IFA` refiere a los activos con acceso a Internet). El SCP impide la creación de otros EC2 recursos de Amazon, como instancias e interfaces de red elásticas. Te recomendamos que utilices una CI/CD canalización que asuma la `AutomationAdminRole` función de crear recursos de VPC para que estas etiquetas se apliquen correctamente a las subredes públicas.

Tools (Herramientas)

Servicios de AWS

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Organizations es un servicio de administración de cuentas que le permite agrupar varias cuentas de AWS en una organización que usted crea y administra de manera centralizada. En AWS Organizations, puede implementar políticas de control de servicios (SCPs), que son un tipo de política que puede usar para administrar los permisos en su organización.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Epics

Aplicación del SCP

Tarea	Descripción	Habilidades requeridas
Cree un rol de administrador de pruebas.	Cree un rol de IAM denominado `TestAdminRole` en la cuenta destino de AWS. Adjunte la política de IAM gestionada por AdministratorAccessAWS a la nueva función. Para obtener instrucciones, consulte Crear un rol para delegar permisos a un usuario de IAM en la documentación de IAM.	Administrador de AWS
Cree el rol de administrador de automatización.	1. Cree un rol de IAM denominado `AutomationAdminRole` en la cuenta destino de AWS. 2. Adjunte la política de IAM gestionada por AdministratorAccessAWS a la nueva función. El siguiente es un ejemplo de política de confianza que puede usar para probar el rol de la cuenta de `111122223333` . `{ "Version": "2012-10-17", "Statement": [`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	<pre>{
	"Effect": "Allow",
	"Principal": {
	"AWS": [
	"arn:aws:iam::111122223333:root"
	]
	},
	"Action": "sts:AssumeRole",
	"Condition": {}
	}
	]
	}</pre>	

Cree y adjunte el SCP.	1. Con el código de ejemplo que se proporciona en la sección de información adicional, cree una política de control de seguridad. Para obtener instrucciones, consulte Creación de un SCP en la documentación de AWS Organizations. 2. Adjunte el SCP a la cuenta o unidad organizativa de AWS de destino. Para obtener instrucciones, consulte Adjuntar y separar políticas de control de servicios en la documentación de AWS Organizations.	Administrador de AWS

Pruebe el SCP

Tarea	Descripción	Habilidades requeridas
Cree una VPC o subred.	1. Asuma el rol `TestAdmin Role` en la cuenta de AWS de destino. 2. Intente crear una VPC o una nueva subred pública en una VPC existente. Para obtener instrucciones, consulte Creación de una VPC, subredes y otros recursos de la VPC en la documentación de Amazon VPC. No debería poder crear estos recursos. 3. Asuma el rol `Automatio nAdminRole` y vuelva a intentar el paso anterior. Ahora debería poder crear los recursos de red.	Administrador de AWS
Administrar etiquetas.	1. Asuma el rol `TestAdmin Role` en la cuenta de AWS de destino. 2. Añada una etiqueta `SubnetType:IFA` a una subred pública disponibl e. Debería poder añadir esta etiqueta. Para obtener instrucciones sobre cómo añadir etiquetas a través de la Interfaz de la línea de comandos de AWS (AWS CLI), consulte create-ta	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	gs en la Referencia de los comandos de la CLI de AWS. 3. Sin cambiar sus credencia les, intente modificar la etiqueta `SubnetTyp e:IFA` asignada a esta subred. No debería poder modificar esta etiqueta. 4. Asuma el rol `Automatio nAdminRole` y vuelva a intentar los pasos anteriore s. Este rol debería poder añadir y modificar esta etiqueta.	

Tarea	Descripción	Habilidades requeridas
Implemente recursos en las subredes de destino.	1. Asumir el rol `TestAdmin Role` . 2. Para una subred pública que tenga la `SubnetTyp e:IFA` etiqueta, intente crear una EC2 instancia . Para obtener instrucci ones, consulta Cómo lanzar una instancia en la EC2 documentación de Amazon. En esta subred, no deberías poder crear, modificar ni eliminar ningún EC2 recurso de Amazon excepto las puertas de enlace NAT. 3. Cree una puerta de enlace NAT en la misma subred. Para obtener instrucciones, consulte Creación de una puerta de enlace NAT en la documentación de Amazon VPC. Debería poder crear, modificar o eliminar puertas de enlace NAT en esta subred.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Administre el rol AutomationAdminRole .	1. Asumir el rol `TestAdminRole` . 2. Intente modificar el rol `AutomationAdminRole` . Para obtener instrucciones, consulte Modificación de un rol en la documentación de IAM. No debería poder modificar este rol. 3. Asuma el rol `AutomationAdminRole` y vuelva a intentar el paso anterior. Ahora debería poder modificar el rol.	Administrador de AWS

Limpieza

Tarea	Descripción	Habilidades requeridas
Limpie los recursos desplegados.	1. Separe el SCP de la cuenta o unidad organizativa de AWS. Para obtener instrucciones, consulte Separar un SCP en la documentación de AWS Organizations. 2. Elimine la SCP. Para obtener instrucciones, consulte Eliminar un SCP (documentación de AWS Organizations). 3. Elimine el rol `AutomationAdminRole` y el rol	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	`TestAdminRole` . Para obtener instrucciones, consulte Eliminar funciones en la documentación de IAM. 4. Elimine todos los recursos de red, como VPCs las subredes, que haya creado para esta solución.	

Recursos relacionados

Documentación de AWS

- Acoplamiento y desconexión SCPs
- Crear, actualizar y eliminar SCPs
- Implementación de controles de acceso basados en atributos de detección para subredes públicas mediante AWS Config
- Controles de detección
- Referencia de autorizaciones de servicio
- Etiquetado de recursos de AWS
- ¿Qué es ABAC para AWS?

Referencias adicionales de AWS

- Proteger las etiquetas de recursos utilizadas para la autorización mediante una política de control de servicios en AWS Organizations (entrada del blog de AWS)

Información adicional

La siguiente política de control de servicios es un ejemplo que puede utilizar para probar este enfoque en su organización.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyVPCActions",
      "Effect": "Deny",
      "Action": [
        "ec2:CreateVPC",
        "ec2:CreateRoute",
        "ec2:CreateSubnet",
        "ec2:CreateInternetGateway",
        "ec2:DeleteVPC",
        "ec2:DeleteRoute",
        "ec2:DeleteSubnet",
        "ec2:DeleteInternetGateway"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:*"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN": ["arn:aws:iam::*:role/AutomationAdminRole"]
        }
      }
    },
    {
      "Sid": "AllowNATGWOnIFASubnet",
      "Effect": "Deny",
      "NotAction": [
        "ec2:CreateNatGateway",
        "ec2:DeleteNatGateway"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition": {
        "ForAnyValue:StringEqualsIfExists": {
          "aws:ResourceTag/SubnetType": "IFA"
        },
        "StringNotLike": {
          "aws:PrincipalARN": ["arn:aws:iam::*:role/AutomationAdminRole"]
        }
      }
```

```
    },
    {
      "Sid": "DenyChangesToAdminRole",
      "Effect": "Deny",
      "NotAction": [
        "iam:GetContextKeysForPrincipalPolicy",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Resource": [
        "arn:aws:iam::*:role/AutomationAdminRole"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN": ["arn:aws:iam::*:role/AutomationAdminRole"]
        }
      }
    }
  ]
}
```

Detección de las instancias de bases de datos de Amazon RDS y Aurora que tienen certificados CA vencidos

Stephen DiCato y Eugene Shifer, Amazon Web Services

Resumen

Como práctica recomendada de seguridad, se recomienda cifrar los datos en tránsito entre los servidores de aplicaciones y las bases de datos relacionales. Puede usar SSL o TLS para cifrar una conexión a una instancia o clúster de base de datos (DB). Estos protocolos ayudan a proporcionar confidencialidad, integridad y autenticidad entre una aplicación y una base de datos. La base de datos utiliza un certificado de servidor, emitido por una autoridad de certificación (CA) y que se utiliza para realizar la verificación de la identidad del servidor. Los certificados SSL o TLS comprueban la autenticidad del certificado validando su firma digital y asegurándose de que no haya caducado.

En el Consola de administración de AWS, Amazon Relational Database Service (Amazon RDS) y Amazon Aurora proporcionan notificaciones sobre las instancias de base de datos que requieren actualizaciones de certificados. Sin embargo, para comprobar estas notificaciones, debe iniciar sesión en cada una de ellas Cuenta de AWS y acceder a la consola de servicio de cada una de ellas. Región de AWS Esta tarea se vuelve más compleja si necesita evaluar la validez de los certificados en muchos de los Cuentas de AWS que se administran como una organización AWS Organizations.

Al aprovisionar la infraestructura como código (IaC) proporcionada en este patrón, puede detectar los certificados de CA que están venciendo para todas las instancias de base de datos de Amazon RDS y Aurora de su organización. Cuenta de AWS AWS La AWS CloudFormationplantilla proporciona una AWS Config regla, una AWS Lambda función y los permisos necesarios. Puede implementarla en una sola cuenta como una pila o puede implementarla en toda la AWS organización como un conjunto de pilas.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Si va a realizar la implementación en una sola Cuenta de AWS:
  - Asegúrese de tener permisos para crear CloudFormation pilas.
  - Actívala AWS Config en la cuenta de destino.
  - (Opcional) Habilitar AWS Security Hub CSPM en la cuenta de destino.

- Si vas a realizar un despliegue en una AWS organización:
  - Asegúrese de tener permisos para crear conjuntos de CloudFormation pilas.
  - Habilite Security Hub CSPM con AWS Organizations la integración.
  - AWS Config Actívela en las cuentas en las que vaya a implementar esta solución.
  - Designe Cuenta de AWS a un administrador delegado de Security Hub CSPM. AWS Config

Limitaciones

- Si va a realizar la implementación en una cuenta individual que no tiene activado el CSPM de Security Hub, puede utilizarla AWS Config para evaluar los resultados.
- Si va a realizar el despliegue en una organización que no tiene un administrador delegado para AWS Config el CSPM de Security Hub, debe iniciar sesión en las cuentas de los miembros individuales para ver los resultados.
- Si solía administrar y AWS Control Tower controlar las cuentas de su organización, implemente el IaC siguiendo este patrón mediante Customizations for (cFCT). AWS Control Tower El uso de la CloudFormation consola provocará desviaciones en la configuración y AWS Control Tower será necesario volver a inscribir las unidades organizativas () o las cuentas gestionadas. OUs
- Algunas Servicios de AWS no están disponibles en todas las versiones. Regiones de AWS Para obtener información sobre la disponibilidad en regiones, consulte la página Service endpoints and quotas y seleccione el enlace correspondiente al servicio.

Arquitectura

Desplegarse en un individuo Cuenta de AWS

El siguiente diagrama de arquitectura muestra el despliegue de los AWS recursos en una sola unidad Cuenta de AWS. Se implementa mediante una CloudFormation plantilla directamente a través de la CloudFormation consola. Si el CSPM de Security Hub está activado, puede ver los resultados en el CSPM AWS Config o en el Security Hub. Si el CSPM de Security Hub no está activado, solo podrá ver los resultados en la AWS Config consola.

En el diagrama se muestran los siguientes pasos:

1. Creas una CloudFormation pila. Esto despliega una función Lambda y AWS Config una regla. Tanto la regla como la función se configuran con los permisos AWS Identity and Access

Management (de IAM) necesarios para publicar las evaluaciones de los recursos en AWS Config los registros.

2. La AWS Config regla funciona en modo de evaluación detectivesca y se ejecuta cada 24 horas.
3. Security Hub CSPM recibe todos los AWS Config resultados.
4. Puede ver los resultados en Security Hub CSPM o en AWS Config, según la configuración de la cuenta.

Implementar en una organización AWS

El siguiente diagrama muestra la evaluación de la caducidad de los certificados en varias cuentas que se administran mediante AWS Organizations y AWS Control Tower. La CloudFormation plantilla se implementa a través de cFCT. Los resultados de la evaluación se centralizan en Security Hub CSPM en la cuenta de administrador delegado. El AWS CodePipeline flujo de trabajo que se muestra en el diagrama muestra los pasos básicos que se producen durante la implementación del cFCT.

En el diagrama se muestran los siguientes pasos:

1. Según la configuración de cFCT, en la cuenta de administración, se envía el IaC a un AWS CodeCommit repositorio o se carga un archivo comprimido (ZIP) del iAC a un bucket de Amazon Simple Storage Service (Amazon S3).
2. La canalización cFCT descomprime el archivo, ejecuta las comprobaciones de cfn-nag (GitHub) y lo despliega como un conjunto de pilas. CloudFormation
3. Según la configuración especificada en el archivo de manifiesto de cFCT, CloudFormation StackSets despliega las pilas en cuentas individuales o especificadas. OUs Esto despliega una función Lambda y AWS Config una regla en las cuentas de destino. Tanto la regla como la función se configuran con los permisos de IAM necesarios para publicar las evaluaciones de los recursos y los AWS Config registros.
4. La AWS Config regla funciona en modo de evaluación detectivesca y se ejecuta cada 24 horas.
5. AWS Config reenvía todos los resultados a Security Hub CSPM.
6. Los resultados del CSPM de Security Hub se agregan a la cuenta del administrador delegado.
7. Puede ver los resultados en Security Hub CSPM en la cuenta de administrador delegado.

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y administrarlos a lo largo de su ciclo de vida en Cuentas de AWS todas las regiones.
- AWS Configproporciona una vista detallada de sus recursos Cuenta de AWS y de cómo están configurados. Le ayuda a identificar cómo se relacionan los recursos entre sí y cómo han cambiado sus configuraciones a lo largo del tiempo. Una AWS Config regla define los parámetros de configuración ideales para un recurso y AWS Config puede evaluar si AWS los recursos cumplen las condiciones de las reglas.
- AWS Control Towerle ayuda a configurar y administrar un entorno de AWS múltiples cuentas, siguiendo las prácticas recomendadas prescriptivas. Las personalizaciones de AWS Control Tower (cFCT) te ayudan a personalizar tu AWS Control Tower landing zone y a mantenerte alineado con las AWS mejores prácticas. Las personalizaciones se implementan con CloudFormation plantillas y políticas de control de servicios (). SCPs
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar múltiples cuentas Cuentas de AWS en una organización que puede crear y administrar de forma centralizada.
- AWS Security Hub CSPMproporciona una visión completa del estado de su seguridad en AWS. También le ayuda a comparar su AWS entorno con los estándares y las mejores prácticas del sector de la seguridad.

Otras herramientas

- Python es un lenguaje de programación informático de uso general.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub Detect Amazon RDS con certificados de CA vencidos.

Prácticas recomendadas

Le recomendamos que siga las prácticas recomendadas en los siguientes recursos:

- Prácticas recomendadas para unidades organizativas con AWS Organizations(blog sobre operaciones y migraciones AWS en la nube)
- Guía para establecer una base inicial mediante AWS Control Tower el uso de AWS (biblioteca de AWS soluciones)
- Guía para crear y modificar AWS Control Tower recursos (AWS Control Tower documentación)
- Consideraciones sobre el despliegue de CFCT (AWS Control Tower documentación)

Epics

Revisión de la solución y el código

Tarea	Descripción	Habilidades requeridas
Determine su estrategia de implementación.	Revise la solución y el código para determinar cómo los implementará en su AWS entorno. Determine si la implementará en una sola cuenta o en una AWS organización.	Propietario de la aplicación, AWS general
Clonar el repositorio.	Introduzca el siguiente comando para clonar el repositorio de detección de instancias de Amazon RDS con certificados CA que vencen. `git clone https://github.com/aws-samples/config-rds-ca-expiry.git`	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Valide la versión de Python.	1. Vaya al directorio de nivel superior del repositorio clonado. `cd config-rds-ca-expiry` 2. Abre config-rds-ca-expiry.yaml. 3. En el recurso de `CertExpirationCheckLambdaFunction`, confirme que la versión de Python es compatible con su objetivo de Regiones de AWS. De forma predeterminada, esta función usa Python 3.12. Para más información, consulte AWS Lambda adds support for Python 3.12. Si es necesario, actualice la versión de Python. 4. Guarda y cierra .yamlconfig-rds-ca-expiry.	Desarrollador de aplicaciones, propietario de la aplicación

Implementar la solución

Tarea	Descripción	Habilidades requeridas
Implemente la plantilla CloudFormation .	Implemente la CloudFormation plantilla en su AWS entorno. Realice una de las siguientes acciones:	Desarrollador de aplicaciones, administrador de AWS, AWS general

Tarea	Descripción	Habilidades requeridas
	• Si va a realizar la implement ación en una sola Cuenta de AWS unidad, siga las instrucciones de Cómo crear una pila. • Si vas a realizar el despliegue en una organización que no está gestionada por AWS Control Tower, sigue las instrucci ones de Cómo crear un conjunto de pilas. • Si vas a realizar el despliegue en una organización gestionada por AWS Control Tower, consulta las instrucciones de la sección Crea tus propias personalizaciones.	
Comprobar la implementación.	En la CloudFormation consola, compruebe que la pila o el conjunto de pilas se hayan desplegado correctamente.	Administrador de AWS, propietario de la aplicación

Revisión de resultados

Tarea	Descripción	Habilidades requeridas
Vea los resultados de la AWS Config regla.	En Security Hub CSPM, haga lo siguiente para ver una lista de las conclusiones individua les:	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	1. Abra la consola CSPM de Security Hub. 2. En el panel de navegación, seleccione Resultados. 3. En el cuadro Agregar filtros, agregue los siguientes filtros: • El estado de conformidad es `FAILED` • El título es `rds-has-expiring-ca` 4. Seleccione Aplicar. En Security Hub CSPM, haga lo siguiente para ver una lista del total de hallazgos agrupados por: Cuenta de AWS 1. Abra la consola CSPM de Security Hub. 2. En el panel de navegación, elija Hallazgos. 3. Seleccione Crear hallazgo. 4. Para seleccionar el atributo de agrupación para el conocimiento: a. Seleccione el cuadro de búsqueda para ver las opciones de filtro. b. Elija Group by (Agrupar por).	

Tarea	Descripción	Habilidades requeridas
	c. Seleccione AwsAccountId. d. Seleccione Aplicar. 5. En el cuadro Agregar filtros, agregue los siguientes filtros: • El título es `rds-has-expiring-ca` • El estado de conformidad es `FAILED` 6. Seleccione Crear hallazgo. 7. Escriba un Nombre del hallazgo y elija Crear hallazgo. En AWS Config, para ver una lista de las conclusiones, siga las instrucciones que se indican en la documentación sobre la visualización de la información de conformidad y los resultados de la AWS Config evaluación.	

Resolución de problemas

Problema	Solución
CloudFormation se produce un error al crear o eliminar un conjunto de pilas	Cuando AWS Control Tower se despliega, impone las barreras de protección necesarias y asume el control de los AWS Config agregadores y las reglas. Esto incluye evitar cualquier

Problema	Solución
	alteración directa. CloudFormation Para implementar o eliminar correctamente esta CloudFormation plantilla, incluidos todos los recursos asociados, debe utilizar cFCT.
cFct no puede eliminar la plantilla CloudFormation	Si la CloudFormation plantilla persiste incluso después de realizar los cambios necesarios en el archivo de manifiesto y eliminar los archivos de plantilla, confirme que el archivo de manifiesto contiene el `enable_stack_set_deletion` parámetro y que el valor está establecido en. `false` Para más información, consulte Eliminación de un conjunto de pilas en la documentación de CfCT.

Recursos relacionados

- Utilización SSL/TLS para cifrar una conexión a una instancia de base de datos o un clúster (documentación de Amazon RDS)
- AWS Config Reglas personalizadas (documentación)AWS Config

Genere dinámicamente una política de IAM con IAM Access Analyzer mediante Step Functions

Thomas Scott, Koen van Blijderveen, Adil El Kanabi y Rafal Pawlaszek, Amazon Web Services

Resumen

El privilegio mínimo es la práctica recomendada de seguridad que consiste en conceder los permisos mínimos necesarios para realizar una tarea. Implementar el acceso con privilegios mínimos en una cuenta de Amazon Web Services (AWS) que ya está activa puede resultar difícil, ya que no se quiere impedir que los usuarios realicen sus tareas laborales cambiando sus permisos de forma involuntaria. Antes de poder implementar cambios en las políticas AWS Identity and Access Management (de IAM), debe comprender las acciones y los recursos que están realizando los usuarios de la cuenta.

Este patrón está diseñado para ayudarle a aplicar el principio del acceso con privilegio mínimo, sin bloquear ni ralentizar la productividad del equipo. En él se describe cómo utilizar el analizador de acceso de IAM y AWS Step Functions cómo generar de forma dinámica una política de up-to-date IAM para su función, en función de las acciones que se estén realizando actualmente en la cuenta. La nueva política está diseñada para permitir la actividad actual, pero eliminar cualquier privilegio elevado e innecesario. Puede personalizar la política generada definiendo reglas de autorización y denegación, y la solución integra sus reglas personalizadas.

Este patrón incluye opciones para implementar la solución con AWS Cloud Development Kit (AWS CDK) un HashiCorp CDK para Terraform (CDKTF). A continuación, puede asociar la nueva política al rol mediante una canalización de integración y entrega continuas (CI/CD). Si tiene una arquitectura de varias cuentas, puede implementar esta solución en cualquier cuenta en la que desee generar políticas de IAM actualizadas para las funciones, lo que aumentará la seguridad de todo su entorno. Nube de AWS

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS con una AWS CloudTrail ruta habilitada.
- Permisos IAM para lo siguiente:

  - Cree e implemente flujos de trabajo de Step Functions. Para obtener más información, consulte Acciones, recursos y claves de condición de AWS Step Functions (documentación de Step Functions).
  - Crea AWS Lambda funciones. Para obtener más información, consulte Rol de ejecución y permisos de usuario (documentación de Lambda).
  - Crear roles de IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un usuario de IAM (documentación de IAM).
- npm instalado. Para obtener más información, consulte Descargar e instalar Node.js y npm (documentación de npm).
- Si va a implementar esta solución con AWS CDK (opción 1):
  - AWS CDK Kit de herramientas, instalado y configurado. Para obtener más información, consulte Instalar el AWS CDK (AWS CDK documentación).
- Si va a implementar esta solución con CDKTF (opción 2):
  - Ha instalado y configurado CDKTF. Para obtener más información, consulte Instalar el CDK para Terraform (documentación de CDKTF).
  - Terraform, instalado y configurado. Para obtener más información, consulte Introducción (documentación de Terraform).
- AWS Command Line Interface (AWS CLI) instalado y configurado localmente para su Cuenta de AWS. Para obtener más información, consulte Instalación o actualización de la última versión de la AWS CLI (AWS CLI documentación).

Limitaciones

- Este patrón no aplica la nueva política de IAM al rol. Al final de esta solución, la nueva política de IAM se almacena en un AWS CodeCommit repositorio. Puedes usar una CI/CD canalización para aplicar políticas a los roles de tu cuenta.

Arquitectura

Arquitectura de destino

1. Una regla de EventBridge eventos de Amazon programada regularmente inicia un flujo de trabajo de Step Functions. Este programa de regeneración se define como parte de la configuración de esta solución.

2. En el flujo de trabajo de Step Functions, una función Lambda genera los intervalos de fechas que se utilizarán al analizar la actividad de la cuenta en los CloudTrail registros.
3. El siguiente paso del flujo de trabajo llama a la API de IAM Access Analyzer para empezar a generar la política.
4. Con el nombre de recurso de Amazon (ARN) del rol que especificó durante la configuración, IAM Access Analyzer analiza los CloudTrail registros para detectar actividad dentro de la tasa de fechas especificada. En función de la actividad, IAM Access Analyzer genera una política de IAM que solo permite las acciones y los servicios que utilice el rol durante el intervalo de fechas especificado. Cuando se completa este paso, se genera un identificador de trabajo.
5. El siguiente paso del flujo de trabajo comprueba el ID del trabajo cada 30 segundos. Cuando se detecta el identificador de trabajo, este paso lo utiliza para llamar a la API de IAM Access Analyzer y recuperar la nueva política de IAM. IAM Access Analyzer devuelve la política como un archivo JSON.
6. El siguiente paso del flujo de trabajo coloca el archivo <IAM role name>/policy.json en un bucket de Amazon Simple Storage Service (Amazon S3). Defina este bucket de S3 como parte de la configuración de esta solución.
7. Una notificación de eventos de Amazon S3 inicia una función de Lambda.
8. La función Lambda recupera la política del bucket de S3, integra las reglas personalizadas que defina en los archivos allow.json y deny.json y, a continuación, envía la política actualizada a. CodeCommit Usted define el CodeCommit repositorio, la rama y la ruta de la carpeta como parte de la configuración de esta solución.

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir y aprovisionar la Nube de AWS infraestructura en el código.
- AWS CDK Toolkit es un kit de desarrollo en la nube de línea de comandos que le ayuda a interactuar con su AWS Cloud Development Kit (AWS CDK) aplicación.
- AWS CloudTraille ayuda a auditar la gobernanza, el cumplimiento y el riesgo operativo de su Cuenta de AWS empresa.
- AWS CodeCommit es un servicio de control de versiones que permite almacenar y administrar repositorios de Git de forma privada, sin necesidad de administrar su propio sistema de control de origen.

- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar Servicios de AWS mediante comandos en su shell de línea de comandos.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos. Este patrón utiliza el analizador de acceso de IAM, una función de IAM, para analizar CloudTrail los registros e identificar las acciones y los servicios que ha utilizado una entidad de IAM (usuario o rol) y, a continuación, generar una política de IAM basada en esa actividad.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Step Functionses un servicio de organización sin servidor que le ayuda a combinar AWS Lambda funciones y otras para crear aplicaciones esenciales para la empresa. Servicios de AWS En este patrón, utiliza las integraciones de servicios de AWS SDK en Step Functions para llamar a las acciones de la API de servicio desde su flujo de trabajo.

Otras herramientas

- CDK para Terraform (CDKTF) le ayuda a definir la infraestructura como código (IaC) mediante el uso de idiomas de programación comunes, como Python y Typescript.
- Lerna es un sistema de compilación para administrar y publicar varios TypeScript paquetes JavaScript o paquetes del mismo repositorio.
- Node.js es un entorno de JavaScript ejecución basado en eventos diseñado para crear aplicaciones de red escalables.
- npm es un registro de software que se ejecuta en un entorno Node.js y se utiliza para compartir o tomar prestados paquetes y administrar la implementación de paquetes privados.

Repositorio de código

El código de este patrón está disponible en el repositorio del generador de políticas de roles de GitHub Automated IAM Access Analyzer.

Epics

Preparación para la implementación

Tarea	Descripción	Habilidades requeridas
Clone el repositorio.	El siguiente comando clona el repositorio del generador de políticas de roles () de Automated IAM Access Analyzer. GitHub `git clone https://github.com/aws-samples/automated-iam-access-analyzer.git`	Desarrollador de aplicaciones
Instale Lerna.	El siguiente comando instala Lerna. `npm i -g lerna`	Desarrollador de aplicaciones

Configure las dependencias.	Ingrese el siguiente comando para instalar las dependencias del repositorio.
	`cd automated-iam-access-analyzer/`
	`npm install && npm run bootstrap`
		Desarrollador de aplicaciones

Crear el código.	El siguiente comando prueba, compila y prepara los paquetes zip de las funciones de Lambda.
	`npm run test:code`
	`npm run build:code`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`npm run pack:code`	
Construya los constructos.	El siguiente comando crea la infraestructura sintetizando las aplicaciones, tanto para CDKTF como para CDKTF. AWS CDK `npm run build:infra`	
Configure todos los permisos personalizados.	En la carpeta repo del repositorio clonado, edite los archivos allow.json y deny.json para definir los permisos personalizados para el rol. Si los archivos allow.jso n y deny.json contienen el mismo permiso, se aplica el permiso de denegación.	Administrador de AWS, desarrollador de aplicaciones

Opción 1: Implemente la solución mediante AWS CDK

Tarea	Descripción	Habilidades requeridas
Implemente la AWS CDK pila.	El siguiente comando despliega la infraestructura mediante AWS CloudForm ation. Defina los siguientes parámetros: • `<NAME_OF_ROLE>` : el ARN del rol de IAM para el que está creando una nueva política.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	• <TRAIL_ARN> — El ARN del registro en el que CloudTrail se almacena la actividad del rol.
	• <CRON_EXPRESSION_TO_RUN_SOLUTION> : la expresión Cron que define el programa de regeneración de la política. El flujo de trabajo de Step Functions se ejecuta según esta programación.
	• <TRAIL_LOOKBACK> : el período, en días, para echar un vistazo a la trayectoria al evaluar los permisos de los roles.
	
	`cd infra/cdk`
	`cdk deploy –-parameters roleArn=<NAME_OF_ROLE> \`
	`–-parameters trailArn=<TRAIL_ARN> \`
	`--parameters schedule=<CRON_EXPRESSION_TO_RUN_SOLUTION> \`
	`[ --parameters trailLookBack=<TRAIL_LOOKBACK> ]`	

Tarea	Descripción	Habilidades requeridas
	Note Los corchetes indican los parámetros opcionales.	
(Opcional) Espere a que aparezca la nueva política.	Si el registro no contiene una cantidad razonable de actividad histórica para el rol, espere hasta que esté seguro de que hay suficiente actividad registrada como para que IAM Access Analyzer genere una política precisa. Si el rol ha estado activo en la cuenta durante un período de tiempo suficiente, es posible que este período de espera no sea necesario.	Administrador de AWS
Revise manualmente la política generada.	En tu CodeCommit repositor io, revisa el archivo.json <ROLE_ARN>generado para confirmar que los permisos de autorización y denegación son adecuados para el rol.	Administrador de AWS

Opción 2: implementar la solución mediante CDKTF

Tarea	Descripción	Habilidades requeridas
Sintetice la plantilla Terraform.	El siguiente comando sintetiza la plantilla de Terraform.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`lerna exec cdktf synth --scope @aiaa/tfm`	

Tarea	Descripción	Habilidades requeridas
Implementar la plantilla Terraform.	El siguiente comando navega hasta el directorio que contiene la infraestructura definida por CDKTF. `cd infra/cdktf` El siguiente comando despliega la infraestructura en el destino. Cuenta de AWS Defina los siguientes parámetros: • `<account_ID>` : el ID de la cuenta de destino. • `<region>`- El objetivo Región de AWS. • `<selected_role_ARN>` : el ARN del rol de IAM para el que está creando una nueva política. • `<trail_ARN>` — El ARN del registro en el que CloudTrail se almacena la actividad del rol. • `<schedule_expression>` : la expresión Cron que define el programa de regeneración de la política. El flujo de trabajo de Step Functions se ejecuta según esta programación. • `<trail_look_back>` : el período, en días, para echar	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	un vistazo a la trayectoria al evaluar los permisos de los roles. `TF_VAR_accountId=<account_ID> \ TF_VAR_region=<region> \ TF_VAR_roleArns=<selected_role_ARN> \ TF_VAR_trailArn=<trail_ARN> \ TF_VAR_schedule=<schedule_expression> \ [ TF_VAR_trailLookBack=<trail_look_back> ] \ cdktf deploy` **Note** Los corchetes indican los parámetros opcionales.	

Tarea	Descripción	Habilidades requeridas
(Opcional) Espere a que aparezca la nueva política.	Si el registro no contiene una cantidad razonable de actividad histórica para el rol, espere hasta que esté seguro de que hay suficiente actividad registrada como para que IAM Access Analyzer genere una política precisa. Si el rol ha estado activo en la cuenta durante un período de tiempo suficiente, es posible que este período de espera no sea necesario.	Administrador de AWS
Revise manualmente la política generada.	En tu CodeCommit repositor io, revisa el archivo.json <ROLE_ARN>generado para confirmar que los permisos de autorización y denegación son adecuados para el rol.	Administrador de AWS

Recursos relacionados

AWS resources

- Puntos de conexión y cuotas de IAM Access Analyzer
- Configurar el AWS CLI
- Empezando con el AWS CDK
- Aplicar permisos de privilegios mínimos

Otros recursos

- CDK para Terraform (sitio web de Terraform)

Habilita Amazon de GuardDuty forma condicional mediante plantillas AWS CloudFormation

Ram Kandaswamy, Amazon Web Services

Resumen

AWS CloudFormation, una herramienta de infraestructura como código (IaC), le ayuda a gestionar AWS los recursos mediante despliegues basados en plantillas. CloudFormation se suele utilizar para gestionar los recursos. AWS Usarlo para habilitar Servicios de AWS, como Amazon GuardDuty, puede presentar desafíos únicos. GuardDuty es un servicio de detección de amenazas que monitorea continuamente sus Cuentas de AWS actividades maliciosas y comportamientos no autorizados. A diferencia de los recursos típicos, que se pueden crear varias veces, GuardDuty es un servicio que debe habilitarse una vez por cuenta y Región de AWS. CloudFormation Las condiciones tradicionales solo admiten comparaciones de valores estáticos, lo que dificulta la comprobación del estado actual de servicios como GuardDuty. Si intentas activar la conexión a GuardDuty través CloudFormation de una cuenta que ya está activa, se produce un error en la implementación de la pila. Esto puede crear desafíos operativos para los DevOps equipos que administran entornos con varias cuentas.

Este patrón presenta una solución a este desafío. Utiliza recursos CloudFormation personalizados respaldados por AWS Lambdafunciones para realizar comprobaciones de estado dinámicas. La lógica condicional GuardDuty solo se activa si aún no está habilitada. Utiliza las salidas de la pila para registrar el GuardDuty estado para futuras referencias.

Si sigue este patrón, puede automatizar las GuardDuty implementaciones en toda su AWS infraestructura y, al mismo tiempo, mantener las operaciones de CloudFormation apilado limpias y predecibles. Este enfoque es particularmente valioso para las organizaciones que:

- Administrar múltiples Cuentas de AWS mediante IaC
- Implementación de servicios de seguridad a escala
- Requiere despliegues de infraestructura idempotentes
- Automatizar los despliegues de servicios de seguridad

Requisitos previos y limitaciones

Requisitos previos

- ¿Un activo Cuenta de AWS
- Un rol AWS Identity and Access Management (IAM) que tiene permisos para crear, actualizar y eliminar pilas CloudFormation
- AWS Command Line Interface (AWS CLI), instalado y configurado

Limitaciones

Si se GuardDuty ha desactivado manualmente para una Cuenta de AWS o Región de AWS, este patrón no se habilita GuardDuty para esa cuenta o región de destino.

Arquitectura

Pila de tecnología de destino

El patrón utiliza CloudFormation la infraestructura como código (IaC). Utiliza un recurso CloudFormation personalizado respaldado por una función Lambda para lograr la capacidad de habilitación dinámica de servicios.

Arquitectura de destino

El siguiente diagrama de arquitectura de alto nivel muestra el proceso de habilitación GuardDuty mediante la implementación de una plantilla: CloudFormation

1. Se implementa una CloudFormation plantilla para crear una CloudFormation pila.
2. La pila crea un rol de IAM y una función de Lambda.
3. La función de Lambda asume el rol de IAM.
4. Si aún no GuardDuty está habilitada en el destino Cuenta de AWS, la función Lambda la habilita.

Automatización y escala

Puede usar la AWS CloudFormation StackSet función para extender esta solución a múltiples Cuentas de AWS y Regiones de AWS. Para obtener más información, consulte Trabajar con AWS CloudFormation StackSets él en la CloudFormation documentación.

Tools (Herramientas)

- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que te ayuda a interactuar Servicios de AWS mediante los comandos de tu shell de línea de comandos.

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y administrarlos a lo largo de su ciclo de vida en Cuentas de AWS todas las regiones.
- Amazon GuardDuty es un servicio de supervisión continua de la seguridad que analiza y procesa los registros para identificar actividades inesperadas y potencialmente no autorizadas en su AWS entorno.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

Epics

Cree la CloudFormation plantilla e implemente la pila

Tarea	Descripción	Habilidades requeridas
Guarde el código en Amazon S3.	1. Copia el código de Python en la sección de información adicional de este patrón. 2. Pegue el código en un editor de texto. 3. Guarde el archivo como `index.py`. 4. Cargue el archivo en un bucket de Amazon Simple Storage Service (Amazon S3). Para más instrucciones, consulte Cargar objetos en la documentación de Amazon S3.	AWS DevOps
Cree la CloudFormation plantilla.	1. Abra la consola de CloudFormation .	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	2. En el panel de navegación izquierdo, elija Infrastructure Composer. 3. Si no ve un lienzo en blanco, cree un proyecto nuevo. 4. Arrastra y suelta una AWS Lambda función en el lienzo. 5. En la vista de plantilla , compruebe que estén presentes una función Lambda y un grupo de registros. 6. Modifique `Runtime` la función Lambda a la última versión de Python. 7. Valide que la `Handler` propiedad tenga un valor de `index.lambda_handler.` 8. Configure la `CodeUri` propiedad para que sea la ubicación de Amazon S3 en la que cargó el código Python. Un valor de ejemplo es `s3://amzn-s3-demo-bucket/key-name` . 9. Añada una `Policies` propiedad para el recurso. Siga las prácticas recomenda	

Tarea	Descripción	Habilidades requeridas
	das de seguridad para proporcionar permisos de acceso con privilegi os mínimos que permitan CloudFormation GuardDuty realizar acciones. Por ejemplo, puede utilizar la política `AWSLambda Execute` gestionada para los registros y una personalizada `iam:Creat eServiceLinkedRole` para GuardDuty. 10. Para añadir una definición de recurso personalizada al fragmento, navegue hasta la vista de plantilla. `CheckResourceExist: Type: 'Custom:: LambdaCustomResour ce' Properties: ServiceToken: ! GetAtt Function.Arn` 11. Guarde la plantilla como. `sample.yaml`	

Tarea	Descripción	Habilidades requeridas

Crea la CloudFormation pila.	1. En AWS CLI, ingresa el siguiente comando. Esto crea una nueva CloudFormation pila utilizando el `sample.yaml` archivo. Para obtener más información, consulte Crear una pila en la CloudFormation documentación.
	`aws cloudformation create-stack \ --stack-name guardduty-cf-stack \ --template-body file://sample.yaml`
	2. Confirme que el siguiente valor aparezca en el AWS CLI, lo que indica que la pila se ha creado correctamente. El tiempo necesario para crear la pila puede variar.
	`"StackStatus": "CREATE_COMPLETE",`
		AWS DevOps

Valide que GuardDuty esté habilitado para Cuenta de AWS.	1. Inicie sesión en la GuardDuty consola Consola de administración de AWS y ábrala. 2. Compruebe que el GuardDuty servicio esté activado.	Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure cuentas o regiones adicionales.	Según sea necesario para su caso de uso, utilice la CloudFormation StackSet función para extender esta solución a múltiples Cuentas de AWS y Regiones de AWS. Para obtener más información, consulte Trabajar con AWS CloudFormation StackSets ella en la CloudFormation documentación.	Administrador de la nube, administrador de AWS

Recursos relacionados

Referencias

- AWS CloudFormation documentación
- AWS Lambda referencia de tipo de recurso
- CloudFormation tipo de recurso: :IAM AWS: :Role
- CloudFormation tipo de recurso:: AWS: :Detector GuardDuty
- Cuatro formas de recuperar cualquier propiedad AWS del servicio mediante AWS CloudFormation (entrada de blog)

Tutoriales y videos

- Simplificación de la administración de la infraestructura con AWS CloudFormation (Tutorial)
- Usa Amazon GuardDuty y protege AWS Security Hub CSPM varias cuentas (AWS re:Invent 2020)
- Mejores prácticas de creación AWS CloudFormation(re:Invent 2019)AWS
- Detección de amenazas en AWS: una introducción a Amazon GuardDuty (AWS re:inForce 2019)

Información adicional

Código Python

```
import boto3
import os
import json
from botocore.exceptions import ClientError
import cfnresponse
guardduty=boto3.client('guardduty')
cfn=boto3.client('cloudformation')
def lambda_handler(event, context):
    print('Event: ', event)
    if 'RequestType' in event:
      if event['RequestType'] in ["Create","Update"]:
          enabled=False
          try:
            response=guardduty.list_detectors()
            if "DetectorIds" in response and len(response["DetectorIds"])>0:
              enabled="AlreadyEnabled"
            elif "DetectorIds" in response and len(response["DetectorIds"])==0:
              cfn_response=cfn.create_stack(
                StackName='guardduty-cfn-stack',
                TemplateBody='{ "AWSTemplateFormatVersion": "2010-09-09",
   "Description": "Guard duty creation template",    "Resources":
 { "IRWorkshopGuardDutyDetector": {  "Type": "AWS::GuardDuty::Detector",
 "Properties": {   "Enable": true  }   } } }'
                )
              enabled="True"
          except Exception as e:
              print("Exception: ",e)
          responseData = {}
          responseData['status'] = enabled
          cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,
 "CustomResourcePhysicalID" )
      elif event['RequestType'] == "Delete":
          cfn_response=cfn.delete_stack(
                  StackName='guardduty-cfn-stack')
          cfnresponse.send(event, context, cfnresponse.SUCCESS, {})
```

Habilitar el cifrado transparente de datos en Amazon RDS para SQL Server

Ranga Cherukuri, Amazon Web Services

Resumen

Este patrón describe cómo implementar el cifrado transparente de datos (TDE) en Amazon Relational Database Service (Amazon RDS) para SQL Server con el fin de cifrar los datos en reposo.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Instancia de base de datos de Amazon RDS para SQL Server

Versiones de producto

Actualmente, Amazon RDS admite TDE para las siguientes versiones y ediciones de SQL Server:

- SQL Server 2016 Enterprise Edition
- SQL Server 2017 Enterprise Edition
- SQL Server 2019: Standard y Enterprise Editions
- SQL Server 2022: Standard y Enterprise Editions

Para obtener la información más reciente sobre las versiones y ediciones compatibles, consulte Compatibilidad con cifrado de datos transparente en SQL Server en la documentación de Amazon RDS.

Arquitectura

Pila de tecnología

- Amazon RDS para SQL Server

Arquitectura

Tools (Herramientas)

- Microsoft SQL Server Management Studio (SSMS) es un entorno integrado para administrar infraestructuras de SQL Server. Proporciona una interfaz de usuario y un grupo de herramientas con editores de scripts enriquecidos que interactúan con SQL Server.

Epics

Cree un conjunto de opciones en la consola de Amazon RDS

Tarea	Descripción	Habilidades requeridas
Abra la consola de Amazon RDS.	Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon RDS.	Desarrollador, Administrador de base de datos
Crear un grupo de opciones.	En el panel de navegación, elija Opciñon grupos, Crear grupo. Seleccione sqlserver -ee como motor de base de datos y, a continuación, seleccione la versión del motor.	Desarrollador, Administrador de base de datos
Agregue la opción TRANSPARENT_DATA_ENCRYPTION.	Edite el conjunto de opciones que ha creado y añada la opción denominada `TRANSPARENT_DATA_ENCRYPTION` .	Desarrollador, Administrador de base de datos

Asociar el grupo de opciones a la instancia de base de datos

Tarea	Descripción	Habilidades requeridas
Elija la instancia de base de datos.	En la consola de Amazon RDS, en el panel de navegación, elija Bases de datos y, a continuación, seleccione la instancia de base de datos que desea asociar con el grupo de opciones.	Desarrollador, Administrador de base de datos
Asocie la instancia de base de datos con el grupo de opciones.	Seleccione Modificar y, a continuación, use la configuración del conjunto de opciones para asociar la instancia de base de datos de SQL Server con el conjunto de opciones que creó anteriormente.	Desarrollador, Administrador de base de datos
Aplique los cambios.	Aplique los cambios inmediatamente o durante la siguiente ventana de mantenimiento, según desee.	Desarrollador, Administrador de base de datos

Obtenga el nombre del certificado.	Obtenga el nombre predeterminado del certificado ejecutando la siguiente consulta.
	`USE [master]`
	`GO`
	`SELECT name FROM sys.certificates WHERE name LIKE 'RDSTDECertificate%'`
	`GO`
		Desarrollador, Administrador de base de datos

Cree la clave de cifrado de la base de datos

Tarea	Descripción	Habilidades requeridas
Conéctese a la instancia de base de datos de Amazon RDS para SQL Server mediante SSMS.	Para obtener instrucciones, consulte Uar SSMS en la documentación de Microsoft.	Desarrollador, Administrador de base de datos

Cree la clave de cifrado de la base de datos usando el certificado predeterminado.	Crear una clave de encriptación de la base de datos utilizando el nombre del certificado por defecto que obtuvo anteriormente. Ejecute la siguiente consulta de T-SQL para crear una clave de cifrado de base de datos. Puede especificar el algoritmo AES_256 en lugar de AES_128.
	`USE [Databasename]`
	`GO`
	`CREATE DATABASE`
	`ENCRYPTION KEY`
	`WITH ALGORITHM = AES_128`
	`ENCRYPTION BY SERVER`
	`CERTIFICATE [certificatename]`
	`GO`
		Desarrollador, Administrador de base de datos

Habilite el cifrado en la base de datos.	Ejecute la siguiente consulta T-SQL para habilitar el cifrado de base de datos.
	`ALTER DATABASE [Database Name]`
	`SET ENCRYPTION ON`
		Desarrollador, Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`GO`	
Compruebe el estado del cifrado.	Ejecute la siguiente consulta T-SQL para comprobar el estado del cifrado. `SELECT DB_NAME(database_id) AS DatabaseName, encryption_state, percent_complete FROM sys.dm_database_encryption_keys`	Desarrollador, Administrador de base de datos

Recursos relacionados

- Compatibilidad con el Cifrado de datos transparente en SQL Server (documentación de Amazon RDS)
- Trabajo con conjuntos de opciones (documentación de Amazon RDS)
- Cómo modificar una instancia de base de datos de Amazon RDS (documentación de Amazon RDS)
- Cifrado de datos transparente para SQL Server (documentación de Microsoft)
- Uso de SSMS (documentación de Microsoft)

Supervisar y corregir la eliminación programada de las claves de AWS KMS

Mikesh Khanal y Ramya Pulipaka, Amazon Web Services

Resumen

En la nube de Amazon Web Services (AWS), eliminar una clave de AWS Key Management Service (AWS KMS) puede provocar la pérdida de datos. El borrado elimina el material de la clave y todos los metadatos asociados a la clave de AWS KMS, y es irreversible. Una vez eliminada una clave de AWS KMS, ya no podrá descifrar los datos que estaban cifrados bajo esa clave de AWS KMS, por lo que no se podrán recuperar esos datos.

Este patrón configura la supervisión, con notificaciones cuando una aplicación o un usuario programa la eliminación de una clave de AWS KMS. Si recibe una notificación, puede cancelar la eliminación de la clave de AWS KMS y reconsiderar su decisión de eliminarla. El patrón utiliza el manual de automatización de AWS Systems Manager AWSConfigRemediation-CancelKeyDeletionpara facilitar la cancelación de la eliminación de una clave de AWS KMS.

> **Note**
>
> La CloudFormation plantilla del patrón debe implementarse en todas las regiones de AWS en las que desee supervisar la eliminación de las claves de AWS KMS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Comprender los siguientes servicios de AWS:
  - Amazon EventBridge
  - AWS KMS
  - Amazon Simple Notification Service (Amazon SNS)
  - AWS Systems Manager

Limitaciones

- Cualquier personalización de la solución requiere conocer las CloudFormation plantillas de AWS y los servicios de AWS utilizados en este patrón.
- Actualmente, esta solución utiliza el bus de eventos predeterminado y se puede personalizar de acuerdo con los requisitos. Para obtener más información sobre el bus de eventos personalizado, consulte la documentación de AWS.

Arquitectura

Pila de tecnología de destino

- Amazon EventBridge
- AWS KMS
- Amazon SNS
- AWS Systems Manager
- Automatización mediante lo siguiente:
  - Interfaz de la línea de comandos de AWS (AWS CLI) o AWS SDK
  - CloudFormation Pila de AWS

Arquitectura de destino

1. La eliminación de una clave de AWS KMS está programada.
2. El evento de eliminación programada se evalúa mediante una regla. EventBridge
3. La EventBridge regla aborda el tema de Amazon SNS.
4. La EventBridge regla inicia la automatización y los manuales de ejecución de Systems Manager.
5. Los manuales de procedimientos cancelan la eliminación.

Automatización y escala

La CloudFormation pila despliega todos los recursos y servicios necesarios para que esta solución funcione. El patrón se puede ejecutar de forma independiente en una sola cuenta o se puede ejecutar mediante AWS CloudFormation StackSets para varias cuentas independientes o una organización.

```
aws cloudformation create-stack --stack-name  <stack-name>\
```

```
    --template-body file://<Full-Path-of-file> \
    --parameters ParameterKey=,ParameterValue= \
    --capabilities CAPABILITY_NAMED_IAM
```

Tools (Herramientas)

Herramientas

- AWS CloudFormation: AWS CloudFormation es un servicio que le ayuda a modelar y configurar sus recursos de Amazon Web Services para que pueda dedicar menos tiempo a gestionar esos recursos y más a centrarse en las aplicaciones que se ejecutan en AWS. Puede usar una CloudFormation plantilla para crear pilas en una cuenta de AWS en una región de AWS. La plantilla describe todos los recursos de AWS que desea y los CloudFormation aprovisiona y configura por usted.
- AWS CLI: la interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de líneas de comandos.
- Amazon EventBridge: Amazon EventBridge es un servicio de bus de eventos sin servidor que conecta sus aplicaciones con datos de diversas fuentes. EventBridge ofrece un flujo de datos en tiempo real desde sus propias aplicaciones y servicios de AWS, y dirige esos datos a objetivos como AWS Lambda. EventBridge simplifica el proceso de creación de arquitecturas basadas en eventos.
- AWS KMS – AWS Key Management Service (AWS KMS) es un servicio administrado para crear y controlar las claves de AWS KMS, las claves de cifrado que se utilizan para cifrar sus datos.
- AWS SDKs: las herramientas de AWS se incluyen SDKs para que pueda desarrollar y administrar aplicaciones en AWS en el lenguaje de programación que prefiera.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio administrado con el que se ofrece la entrega de mensajes de los publicadores a los suscriptores (también conocido como productores y consumidores). Los publicadores se comunican de forma asíncrona con los suscriptores mediante el envío mensajes a un tema, que es un punto de acceso lógico y un canal de comunicación.
- AWS Systems Manager: AWS Systems Manager es un servicio que puede utilizar para ver y controlar su infraestructura en AWS. Mediante la consola de Systems Manager, puede automatizar las tareas operativas en sus recursos de AWS. Systems Manager le ayuda a mantener la seguridad y la conformidad mediante el análisis de sus instancias administradas y el informe sobre

las infracciones de las políticas que detecte o la toma de medidas correctivas con respecto a estas.

Código

- Se adjunta la `alerting_ct_logs.yaml` CloudFormation plantilla del proyecto.

Epics

Preparación de la cuenta de AWS

Tarea	Descripción	Habilidades requeridas
Instalar y configurar la CLI de AWS.	Instale la CLI de AWS versión 2. A continuación, configure los ajustes de las credencia les de seguridad para una identidad, el formato de salida predeterminado y la región de AWS predeterminada que la CLI de AWS utiliza para interactuar con AWS. La identidad debe tener los permisos necesarios para realizar las tareas.	Desarrollador, ingeniero de seguridad

Implemente la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Descarga la CloudFormation plantilla.	Descargue el archivo adjunto a una ruta local en su computadora y extraiga el archivo `alerting_`	Desarrollador, ingeniero de seguridad

Tarea	Descripción	Habilidades requeridas
	`ct_logs.yaml` de plantilla .	
Implemente la plantilla.	En la ventana de terminal en la que se ha configurado el perfil de la cuenta de AWS, ejecute el siguiente comando. `aws cloudformation create-stack --stack-name <stack_name> \ --capabilities <Value> \ --template-body file://<Full_Path> \ --parameters ParameterKey=DestinationEmailAddress,ParameterValue=<Value> \ ParameterKey=SNSTopicName,ParameterValue=<Value> \ ParameterKey=EnableRemediation ,ParameterValue=<Value> \ ParameterKey=AutomationAssumeRole, ParameterValue=<Value>` En el siguiente paso, introduzca los valores de los parámetros de la plantilla.	Desarrollador, ingeniero de seguridad

Tarea	Descripción	Habilidades requeridas
Complete los parámetros de la plantilla.	Introduzca valores requeridos para los parámetros. • `DestinationEmailAddress` – La dirección de correo electrónico para recibir una alerta cuando esté programada la eliminación de una clave de AWS KMS. • `SNSTopicName` – El nombre del tema de Amazon SNS. • `EnableRemediation` – Cancelación de la eliminación programada de claves mediante un manual de procedimientos de Systems Manager. Los valores permitidos son `true` y `false`. • `AutomationAssumeRole` : el nombre de recurso de Amazon (ARN) del rol que permite a System Manager Automation realizar las acciones en su nombre. Para obtener más información, consulte la sección Permisos de IAM necesarios en la AWSConfigRemediation-CancelKeyDeletiondocumentación.	Desarrollador, ingeniero de seguridad

Tarea	Descripción	Habilidades requeridas
	• `Capabilities` — Para CloudFormation que AWS cree la pila, debe reconocer explícitamente que la plantilla de pila contiene determinadas capacidades.	

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Verifique la bandeja de entrada de correo electrónico y elija Confirmar la suscripción en el mensaje de correo electrónico que reciba de Amazon SNS. Se abrirá una ventana del navegador web que mostrará una confirmación de suscripción y su ID de suscripción.	Desarrollador, ingeniero de seguridad

Recursos relacionados

Referencias

- Creación de una regla para un servicio de AWS
- Crear una CloudWatch alarma de Amazon para detectar el uso de una clave de AWS KMS pendiente de eliminación

Tutoriales y videos

- Cómo empezar con Amazon EventBridge
- Profundice en Amazon EventBridge (charlas técnicas en línea de AWS)

Taller de AWS

- ¿Trabajando con EventBridge reglas

Información adicional

En el siguiente código se proporcionan ejemplos para ampliar la solución a fin de supervisar y notificarlo sobre cualquier cambio en cualquier servicio de AWS. Los ejemplos incluyen patrones predefinidos y patrones personalizados. Para obtener más información, consulte Eventos y patrones de eventos en EventBridge.

```
EventPattern:
        source:
        - aws.kms
        detail-type:
        - AWS API Call via CloudTrail
        detail:
          eventSource:
          - kms.amazonaws.com
          eventName:
          - ScheduleKeyDeletion
```

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Identifique los buckets públicos de Amazon S3 AWS Organizations mediante Security Hub (CSPM)

Mourad Cherfaoui, Arun Chandapillai y Parag Nagwekar, Amazon Web Services

Resumen

Este patrón le muestra cómo crear un mecanismo para identificar los depósitos públicos de Amazon Simple Storage Service (Amazon S3) en sus cuentas. AWS Organizations El mecanismo funciona mediante el uso de controles del estándar AWS Foundational Security Best Practices (FSBP) AWS Security Hub CSPM para monitorear los buckets de Amazon S3. Puedes usar Amazon EventBridge para procesar las conclusiones del CSPM de Security Hub y, después, publicarlas en un tema del Servicio de Notificación Simple de Amazon (Amazon SNS). Las partes interesadas de su organización pueden suscribirse al tema y recibir notificaciones inmediatas por correo electrónico sobre los hallazgos.

Los nuevos buckets de Amazon S3 y sus objetos no permiten el acceso público de forma predeterminada. Puede utilizar este patrón en situaciones en las que deba modificar las configuraciones predeterminadas de Amazon S3 en función de los requisitos de su organización. Por ejemplo, este podría ser un escenario en el que tenga un bucket de Amazon S3 que aloje un sitio web de acceso público o archivos que todos los usuarios de Internet puedan leer desde su bucket de Amazon S3.

El Security Hub CSPM se suele implementar como un servicio central para consolidar todos los hallazgos de seguridad, incluidos los relacionados con los estándares de seguridad y los requisitos de cumplimiento. Hay otros Servicios de AWS que puede utilizar para detectar buckets públicos de Amazon S3, pero este patrón utiliza una implementación CSPM de Security Hub existente con una configuración mínima.

Requisitos previos y limitaciones

Requisitos previos

- Una configuración AWS de varias cuentas con una cuenta de administrador CSPM de Security Hub dedicada
- Security Hub (CSPM) y AWS Config, habilitado en el Región de AWS que desee monitorizar

> **Note**
>
> Debe habilitar la agregación entre regiones en Security Hub CSPM si quiere monitorear varias regiones desde una sola región de agregación.

- Permisos de usuario para acceder y actualizar la cuenta de administrador CSPM de Security Hub, acceso de lectura a todos los buckets de Amazon S3 de la organización y permisos para desactivar el acceso público (si es necesario)

Arquitectura

El siguiente diagrama muestra una arquitectura para usar Security Hub CSPM para identificar los buckets públicos de Amazon S3.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Security Hub CSPM supervisa la configuración de los buckets de Amazon S3 en todas AWS Organizations las cuentas (incluida la cuenta de administrador) mediante los controles S3.2 y S3.3 del estándar de seguridad FSBP y detecta si un bucket está configurado como público.
2. La cuenta de administrador de CSPM de Security Hub accede a los resultados (incluidos los de S3.2 y S3.3) desde todas las cuentas de los miembros.
3. Security Hub CSPM envía automáticamente todos los hallazgos nuevos y todas las actualizaciones de los hallazgos existentes EventBridge como Security Hub CSPM Findings: Imported events. Esto incluye eventos para conocer los resultados de las cuentas del administrador y de los miembros.
4. Una EventBridge regla filtra los resultados de las versiones S3.2 y S3.3 que tienen un `ComplianceStatus` de`FAILED`, un estado de flujo de trabajo de y un de. `NEW` `RecordState` `ACTIVE`
5. Las reglas utilizan los patrones de eventos para identificar los eventos y enviarlos a un tema de Amazon SNS una vez que coinciden.
6. Un tema de Amazon SNS envía los eventos a sus suscriptores (por ejemplo, por correo electrónico).
7. Los analistas de seguridad designados para recibir las notificaciones por correo electrónico revisan el bucket de Amazon S3 en cuestión.

8. Si el depósito está aprobado para el acceso público, el analista de seguridad establece el estado del flujo de trabajo del hallazgo correspondiente en Security Hub CSPM en. `SUPPRESSED` De lo contrario, el analista establece el estado como `NOTIFIED`. Esto elimina las notificaciones futuras para el bucket de Amazon S3 y reduce el ruido de las notificaciones.
9. Si el estado del flujo de trabajo está establecido como `NOTIFIED`, el analista de seguridad analiza los resultados con el propietario del bucket para determinar si el acceso público está justificado y si cumple con los requisitos de privacidad y protección de datos. Como resultado de la investigación, se elimina el acceso público al bucket o se aprueba el acceso público. En este último caso, el analista de seguridad establece el estado del flujo de trabajo como `SUPPRESSED`.

> **Note**
>
> El diagrama de arquitectura se aplica a las implementaciones de agregación de una sola región y entre regiones. En las cuentas A, B y C del diagrama, el CSPM de Security Hub puede pertenecer a la misma región que la cuenta de administrador o pertenecer a regiones diferentes si está habilitada la agregación entre regiones.

Tools (Herramientas)

- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. EventBridge ofrece un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones de software como servicio (SaaS) y. Servicios de AWS EventBridge enruta esos datos a destinos como los temas y AWS Lambda funciones de Amazon SNS si los datos coinciden con las reglas definidas por el usuario.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados en los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Security Hub CSPMproporciona una visión completa del estado de su seguridad en. AWS Security Hub CSPM también le ayuda a comprobar su AWS entorno según los estándares y las mejores prácticas del sector de la seguridad. Security Hub CSPM recopila datos de seguridad de todos Cuentas de AWS los servicios y productos de socios externos compatibles y, a continuación,

ayuda a analizar las tendencias de seguridad e identificar los problemas de seguridad de mayor prioridad.

Epics

Configurar cuentas CSPM de Security Hub

Tarea	Descripción	Habilidades requeridas
Habilite Security Hub CSPM en AWS Organizations las cuentas.	Para habilitar el CSPM de Security Hub en las cuentas de la organización en las que desee supervisar los buckets de Amazon S3, consulte las directrices de Designación de una cuenta de administrador de CSPM de Security Hub (consola) y Administración de cuentas de miembros que pertenecen a una organización en la documentación de Security Hub CSPM.	Administrador de AWS
(Opcional) Habilite la agregación entre regiones.	Si desea supervisar los buckets de Amazon S3 en varias regiones desde una sola región, configure la agregación entre regiones.	Administrador de AWS
Active los controles S3.2 y S3.3 para el estándar de seguridad FSBP.	Debe habilitar los controles S3.2 y S3.3 para el estándar de seguridad FSBP. 1. Para habilitar los controles S3.2, siga las instrucciones de [S3.2] Los buckets S3 deberían prohibir el acceso	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	de lectura público en la documentación del CSPM de Security Hub. 2. Para habilitar los controles S3.3, siga las instrucciones de [3] Los buckets S3 deberían prohibir el acceso de escritura público en la documentación de CSPM de Security Hub.	

Configuración del entorno

Tarea	Descripción	Habilidades requeridas
Configure el tema de Amazon SNS y la suscripción por correo electrónico.	1. Inicie sesión en la consola de Amazon SNS Consola de administración de AWS y ábrala. 2. En el panel de navegación, elige Temas y, a continuación, seleccione Crear tema. 3. En Tipo, seleccione Estándar. 4. En Nombre, especifique un nombre para el tema (por ejemplo, public-s3-buckets). 5. Seleccione Create new topic (Crear nuevo tema). 6. En la pestaña Suscripciones, seleccione Crear suscripción.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	7. En Protocol, seleccione Email. 8. En Endpoint (Punto de conexión), ingrese una dirección de correo electrónico para recibir las notificaciones. Puede utilizar la dirección de correo electrónico de un AWS administrador, un profesional de TI o un profesional de Infosec. 9. Seleccione Crear subscripción. Para crear suscripciones de correo electrónico adicionales, repita los pasos 6 a 8 según sea necesario.	

Tarea	Descripción	Habilidades requeridas
Configure la EventBridge regla.	1. Abra la consola de EventBridge . 2. En la sección Comenzar, selecciona EventBridge Regla y, a continuación, selecciona Crear regla. 3. En la página Definir detalles de la regla, en Nombre, especifique un nombre para la regla (por ejemplo, public-s3-buckets). Seleccione Next (Siguiente). 4. En la sección Event pattern (Patrón de eventos), seleccione Event pattern form (Formulario de patrón de eventos). 5. Copie el siguiente código, péguelo en el editor de códigos de Patrones de eventos y, a continuación, selecciona Siguiente. `{ "source": ["aws.securityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "Compliance": { "Status": ["FAILED"]`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	<pre>},
	"RecordState":
	["ACTIVE"],
	"Workflow": {
	"Status":
	["NEW"]
	},
	"ProductF
	ields": {
	"ControlId":
	["S3.2", "S3.3"]
	}
	}
	}
	}</pre> 6. En la página Seleccionar destinos, en Seleccione un destino, seleccione Tema de SNS como destino y, a continuación, seleccione el tema que creó anteriorm ente.
	7. Elija Siguiente, vuelva a elegir Siguiente y, a continuación, elija Crear regla.	

Resolución de problemas

Problema	Solución
Tengo un bucket de Amazon S3 con acceso público activado, pero no recibo notificaciones por correo electrónico al respecto.	Esto podría deberse a que el depósito se creó en otra región y la agregación entre regiones no está habilitada en la cuenta de administr ador CSPM de Security Hub. Para resolver este problema, habilite la agregación entre

Problema	Solución
	regiones o implemente la solución de este patrón en la región en la que reside actualmente su bucket de Amazon S3.

Recursos relacionados

- ¿Qué es? AWS Security Hub CSPM (documentación de Security Hub CSPM)
- AWS Estándar de mejores prácticas de seguridad fundamentales (FSBP) (documentación de Security Hub CSPM)
- AWS Security Hub CSPM scripts de activación de múltiples cuentas (Labs)AWS
- Prácticas recomendadas de seguridad para Amazon S3 (documentación de Amazon S3)

Información adicional

Flujo de trabajo para supervisar buckets públicos de Amazon S3

El siguiente flujo de trabajo ilustra cómo puede supervisar los buckets de Amazon S3 públicos de su organización. El flujo de trabajo supone que ha completado los pasos descritos en la historia Configuración del tema de Amazon SNS y la suscripción de correo electrónico de este patrón.

1. Recibirá una notificación por correo electrónico cuando un bucket de Amazon S3 esté configurado con acceso público.
   - Si el depósito está aprobado para el acceso público, defina el estado del flujo de trabajo del hallazgo correspondiente `SUPPRESSED` en la cuenta de administrador de CSPM de Security Hub. Esto evita que Security Hub CSPM emita más notificaciones para este depósito y puede eliminar las alertas duplicadas.
   - Si el depósito no está aprobado para el acceso público, defina el estado del flujo de trabajo del hallazgo correspondiente en la cuenta de administrador de CSPM de Security Hub en. `NOTIFIED` Esto impide que el Security Hub CSPM emita más notificaciones para este bucket desde el Security Hub CSPM y puede eliminar el ruido.
2. Si el bucket puede contener datos confidenciales, desactive el acceso público inmediatamente hasta que se complete la revisión. Si desactiva el acceso público, Security Hub CSPM cambiará el

estado del flujo de trabajo a. `RESOLVED` A continuación, se detienen las notificaciones por correo electrónico del bucket.

3. Busque al usuario que configuró el depósito como público (por ejemplo, mediante el uso AWS CloudTrail) e inicie una revisión. Como resultado de la revisión, se elimina el acceso público al bucket o se aprueba el acceso público. Si se aprueba el acceso público, defina el estado del flujo de trabajo del resultado correspondiente a `SUPPRESSED`.

Ingesta y análisis de registros de seguridad de AWS en Microsoft Sentinel

Ivan Girardi y Sebastian Wenzel, Amazon Web Services

Resumen

Este patrón describe cómo automatizar la ingesta de registros de AWS seguridad, como AWS CloudTrail registros, datos de Amazon Logs, datos de Amazon CloudWatch VPC Flow Logs y hallazgos de GuardDuty Amazon, en Microsoft Sentinel. Si su organización usa Microsoft Sentinel como sistema de administración de eventos e información de seguridad (SIEM), esto lo ayuda a supervisar y analizar los registros de forma centralizada para detectar eventos relacionados con la seguridad. En cuanto los registros están disponibles, se envían automáticamente a un bucket de Amazon Simple Storage Service (Amazon S3) en menos de 5 minutos. Esto puede ayudarle a detectar rápidamente los eventos de seguridad en su entorno. AWS

Microsoft Sentinel ingiere CloudTrail los registros en un formato tabular que incluye la marca de tiempo original del momento en que se registró el evento. La estructura de los registros ingeridos habilita las capacidades de consulta mediante el lenguaje de consulta Kusto en Microsoft Sentinel.

El patrón implementa una solución de supervisión y alertas que detecta los errores de ingesta en menos de 1 minuto. También incluye un sistema de notificaciones que el SIEM externo puede supervisar. Se utilizan AWS CloudFormation para implementar los recursos necesarios en la cuenta de registro.

Público objetivo

Este patrón se recomienda para los usuarios que tienen experiencia con AWS Control Tower AWS Organizations, CloudFormation, AWS Identity and Access Management (IAM) y AWS Key Management Service (AWS KMS).

Requisitos previos y limitaciones

Requisitos previos

A continuación, se indican los requisitos previos para implementar esta solución:

- Cuentas de AWS Activos que se gestionan como una organización en una AWS Control Tower landing zone AWS Organizations y forman parte de ella. La organización debe incluir una cuenta

dedicada al registro. Para obtener instrucciones, consulte Creación y configuración de una organización en la AWS Organizations documentación.

- Un CloudTrail registro que registra los eventos de toda la organización y almacena los registros en un bucket de Amazon S3 en la cuenta de registro. Para obtener instrucciones, consulte Creating a trail for an organization.
- En la cuenta de registro, permisos para asumir un rol de IAM existente que tenga los permisos siguientes:
  - Implemente los recursos definidos en la CloudFormation plantilla proporcionada.
  - Implemente la CloudFormation plantilla proporcionada.
  - Modifique la política de AWS KMS claves si los registros están cifrados con una clave administrada por el cliente.
- AWS Command Line Interface (AWS CLI), instalado y configurado.
- Una cuenta de Microsoft Azure con una suscripción para usar Microsoft Sentinel.
- Habilite y configure Microsoft Sentinel. Para obtener instrucciones, consulte Enable Microsoft Sentinel and initial features and content en la documentación de Microsoft Sentinel.
- Cumpla los requisitos previos para configurar el conector de S3 de Microsoft Sentinel.

Limitaciones

- Esta solución reenvía los registros de seguridad de un bucket de Amazon S3 en la cuenta de registro a Microsoft Sentinel. Las instrucciones sobre cómo enviar los registros a Amazon S3 no se proporcionan de forma explícita.
- Este patrón proporciona instrucciones para el despliegue en una zona de AWS Control Tower landing zone. Sin embargo, no AWS Control Tower es obligatorio el uso de.
- Esta solución es compatible con un entorno en el que el depósito de registro de Amazon S3 está restringido por políticas de control de servicios (SCPs), como la política de no permitir cambios en el depósito para depósitos de Amazon S3 AWS Control Tower creados en Log Archive.
- Este patrón proporciona instrucciones para reenviar CloudTrail registros, pero puede adaptar esta solución para enviar otros registros compatibles con Microsoft Sentinel, como registros de Logs CloudWatch , Amazon VPC Flow Logs y. GuardDuty
- En las instrucciones se utiliza el AWS CLI para implementar la CloudFormation plantilla, pero también puede utilizar el. Consola de administración de AWS Para obtener instrucciones, consulte Uso de la AWS CloudFormation consola. Si usa la consola para implementar la pila, despliéguela en el mismo lugar Región de AWS que en el depósito de registro.

- Esta solución implementa una cola de Amazon Simple Queue Service (Amazon SQS) para enviar las notificaciones de Amazon S3. La cola contiene mensajes con las rutas de los objetos cargados en el bucket de Amazon S3, no con datos reales. La cola utiliza el cifrado SSE-SQS para ayudar a proteger el contenido de los mensajes. Si desea cifrar la cola de SQS con SSE-KMS, puede utilizar una clave de KMS administrada por el cliente. Para obtener más información, consulte Encryption at rest in Amazon SQS.

Arquitectura

En esta sección se ofrece información general sobre la arquitectura que establece el código de ejemplo. En el siguiente diagrama se muestran los recursos implementados en la cuenta de registro para ingerir los registros de un bucket de Amazon S3 existente a Microsoft Sentinel.

En el siguiente diagrama de arquitectura se muestran las siguientes interacciones de los recursos:

1. En la cuenta de registro, Microsoft Sentinel asume un rol de IAM a través de OpenID Connect (OIDC) para acceder a los registros de un bucket de Amazon S3 y una cola de Amazon SQS específicos.
2. Amazon Simple Notification Service (Amazon SNS) y Amazon S3 AWS KMS se utilizan para el cifrado.
3. Amazon S3 envía mensajes de notificación a la cola de Amazon SQS cada vez que recibe nuevos registros.
4. Microsoft Sentinel comprueba si hay mensajes nuevos en Amazon SQS. La cola de Amazon SQS utiliza el cifrado SSE-SQS. El periodo de retención de mensajes está establecido en 14 días.
5. Microsoft Sentinel extrae mensajes de la cola de Amazon SQS. Los mensajes contienen la ruta de los objetos de Amazon S3 cargados. Microsoft Sentinel ingiere esos objetos del bucket de Amazon S3 en la cuenta de Microsoft Azure.
6. Una CloudWatch alarma monitorea la cola de Amazon SQS. Si los mensajes no se reciben y se eliminan de la cola de Amazon SQS en 5 minutos, se inicia una notificación de Amazon SNS que envía un correo electrónico.

AWS Control Tower le ayuda a configurar la estructura de la unidad organizativa fundamental (OU) y centraliza los CloudTrail registros en la cuenta de registro. También implementa la obligación de SCPs proteger el depósito de registro.

Hemos proporcionado la arquitectura objetivo en una AWS Control Tower landing zone, pero no es estrictamente necesaria. En este diagrama, los recursos de la cuenta de administración reflejan una AWS Control Tower implementación y un CloudTrail registro que registra los eventos de toda la organización.

Este patrón se centra en la implementación de recursos en la cuenta de registro. Si los registros almacenados en Amazon S3 en su AWS Control Tower landing zone están cifrados con una clave KMS administrada por el cliente, debe actualizar la política de claves para permitir que Microsoft Sentinel descifre los registros. En una AWS Control Tower landing zone, la política de claves se administra desde la cuenta de administración, que es donde se creó la clave.

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todas Cuentas de AWS las regiones.
- Amazon le CloudWatch ayuda a supervisar las métricas de sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.
- AWS Control Towerle ayuda a configurar y administrar un entorno de AWS múltiples cuentas, siguiendo las mejores prácticas.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar varias cuentas Cuentas de AWS en una organización que puede crear y administrar de forma centralizada.
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

- Microsoft Sentinel es un sistema de SIEM nativo en la nube que proporciona orquestación, automatización y respuesta de seguridad (SOAR).

Repositorio de código

El código de este patrón está disponible en los registros de AWS seguridad de GitHub Ingest and Analyze del repositorio Sentinel de Microsoft.

Prácticas recomendadas

- Siga el principio del privilegio mínimo (documentación de IAM).
- Siga las prácticas recomendadas para AWS Control Tower administradores (documentación)AWS Control Tower .
- Siga las prácticas AWS CloudFormation recomendadas (CloudFormation documentación).
- Utilice herramientas de análisis de código, como cfn_nag, para escanear las plantillas generadas. CloudFormation La herramienta cfn_nag identifica posibles problemas de seguridad en las plantillas mediante la búsqueda de patrones. CloudFormation

Epics

Conexión de Microsoft Sentinel a Amazon S3

Tarea	Descripción	Habilidades requeridas
Preparar el conector de S3 de Microsoft Sentinel.	1. En Microsoft Sentinel, elija Conectores de datos. 2. En la galería de conectores de datos, elija Amazon Web Services S3. **Note** Si no ve el conector, instale la solución de Amazon Web Services desde el centro de contenido de Microsoft Sentinel.	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas
	3. En el panel de detalles del conector, elija Abrir página de conectores. 4. En la sección Configuración, copie el valor de ID externo. Necesitará este ID más adelante.	

Implemente la CloudFormation pila

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	En un intérprete de comandos de bash, ingrese el siguiente comando. Esto clona los registros de AWS seguridad de ingesta y análisis en el repositorio Sentinel de Microsoft. `git clone https://github.com/aws-samples/ingest-and-analyze-aws-security-logs-in-microsoft-sentinel.git`	DevOps ingeniero, AWS general
Asumir el rol de IAM en la cuenta de registro.	En la cuenta de registro, asuma el rol de IAM que tiene permisos para implementar la CloudFormation pila. Para obtener más información sobre cómo asumir una función de IAM en la AWS	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas
	CLI, consulte Usar una función de IAM en la. AWS CLI	

Tarea	Descripción	Habilidades requeridas
Implemente la pila.	Para implementar la CloudFormation pila, ingresa el siguiente comando, donde: • `<Bucket name>` es el nombre del bucket de Amazon S3 de registro. • `<Sentinel external ID>` es el ID externo del conector de Amazon S3 en Microsoft Sentinel. • `<Email address>` es una dirección de correo electrónico válida donde desea recibir las notificaciones. • `<Customer managed key ARN>` es el nombre de recurso de Amazon (ARN) de la clave de KMS administrada por el cliente. Proporcione este parámetro solo si los registros están cifrados con una clave de KMS administrada por el cliente. • `<Suffix>` es un parámetro opcional para evitar conflictos en los nombres de los recursos. • `<ARN for the OIDC provider>` es el ARN del proveedor de OIDC si ya existe. Si no proporciona	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas
	este parámetro, CloudFormation crea el proveedor OIDC. **Important** Si la AWS organización está supervisada con Microsoft Code Defender, el proveedor de OIDC para Microsoft ya se ha implementado. Debe proporcionar este parámetro y el ARN del proveedor existente. `aws cloudformation deploy --stack-name cloudtrail-sentinel-integration \ --no-fail-on-empty-changeset \ --template-file template.yml \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM CAPABILITY_AUTO_EXPAND \ --parameter-overrides \ ControlTowerS3BucketName="<Bucket name>" \`	

Tarea	Descripción	Habilidades requeridas
	`AzureWorkspaceID="<Sentinel external ID>" \ EmailAddress="<Email address>" \ KMSKeyArn="<Customer managed key ARN>" \ Suffix="<Suffix to avoid name conflicts>" \ OIDCProviderArn="<ARN for the OIDC provider>"`	
Copiar las salidas.	De la salida de la CloudFormation pila, copie los valores de `SentinelRoleArn` y `SentinelSQS` . Utilizará estos valores más adelante para completar la configuración en Microsoft Sentinel.	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas
Modificar la política de claves.	Si no utiliza una clave de KMS administrada por el cliente para cifrar los registros en el bucket de Amazon S3, puede omitir este paso. Si los registros están cifrados con una clave de KMS administrada por el cliente, modifique la política de claves para conceder permiso a Microsoft Sentinel para descifrar los registros. A continuación, se muestra una política de claves de ejemplo. Este ejemplo de política permite el acceso entre cuentas si la clave de KMS está en otra Cuenta de AWS. `{ "Version": "2012-10-17", "Id": "key-policy", "Statement": [ ... { "Sid": "Grant access to decrypt", "Effect": "Allow", "Principal": { "AWS": "<SentinelRoleArn>" }, `	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas
	<pre>"Action": "kms:Decrypt", "Resource": "<KeyArn>" }] }</pre>	

Configuración del conector en Microsoft Sentinel

Tarea	Descripción	Habilidades requeridas
Completar la configuración en Microsoft Sentinel.	1. En Microsoft Sentinel, elija Conectores de datos. 2. En la galería de conectores de datos, elija Amazon Web Services S3. 3. En el panel de detalles del conector, elija Abrir página de conectores. 4. En la sección Configuración, haga lo siguiente: a. En Rol que agregar, ingrese el valor de `SentinelRoleArn` que ha copiado. b. En URL de SQS, ingrese el valor de `SentinelSQS` que ha copiado. c. En la lista Tablas de destinos, elija `AWSCloudTrail` . 5. Elija Agregar conexión.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Enviar notificaciones de eventos de Amazon S3 a Amazon SQS.	Siga las instrucciones de Habilitación y configuración de notificaciones de eventos mediante la consola de Amazon S3 para configurar el bucket de registro de Amazon S3 para enviar notificac iones de eventos a la cola de Amazon SQS. Si se CloudTrai l ha configurado para toda la organización, los registros de este depósito tienen el prefijo`<OrgID>/AWSLogs/ <OrgID>/` , donde `<OrgID>` está el ID de la organización. Para obtener más información, consulte Viewing details about your organization.	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas
Confirmar que los registros estén ingeridos.	1. Espere a que los registros se ingieran en Microsoft Sentinel. Esto puede tardar varios minutos. 2. En Microsoft Sentinel, abra la página del conector de datos de Amazon S3 y, a continuación, haga lo siguiente: • Confirme que el estado del conector de datos de Amazon S3 sea `Connected` . • Compruebe el volumen de datos en el gráfico Datos recibidos. Para obtener más información acerca de la inspección de la actividad del conector de datos, consulte Data connector en la documentación de Microsoft.	DevOps ingeniero

Validación de la solución

Tarea	Descripción	Habilidades requeridas
Registros de CloudWatch Compare y Sentinel.	En la configuración predeterminada de AWS Control Tower, CloudTrail los registros se envían a Amazon CloudWatch y se almacenan en la cuenta AWS Control Tower de	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas
	administración. Para obtener más información, consulte Inicio de sesión y supervisión AWS Control Tower. Siga estos pasos para confirmar que los registros se ingieren automáticamente en Microsoft Sentinel: 1. Abra la consola de CloudWatch . 2. En el panel de navegación, elija Registros y, luego, Información de registros. 3. En Seleccionar grupo (s) de registros, seleccione el grupo de registros en el que se almacenan CloudTrail los registros, por ejemplo`aws-controltower/CloudTrailLogs` . 4. En el cuadro del editor de consultas, escriba `fields eventID`. 5. Elija Ejecutar consulta. 6. Elija Exportar resultados y, a continuación, elija Copiar tabla al portapapeles (CSV). 7. Pegue los resultados en un editor de texto. 8. Cambie el formato de la salida para poder utilizarl	

Tarea	Descripción	Habilidades requeridas

	a en una consulta de Microsoft Sentinel. A continuación, se muestra un ejemplo en el que se utiliza el lenguaje de consulta Kusto:
	
	`AWSCloudTrail`
	`| where AwsEventId in`
	`(`
	`'aa08b5fe-3bfb-391a-a14e-5fcebe14dab2',`
	`'9decd805-269c-451c-b75b-762f5dce59f9'`
	`)`
	
	9. En Microsoft Sentinel, abra la página del conector de datos de Amazon S3. Junto al gráfico Datos recibidos, elija Ir a análisis de registros.
	10. En el cuadro del editor de consultas, escriba la consulta y, a continuación, elija Ejecutar.
	11. En Microsoft Sentinel y CloudWatch, compruebe que el número de entradas es el mismo. Adapte el intervalo de tiempo si es necesario.	

Recursos relacionados

AWS documentación y recursos

- AWS CLI Referencia de comandos (AWS CLI documentación)
- Configurar opcionalmente AWS KMS keys (AWS Control Tower documentación)
- Encryption at rest in Amazon SQS (documentación de Amazon SQS)
- ¿Cómo puedo evitar que los destinatarios de las listas de correo cancelen la suscripción de todos los demás destinatarios de mis correos electrónicos con temas de Amazon SNS? (Centro de AWS conocimiento)

Documentación de Microsoft

- Connect Microsoft Sentinel a Amazon Web Services para ingerir datos de registro de AWS servicios
- Kusto Query Language in Microsoft Sentinel

Gestione AWS Organizations las políticas como código mediante AWS CodePipeline Amazon Bedrock

Andre Cavalcante y Mariana Pessoa de Queiroz, Amazon Web Services

Resumen

Puede usar las políticas de autorización AWS Organizations para configurar y administrar de forma centralizada el acceso de los principales y los recursos de las cuentas de sus miembros. Las políticas de control de servicios (SCPs) definen los permisos máximos disponibles para los roles y usuarios AWS Identity and Access Management (IAM) de su organización. Las políticas de control de recursos (RCPs) definen los permisos máximos disponibles para los recursos de su organización.

Este patrón le ayuda a gestionar SCPs la infraestructura RCPs como código (IaC) que se despliega mediante un proceso de integración y despliegue continuos (CI/CD). Al utilizar Terraform AWS CloudFormation o Hashicorp para gestionar estas políticas, puede reducir la carga asociada a la creación y el mantenimiento de varias políticas de autorización.

Este patrón incluye las siguientes características:

- Puede crear, eliminar y actualizar las políticas de autorización mediante archivos de manifiesto (`scp-management.json` y `rcp-management.json`).
- Trabaja con barreras de protección en lugar de políticas. Las barreras de protección y sus objetivos se definen en los archivos de manifiesto.
- La canalización, que utiliza AWS CodeBuild y AWS CodePipeline, fusiona y optimiza las barreras de protección de los archivos de manifiesto. Para cada declaración del archivo de manifiesto, la canalización combina las barreras de protección en una única SCP o RCP y, a continuación, las aplica a los objetivos definidos.
- AWS Organizations aplica las políticas a sus objetivos. Un objetivo puede ser una Cuenta de AWS unidad organizativa (OU), un entorno (que es un grupo de cuentas o lo OUs que definas en el `environments.json` archivo) o un grupo de cuentas que comparten una AWS etiqueta.
- Amazon Bedrock lee los registros de la canalización y resume todos los cambios de política.
- La canalización requiere una aprobación manual. El aprobador puede revisar el resumen ejecutivo que Amazon Bedrock ha preparado, lo que lo ayuda a entender los cambios.

Requisitos previos y limitaciones

Requisitos previos

- Múltiples Cuentas de AWS que se administran como una organización en AWS Organizations. A fin de obtener más información, consulte Creación de una organización.
- Las funciones SCP y RCP están habilitadas en. AWS Organizations Para obtener más información, consulte Enabling a policy type.
- La versión 1.9.8 o posterior de Terraform instalada.
- Si no va a implementar esta solución a través de una canalización de Terraform, el archivo de estado de Terraform debe almacenarse en un depósito de Amazon Simple Storage Service (Amazon S3) en el Cuenta de AWS lugar donde vaya a implementar la canalización de administración de políticas.
- La versión 3.13.3 o posterior de Python instalada.

Limitaciones

- No puede usar este patrón para administrar SCPs o RCPs crear fuera de esta CI/CD canalización. Sin embargo, puede recrear las políticas existentes a través de la canalización. Para obtener más información, consulte Migración de las políticas existentes a la canalización en la sección Información adicional de este patrón.
- El número de cuentas y las políticas de cada cuenta están sujetos a las cuotas y los límites de servicio aplicables AWS Organizations. OUs
- Este patrón no se puede utilizar para configurar políticas de administración AWS Organizations, como las políticas de respaldo, las políticas de etiquetas, las políticas de aplicaciones de chat o las políticas declarativas.

Arquitectura

En el siguiente diagrama se muestra el flujo de trabajo del proceso de administración de políticas y sus recursos asociados.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario confirma los cambios en los archivos de manifiesto `scp-management.json` o `rcp-management.json` de la ramificación principal del repositorio remoto.
2. El cambio en la `main` sucursal inicia la entrada de la canalización. AWS CodePipeline
3. CodePipeline inicia el `Validate-Plan` CodeBuild proyecto. Este proyecto utiliza un script de Python en el repositorio remoto para validar las políticas y los archivos de manifiesto de políticas. Este CodeBuild proyecto hace lo siguiente:
   a. Comprueba que los archivos de manifiesto de SCP y RCP contienen una declaración única IDs ()`Sid`.
   b. Utiliza los scripts `scp-policy-processor/main.py` y `rcp-policy-processor/main.py` de Python para concatenar las barreras de protección de la carpeta de barreras de protección en una sola política RCP o SCP. Combina barreras de protección que tienen los mismos valores de `Resource`, `Action` y `Condition`.
   c. Se utiliza AWS Identity and Access Management Access Analyzer para validar la política final optimizada. Si hay algún resultado, la canalización se detiene.
   d. Crea archivos `scps.json` y `rcps.json`, que Terraform utiliza para crear recursos.
   e. Ejecuta el comando `terraform plan`, que crea un plan de ejecución de Terraform.
4. (Opcional) El `Validate-Plan` CodeBuild proyecto usa el `bedrock-prompt/prompt.py` script para enviar un mensaje a Amazon Bedrock. La petición se define en el archivo `bedrock-prompt/prompt.txt`. Amazon Bedrock utiliza Anthropic Claude Sonnet 3.5 para generar un resumen de los cambios propuestos mediante el análisis de los registros de Terraform y Python.
5. CodePipeline utiliza un tema del Amazon Simple Notification Service (Amazon SNS) para notificar a los aprobadores que los cambios deben revisarse. Si Amazon Bedrock generó un resumen de cambios, la notificación incluye este resumen.
6. Un aprobador de políticas aprueba la acción en. CodePipeline Si Amazon Bedrock generó un resumen de cambios, el aprobador puede revisarlo CodePipeline antes de aprobarlo.
7. CodePipeline inicia el proyecto. `Apply` CodeBuild Este proyecto usa Terraform para aplicar los cambios de RCP y SCP. AWS Organizations

La plantilla de IaC asociada a esta arquitectura también implementa los siguientes recursos que respaldan la canalización de administración de políticas:

- Un depósito de Amazon S3 para almacenar los CodePipeline artefactos y los scripts, como `scp-policy-processor/main.py` `bedrock-prompt/prompt.py`

- Una clave AWS Key Management Service (AWS KMS) que cifra los recursos creados por esta solución

Tools (Herramientas)

Servicios de AWS

- Amazon Bedrock es un servicio de IA totalmente administrado que pone a disposición de los usuarios muchos modelos fundacionales de alto rendimiento a través de una API unificada.
- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- AWS CodePipeline permite diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software y automatizar los pasos necesarios para lanzar los cambios en el software de manera continua.
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar múltiples cuentas Cuentas de AWS en una organización que usted crea y administra de forma centralizada.
- AWS SDK para Python (Boto3)es un kit de desarrollo de software que le ayuda a integrar su aplicación, biblioteca o script de Python con Servicios de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

- HashiCorp Terraform es una herramienta de IaC que le ayuda a usar código para aprovisionar y administrar la infraestructura y los recursos de la nube.

Repositorio de código

El código de este patrón está disponible en el organizations-policy-pipeline GitHub repositorio. Los archivos clave que se incluyen en la carpeta `sample-repository` son los siguientes:

- En la carpeta `environments`, `environments.json` contiene una lista de entornos. Los entornos son un grupo de objetivos y pueden contener Cuenta de AWS IDs o unidades organizativas (OUs).
- En la carpeta `rcp-management`:

  - La `guardrails` carpeta contiene las barandillas individuales para su RCPs
  - La `policies` carpeta contiene a la persona RCPs
  - El archivo de `rcp-management.json` manifiesto le ayuda a gestionar las barandillas RCP, completas RCPs, y sus objetivos asociados.
- En la carpeta `scp-management`:
  - La `guardrails` carpeta contiene las barandillas individuales de su SCPs
  - La `policies` carpeta contiene a la persona SCPs
  - El archivo de `scp-management.json` manifiesto le ayuda a gestionar las barandillas SCP, completas SCPs, y sus objetivos asociados.
- La `utils` carpeta contiene scripts que pueden ayudarte a migrar los actuales SCPs y a gestionarlos a RCPs lo largo del proceso. Para obtener más información, consulte la sección Información adicional de este patrón.

Prácticas recomendadas

- Antes de configurar la canalización, te recomendamos que compruebes que no has alcanzado los límites de tus AWS Organizations cuotas.
- Le recomendamos que utilice la cuenta AWS Organizations de administración solo para las tareas que se deben realizar en esa cuenta. Para obtener más información, consulte Best practices for the management account.

Epics

Configuración de la cuenta de destino

Tarea	Descripción	Habilidades requeridas
Creación de un repositorio.	Cree un repositorio desde el que su equipo de operaciones de seguridad administre las políticas. Utilice uno de los proveedores de repositorios de terceros AWS CodeConnections compatibles.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Delegar la administración de políticas.	Delegue la administración de AWS Organizations las políticas a la cuenta de miembro en la que vaya a implementar la canalización. Para obtener instrucciones, consulte Crear una política de delegación basada en recursos con. AWS Organizations Para ver un ejemplo de política, consulte Política de delegación basada en recursos de ejemplo en la sección Información adicional de este patrón.	Administrador de AWS
(Opcional) Habilitar el modelo fundacional.	Si desea generar resúmenes de los cambios en la política, habilite el acceso al modelo básico Anthropic Claude 3.5 Sonnet en Amazon Bedrock, Cuenta de AWS donde vaya a implementar la canalización. Para obtener instrucciones, consulte Add or remove access to Amazon Bedrock foundation models.	AWS general

Implementación de recursos para la canalización

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Introduzca el siguiente comando para clonar el	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	repositorio desde: organizations-policy-pipeline GitHub `git clone https://github.com/aws-samples/organizations-policy-pipeline.git`	

Tarea	Descripción	Habilidades requeridas
Definir el método de implementación.	1. En el repositorio clonado, abra el archivo `variables.tf` . 2. Para `project_name` , ingrese el prefijo que desee aplicar a los nombres de los recursos implementados. 3. Para `provider_type` , ingrese el proveedor del repositorio remoto. Los valores válidos se proporcionan en el archivo. 4. Para `full_repository_name` , ingrese el nombre del repositorio remoto. 5. Para `branch_name` , ingrese el nombre de la ramificación de Git que utilizará para implementar las políticas. Una inserción o fusión en esta ramificación, se inicia la canalización. Normalmente, esta es la rama principal. 6. Para `terraform_version` , ingrese la versión de Terraform que está utilizando. 7. Para `enable_bedrock` , ingrese `true` si desea que Amazon Bedrock resuma los cambios. Ingrese `false`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	si no desea generar un resumen de los cambios. 8. Para `tags`, ingrese los pares de clave-valor que quiera asignar como etiquetas a los recursos implementados. 9. Guarde y cierre el archivo `variables.tf` .	

Implemente la canalización.	1. Ingrese el siguiente comando para crear un plan y revisar los cambios:
	`terraform plan`
	2. Ingrese el siguiente comando para aplicar el plan y crear la infraestr uctura de la canalización:
	`terraform apply`
		DevOps ingeniero, Terraform

Conectar el repositorio remoto.	En el paso anterior, Terraform creó una CodeConnections conexión con el repositorio de terceros. En la consola de herramientas para desarroll adores de AWS, cambie el estado de la conexión de `PENDING` a `AVAILABLE` . Para obtener instrucciones, consulte Update a pending connection.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Suscríbase al tema de Amazon SNS.	Terraform creó un tema de Amazon SNS. Suscriba un punto de conexión al tema y confirme la suscripción para que los aprobadores reciban notificaciones sobre las acciones de aprobación pendientes en la canalización. Para obtener instrucciones, consulte Creating a subscription to an Amazon SNS topic.	AWS general

Definición de las barreras de protección y políticas

Tarea	Descripción	Habilidades requeridas
Completar el repositorio remoto.	Desde el repositorio clonado, copie el contenido de la carpeta `sample-repository` al repositorio remoto. Esto incluye las carpetas `environments`, `rcp-management`, `scp-management` y `utils`.	DevOps ingeniero
Definir sus entornos.	1. En la carpeta `environments`, abra el archivo `environments.json`. Este es el archivo donde defines el objetivo Cuentas de AWS y OUs para tu RCPs y SCPs. 2. Elimine los entornos de ejemplo.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	3. Agregue sus entornos de destino en el siguiente formato: `[ { "ID": "<environment-name>", "Target": [ "<ou-name>:<ou-id>", "<account-name>:<account-id>" ] } ]` Donde: • `<environment-name>` es el nombre que se asigna al grupo de OUs y a las cuentas de AWS. Puede usar este nombre en el archivo de manifiesto para definir dónde quiere aplicar sus políticas. • `<ou-name>` es el nombre de la UO de destino. • `<ou-id>` es el ID de la UO de destino.	

Tarea	Descripción	Habilidades requeridas
	• `<account-name>` es el nombre del objetivo Cuenta de AWS. • `<account-id>` es el identificador del objetivo Cuenta de AWS. Para ver ejemplos, consulte el repositorio de código fuente. 4. Guarde y cierre el archivo `environments.json` .	

Tarea	Descripción	Habilidades requeridas
Definir sus barreras de protección.	1. Acceda a la carpeta `rcp-management/guardrails` de su repositorio remoto. Esta es la carpeta en la que se definen las barreras de protección del archivo de manifiesto de RCP. Cada barrera de protección debe estar en un archivo individual. Los archivos de barreras de protección pueden contener una o más declaraciones. **Note** Puedes usar la misma barrera de protección en varias sentencias de los archivos de manifiesto para SCPs y. RCPs Si modifica la barrera de protección, todas las políticas que la incluyan se verán afectadas. 2. Elimine cualquier ejemplo de barrera de protección que se haya copiado del repositorio de código fuente.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	3. Cree un nuevo archivo .json y asígnele un nombre descriptivo. 4. Abra el archivo .json que creó. 5. Defina la barrera de protección en el siguiente formato: `[ { "Sid": "<guardrail-name>", "Effect": "<effect-value>", "Action": [ "<action-name>" ], "Resource": "<resource-arn>", "Condition": { "<condition-operator>": { "<condition-key>": [ "<condition-value>" ] } } } ]` Donde: • `<guardrail-name>` es un nombre único para	

Tarea	Descripción	Habilidades requeridas
	la barrera de protección. Este nombre no se puede utilizar para ninguna otra barrera de protección. • `<effect-value>` debe ser `Allow` o `Deny`. Para obtener más información, consulte Effect. • `<action-name>` debe ser un nombre válido de una acción compatibl e con el servicio. Para obtener más información, consulte Action. • `<resource-arn>` es el nombre de recurso de Amazon (ARN) del recurso al que se aplica la barrera de protección. También puede utilizar caractere s comodín, como * o ?. Para obtener más información, consulte Resource. • `<condition-operato r>` es un operador de condición válido. Para obtener más información, consulte Operadores de condición. • `<condition-key>` es una clave de contexto de condición global	

Tarea	Descripción	Habilidades requeridas
	válida o una clave de contexto específica de un servicio. Para obtener más información, consulte Condition. • `<condition-value>` es el valor específico que se utiliza en una condición para evaluar si se aplica una barrera de protección. Para obtener más información, consulte Condition. Para ver ejemplos de barreras de protección de RCP, consulte el repositorio de código fuente. 6. Guarde y cierre el archivo .json. 7. Repita estos pasos para crear tantas barreras de protección de RCP como sea necesario. 8. Repita estos pasos en la `scp-management/guardrails` carpeta para crear tantas barandillas como necesite para su. SCPs Para ver ejemplos de barreras de protección de SCP, consulte el repositorio de código fuente.	

Tarea	Descripción	Habilidades requeridas
Definir sus políticas.	1. Acceda a la carpeta `rcp-management/policies` de su repositorio remoto. Esta es la carpeta en la que se definen las políticas completas del archivo de manifiesto de RCP. Cada política debe ser un archivo individual. **Note** Si modifica una política de esta carpeta, los cambios de política afectarán a todas las cuentas o a las OUs que se aplique esta política, tal y como se define en el archivo de manifiesto. 2. Elimine cualquier ejemplo de política que se haya copiado del repositorio de código fuente. 3. Cree un nuevo archivo .json y asígnele un nombre descriptivo. 4. Abra el archivo .json que creó.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	5. Defina la RCP. Por ejemplo RCPs, consulta el repositorio de código fuente o los ejemplos de políticas de control de recursos en la AWS Organizations documentación. 6. Guarde y cierre el archivo .json. 7. Repite estos pasos para crear tantos RCPs como necesites. 8. Repite estos pasos en la `scp-management/policies` carpeta para crear tantos SCPs como necesites. Por ejemplo SCPs, consulte el repositorio de código fuente o consulte los ejemplos de políticas de control de servicios en la AWS Organizations documentación.	

Uso del archivo de manifiesto para administrar las políticas

Tarea	Descripción	Habilidades requeridas
Configurar los archivos de manifiesto.	1. En la carpeta `rcp-management`, abra el archivo `rcp-management.json`. Este es el archivo en el que se definen las barandill	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	as de RCP que se RCPs aplican íntegramente a los entornos de destino. Para ver un ejemplo de este archivo, consulte el repositorio de código fuente. 2. Elimine la declaración de ejemplo. 3. Agregue una nueva declaración con el siguiente formato: `[ { "SID": "<statement-name>", "Target": { "Type": "<target-type>", "ID": "<target-name>" }, "Guardrails": [ "<guardrail-name>" ], "Policy": "<policy-name>", "Comments": "<comment-text>" } ]` Donde:	

Tarea	Descripción	Habilidades requeridas

	• `<statement-name>` es un nombre único para la declaración.
	• `<target-type>` es el tipo de destino al que desea aplicar la política. Los valores válidos son `Account`, `OU`, `Environment` o `Tag`.
	• `<target-name>` es el identificador del destino al que desea aplicar la política. Introduzca una de las siguientes opciones:
	  • En el caso de un Cuenta de AWS, introduzca el identificador como. `<account-name>:<account-id>`
	  • Para una UO, ingrese el identificador como `<OU-name>:<ou-id>`.
	  • Para un entorno, ingrese el nombre único que definió en el archivo `environments.json` .	

Tarea	Descripción	Habilidades requeridas
	• Para una etiqueta, ingrese el par de clave-valor como `<tag-key>:<tag-value>` . • `<guardrail-name>` es el nombre único de la barrera de protección de RCP que definió en la carpeta `rcp-management/guardrails` . Puede agregar varias barreras de protección en este elemento. Puede dejar este campo vacío si no desea aplicar ninguna barrera de protección. • `<policy-name>` es el nombre único de la RCP que definió en la carpeta `rcp-management/policies` . Solo se puede agregar una política en este elemento. Puede dejar este campo vacío si no desea aplicar ninguna política. • `<comment-text>` es una descripción que puede ingresar con fines de documentación. Este campo no se utiliza durante el procesamiento de la canalización. Puede	

Tarea	Descripción	Habilidades requeridas
	dejar este campo vacío si no desea agregar ningún comentario. 4. Repita estos pasos para añadir tantas sentencias como sea necesario RCPs para configurarlas en su organización. 5. Guarde y cierre el archivo `rcp-management.json` . 6. En la carpeta `scp-management` , repita estos pasos en el archivo `scp-management.json` . Este es el archivo en el que se definen las barandillas SCP que se SCPs aplican íntegramente a los entornos de destino. Para ver un ejemplo de este archivo, consulte el repositorio de código fuente.	

Tarea	Descripción	Habilidades requeridas
Iniciar la canalización.	Confirme y envíe los cambios a la ramificación del repositorio remoto que definió en el archivo `variables.tf` . Normalmente, esta es la ramificación `main`. La CI/CD tubería se inicia automáticamente. Si hay algún error en la canalización, consulte la sección Solución de problemas de este patrón.	DevOps ingeniero
Aprobar los cambios.	Cuando se complete el `Validate-Plan` CodeBuild proyecto, los aprobadores de políticas reciben una notificación a través del tema Amazon SNS que configuraste previamente. Haga lo siguiente: 1. Abra el mensaje de notificación. 2. Si está disponible, consulte el resumen de los cambios en la política. 3. Siga las instrucciones de Aprobar o rechazar una acción de aprobación en. CodePipeline	AWS general, aprobador de políticas

Tarea	Descripción	Habilidades requeridas
Valide la implementación.	1. Inicie sesión en la consola de AWS Organizations en la cuenta que es administradora delegada de AWS Organizations. 2. En la página de políticas de control de servicios, confirme que las SCPs que ha creado aparecen en la lista. 3. Elija una SCP que se administre a través de la canalización y confirme que se aplica a los objetivos previstos. 4. En la página Políticas de control de recursos, confirme que las RCPs que ha creado aparecen en la lista. 5. Elija una RCP que se administre a través de la canalización y confirme que se aplica a los objetivos previstos.	AWS general

Resolución de problemas

Problema	Solución
Errores del archivo de manifiesto en la fase `Validate-Plan` de la canalización	En la salida de la canalización, aparece el mensaje “Errores de canalización en la fase de validación y planificación de los archivos de

Problema	Solución
	manifiesto” si hay algún error en los archivos `scp-management.json` o `rcp-management.json`. Los posibles errores incluyen un nombre de entorno incorrecto, campos o valores duplicados SIDs o no válidos. Haga lo siguiente: 1. Siga las instrucciones de View build details in AWS CodeBuild. 2. En el registro de compilación, busque el error de validación. El error proporciona más información sobre la causa del error de compilación. 3. Actualice el archivo .json correspondiente. 4. Confirme y envíe el archivo actualizado al repositorio remoto. La canalización se reinicia. 5. Supervise el estado para confirmar que se ha resuelto el error de validación.

Problema	Solución
Resultados del analizador de acceso de IAM en la fase `Validate-Plan` de la canalización	En la salida de la canalización, aparece el mensaje “Resultados en el analizador de acceso de IAM durante la fase de validación y planificación” si hay algún error en las definiciones de las políticas o las barreras de protección. Este patrón utiliza el analizador de acceso de IAM para validar la política final. Haga lo siguiente: 1. Siga las instrucciones de View build details in AWS CodeBuild. 2. En el registro de compilación, busque el error de validación del analizador de acceso de IAM. El error proporciona más información sobre la causa del error de compilación. Para obtener más información sobre los tipos de resultados, consulte Referencia de la verificación de la validación de la política de IAM. 3. Actualice el archivo .json correspondiente a la barrera de protección o política. 4. Confirme y envíe el archivo actualizado al repositorio remoto. La canalización se reinicia. 5. Supervise el estado para confirmar que se ha resuelto el error de validación.

Recursos relacionados

- Referencia de los elementos de la política de JSON de IAM (documentación de IAM)
- Políticas de control de recursos (AWS Organizations documentación)
- Políticas de control de servicios (AWS Organizations documentación)

- Add or remove access to Amazon Bedrock foundation models (documentación de Amazon Bedrock)
- Apruebe o rechace una acción de aprobación en CodePipeline (CodePipeline documentación)

Información adicional

Política de delegación basada en recursos de ejemplo

El siguiente es un ejemplo de política de delegación basada en recursos para. AWS Organizations Permite que la cuenta de administración delegada administre SCPs y RCPs para la organización. En el siguiente ejemplo de política, sustituya `<MEMBER_ACCOUNT_ID>` por el ID de la cuenta en la que va a implementar la canalización de administración de políticas.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegationToAudit",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<MEMBER_ACCOUNT_ID>:root"
      },
      "Action": [
        "organizations:ListTargetsForPolicy",
        "organizations:CreatePolicy",
        "organizations:DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:DisablePolicyType",
        "organizations:EnablePolicyType",
        "organizations:UpdatePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Migración de las políticas existentes a la canalización

Si ya existe SCPs o RCPs si desea migrar y administrar a través de esta canalización, puede usar los scripts de Python en la `sample-repository/utils` carpeta del repositorio de código. Estos scripts incluyen:

- `check-if-scp-exists-in-env.py`: este script comprueba si una política específica se aplica a algún objetivo de un entorno específico, que define en el archivo `environments.json`. Ingrese el siguiente comando para ejecutar este script:

  ```
  python3 check-if-scp-exists-in-env.py \
     --policy-type <POLICY_TYPE> \
     --policy-name <POLICY_NAME> \
     --env-id <ENV_ID>
  ```

  Sustituya lo siguiente en este comando:

  - `<POLICY_TYPE>` es `scp` or `rcp`
  - `<POLICY_NAME>` es el nombre de la SCP o la RCP.
  - `<ENV_ID>` es el ID del entorno que definió en el archivo `environments.json`.
- `create-environments.py`— Este script crea un archivo environments.json basado en el entorno actual SCPs y RCPs en su entorno. Excluye las políticas implementadas a través de. AWS Control Tower Ingrese el siguiente comando para ejecutar este script, donde `<POLICY_TYPE>` es `scp` o `rcp`:

  ```
  python create-environments.py --policy-type <POLICY_TYPE>
  ```
- `verify-policies-capacity.py`— Este script comprueba cada entorno que defina para determinar cuánta capacidad queda para cada cuota relacionada con las AWS Organizations políticas. Defina los entornos para comprobarlos en el archivo `environments.json`. Ingrese el siguiente comando para ejecutar este script, donde `<POLICY_TYPE>` es `scp` o `rcp`:

  ```
  python verify-policies-capacity.py --policy-type <POLICY_TYPE>
  ```

Administre los conjuntos de AWS IAM Identity Center permisos como código mediante AWS CodePipeline

Andre Cavalcante y Claison Amorim, Amazon Web Services

Resumen

AWS IAM Identity Center le ayuda a gestionar de forma centralizada el acceso mediante el inicio de sesión único (SSO) a todas sus aplicaciones. Cuentas de AWS Puede crear y administrar identidades de usuario en IAM Identity Center, o puede conectar una fuente de identidades existente, como un dominio de Microsoft Active Directory o un proveedor de identidades (IdP) externo. El IAM Identity Center ofrece una experiencia de administración unificada para definir, personalizar y asignar un acceso detallado a su entorno mediante conjuntos de permisos. AWS Los conjuntos de permisos se aplican a los usuarios y grupos federados de su almacén de identidades de IAM Identity Center o de su IdP externo.

Este patrón lo ayuda a administrar los conjuntos de permisos de IAM Identity Center como código en su entorno de cuentas múltiples que se administra como una organización en AWS Organizations. Con este patrón, puede lograr lo siguiente:

- Crear, eliminar y actualizar conjuntos de permisos
- Cree, actualice o elimine las asignaciones de conjuntos de permisos a los destinatarios Cuentas de AWS, a las unidades organizativas (OUs) o a la raíz de su organización.

Para gestionar los permisos y las asignaciones del IAM Identity Center como código, esta solución implementa un proceso de integración y entrega continuas (CI/CD) que utiliza y. AWS CodeBuild AWS CodePipeline Los conjuntos de permisos y las asignaciones se administran en plantillas JSON que se almacenan en un repositorio remoto. Cuando EventBridge las reglas de Amazon detectan un cambio en el repositorio o detectan modificaciones en las cuentas de la unidad organizativa de destino, se inicia una AWS Lambda función. La función Lambda inicia la CI/CD canalización que actualiza los conjuntos de permisos y las asignaciones en IAM Identity Center.

Requisitos previos y limitaciones

Requisitos previos

- Un entorno de varias cuentas administrado como una organización en AWS Organizations. A fin de obtener más información, consulte Creación de una organización.

- IAM Identity Center, habilitado y configurado con una fuente de identidad. Para obtener más información, consulte Introducción en la documentación de IAM Identity Center.
- Una cuenta de miembro que está registrada como administrador delegado para lo siguiente: Servicios de AWS
  - IAM Identity Center: para obtener instrucciones, consulte Register a member account en la documentación de IAM Identity Center.
  - AWS Organizations — Para obtener instrucciones, consulte Administrador delegado para. AWS Organizations Esta cuenta debe tener permisos para enumerar y describir las cuentas y OUs.

> **Note**
>
> Debe usar la misma cuenta de administrador delegado para ambos servicios.

- Permisos para implementar AWS CloudFormation pilas en la cuenta de administrador delegado del IAM Identity Center y en la cuenta de administración de la organización. Para obtener más información, consulte Control del acceso en la documentación. CloudFormation
- Un bucket de Amazon Simple Storage Service (Amazon S3) en la cuenta de administrador delegado de IAM Identity Center. Carga el código del artefacto en este bucket. Para obtener instrucciones, consulte Crear un bucket en la documentación de Amazon S3.
- El ID de la cuenta de gestión de la organización. Para obtener instrucciones, consulte Cómo encontrar su Cuenta de AWS ID.
- Un repositorio en tu servidor de código fuente, como GitHub.

Limitaciones

- Este patrón no se puede usar para administrar o asignar conjuntos de permisos para entornos de una sola cuenta o para cuentas que no se administran como una organización en AWS Organizations.
- Los nombres de los conjuntos de permisos IDs, la asignación y los tipos principales del centro de identidad de IAM IDs no se pueden modificar después de la implementación.
- Este patrón le ayuda a crear y administrar permisos personalizados. No puede usar este patrón para administrar o asignar permisos predefinidos.
- Este patrón no se puede usar para administrar un conjunto de permisos para la cuenta de administración de la organización.

Arquitectura

Arquitectura de destino

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario realiza uno de los siguientes cambios:
   - Realiza uno o más cambios en el repositorio remoto, como GitHub
   - Modifica las cuentas de la OU en AWS Organizations
2. Si el usuario confirmó un cambio en el repositorio remoto de la ramificación principal, se inicia la canalización.

   Si el usuario modificó las cuentas de la OU, la `MoveAccount` EventBridge regla detecta el cambio e inicia una función Lambda en la cuenta de administración de la organización.
3. La función Lambda iniciada inicia la CI/CD canalización en. CodePipeline
4. CodePipeline inicia el `TemplateValidation` CodeBuild proyecto. El `TemplateValidation` CodeBuild proyecto utiliza un script de Python en el repositorio remoto para validar las plantillas del conjunto de permisos. CodeBuild valida lo siguiente:
   - Los nombres de conjunto de permisos son únicos.
   - La sentencia de asignación IDs (`Sid`) es única.
   - Las definiciones de política figuran en el parámetro `CustomPolicy` y son válidas. (Esta validación utiliza AWS Identity and Access Management Access Analyzer.)
   - Los nombres de recursos de Amazon (ARNs) de las políticas gestionadas son válidos.
5. El grupo de `PermissionSet` acciones del `Deploy` CodeBuild proyecto se utiliza AWS SDK para Python (Boto3) para eliminar, crear o actualizar los conjuntos de permisos en el Centro de identidades de IAM. Solo se ven afectados los conjuntos de permisos con la etiqueta `SSOPipeline:true`. Todos los conjuntos de permisos que se administran a través de esta canalización tienen esta etiqueta.
6. El grupo de `Assignments` acciones del `Deploy` CodeBuild proyecto utiliza Terraform para eliminar, crear o actualizar las asignaciones en el IAM Identity Center. Los archivos de estado del backend de Terraform se almacenan en un bucket de Amazon S3 en la misma cuenta.
7. CodeBuild actualiza los conjuntos de permisos y las asignaciones en el Centro de Identidad de IAM.

Automatización y escala

Como todas las cuentas nuevas en un entorno de múltiples cuentas se trasladan a una unidad organizativa específica AWS Organizations, esta solución se ejecuta automáticamente y concede los conjuntos de permisos necesarios a todas las cuentas que especifiques en las plantillas de asignación. No se necesitan automatizaciones ni acciones de escalado adicionales.

En entornos de gran tamaño, la cantidad de solicitudes de API al IAM Identity Center puede provocar que esta solución se ejecute más lentamente. Terraform y Boto3 gestionan automáticamente la limitación para minimizar cualquier degradación del rendimiento.

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todo el mundo Cuentas de AWS . Regiones de AWS
- AWS CodeBuild es un servicio de compilación completamente administrado que le permite compilar código fuente, poner en marcha pruebas unitarias y producir artefactos listos para implementar.
- AWS CodePipeline permite diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software y automatizar los pasos necesarios para lanzar los cambios en el software de manera continua.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, AWS Lambda funciones, puntos finales de invocación HTTP que utilizan destinos de API o buses de eventos en otros. Cuentas de AWS
- AWS IAM Identity Centerle ayuda a gestionar de forma centralizada el acceso mediante inicio de sesión único (SSO) a todas sus aplicaciones y a las de la nube. Cuentas de AWS
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar múltiples cuentas Cuentas de AWS en una organización que puede crear y administrar de forma centralizada.
- AWS SDK para Python (Boto3)es un kit de desarrollo de software que le ayuda a integrar su aplicación, biblioteca o script de Python con Servicios de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Repositorio de código

El código de este patrón está disponible en el repositorio aws-iam-identity-center-pipeline. La carpeta de plantillas del repositorio incluye plantillas de muestra tanto para los conjuntos de permisos como para las asignaciones. También incluye AWS CloudFormation plantillas para implementar la CI/CD canalización y AWS los recursos en las cuentas de destino.

Prácticas recomendadas

- Antes de empezar a modificar el conjunto de permisos y las plantillas de asignación, le recomendamos que planifique los conjuntos de permisos para su organización. Tenga en cuenta cuáles deberían ser los permisos, a qué cuentas o OUs el conjunto de permisos debería aplicarse y qué entidades principales del centro de identidad de IAM (usuarios o grupos) deberían verse afectadas por el conjunto de permisos. Los nombres de los conjuntos de permisos IDs, la asociación y los tipos principales del centro de identidad de IAM IDs no se pueden modificar una vez implementados.
- Cumpla con el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte las mejores prácticas de seguridad y concesión de privilegios mínimos en la AWS Identity and Access Management documentación de IAM.

Epics

Planificar conjuntos de permisos y asignaciones

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	En un intérprete de comandos de bash, ingrese el siguiente comando. Esto clona el repositorio aws-iam-identity-center-pipeline desde. GitHub `git clone https://github.com/aws-samples/aws-iam-identity-center-pipeline.git`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Defina los conjuntos de permisos.	1. En el repositorio clonado, vaya a la carpeta `templates/permissionsets` y, a continuación, abra una de las plantillas disponibles. 2. En el parámetro `Name`, especifique un nombre para el conjunto de permisos. Este valor debe ser único y no se puede cambiar después de la implementación. 3. En el parámetro `Description`, describa brevemente el conjunto de permisos, como por ejemplo su caso de uso. 4. En el parámetro `SessionDuration`, especifique el tiempo durante el que un usuario puede iniciar sesión en una Cuenta de AWS. Utilice el formato de duración ISO-8601 (Wikipedia), por ejemplo, como `PT4H` durante 4 horas. Si no se define ningún valor, el valor predeterminado en IAM Identity Center es de 1 hora. 5. En el parámetro `RelayState`, especifiq	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	ue la URL que proporciona acceso rápido a la consola más adecuada para el rol del usuario. 6. Personalice las políticas del conjunto de permisos. Todos los parámetros siguientes son opcionales y se pueden modificar después de la implementación. Debe usar al menos uno de los parámetros para definir las políticas del conjunto de permisos: • En el `ManagedPolicies` parámetro, introduzca cualquier política AWS gestionada que desee asignar. ARNs • En el parámetro `CustomerManagedPolicies`, introduzca los nombres de cualquier política administrada por el cliente que desee asignar. No utilice el ARN. • En el parámetro `PermissionBoundary`, haga lo siguiente para asignar un límite de permisos: • Si utiliza una política AWS gestionada como	

Tarea	Descripción	Habilidades requeridas
	límite de permisos, en `PolicyType`, enter y `AWS`, en `Policy`, introduzca el ARN de la política. • Si utiliza una política administrada por el cliente como límite de permisos, en `PolicyType`, ingrese `Customer`, y en `Policy`, ingrese el nombre de la política. No utilice el ARN. • En el parámetro `CustomPolicy`, defina cualquier política personalizada con formato JSON que desee asignar. Para obtener más información acerca de la estructura de la política de JSON, consulte Información general de las políticas de JSON. 7. Guarde y cierre la plantilla del conjunto de permisos. Le recomendamos que guarde el archivo con un nombre que coincida con el nombre del conjunto de permisos.	

Tarea	Descripción	Habilidades requeridas
	8. Repita este proceso para crear tantos conjuntos de permisos como necesite su organización y elimine las plantillas de muestra que no sean necesarias.	

Tarea	Descripción	Habilidades requeridas
Defina las asignaciones.	1. En el repositorio clonado, vaya a la carpeta `templates/assignments` y, a continuación, abra `iam-identitycenter-assigments.json`. Este archivo describe cómo desea asignar los conjuntos de permisos a Cuentas de AWS o OUs. 2. En el parámetro `SID` introduzca un identificador para la asignación. Este valor debe ser único y no se puede modificar después de la implementación. 3. En el parámetro `Target`, defina las cuentas u organizaciones a las que desea aplicar el conjunto de permisos. Los valores válidos son cuenta IDs OUs, o `root`. `root` asigna el conjunto de permisos a todas las cuentas de los miembros de la organización, excluida la cuenta de administración. Introduzca los valores entre comillas dobles y separe los valores múltiples con comas. Cuenta IDs y OUs debe seguir el	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	patrón: `{{account_name}}:{{account_id}} o{{ou_name}}:{{ou_id}}` . Si desea asignar permisos de forma recursiva a los anidados OUs, utilice el patrón OU con un comodín al final. Ejemplo: `{{ou_name}}:{{ou_id}}:*` 4. En el parámetro `PrincipalType` , introduzca el tipo de entidad principal del IAM Identity Center que se verá afectada por el conjunto de permisos. Los valores válidos son `USER` o `GROUP`. Este valor no se puede modificar después de la implementación. 5. En el parámetro `PrincipalID` , introduzca el nombre del usuario o grupo del almacén de identidades del IAM Identity Center al que afectará el conjunto de permisos. Este valor no se puede modificar después de la implement ación. 6. En el parámetro `PermissionSetName` introduzca el nombre del	

Tarea	Descripción	Habilidades requeridas
	conjunto de permisos que desea asignar. 7. Repita los pasos del 2 al 6 para crear tantas asignaciones como necesite en este archivo. Normalmente, hay una asignación para cada conjunto de permisos. Elimine cualquier asignación de muestra que no sea necesaria. 8. Guarde y cierre el archivo `iam-identitycenter-assigments.json` .	

Implementación de los conjuntos de permisos y las asignaciones

Tarea	Descripción	Habilidades requeridas
Implemente los recursos en la cuenta de administrador delegado del IAM Identity Center.	1. En la cuenta de administrador delegado de IAM Identity Center, abra la consola de CloudFormation. 2. Implemente la plantilla `iam-identitycenter-pipeline.yaml` . Asigne a la pila un nombre claro y descriptivo y actualice los parámetros según las instrucciones. Para obtener instrucciones, consulte Crear una	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	pila en la CloudFormation documentación.	
Implemente los recursos en la cuenta AWS Organizations de administración.	1. Inicie sesión en la cuenta administrativa de la organización. 2. Abra la consola de AWS CloudFormation. 3. En la barra de navegación, elija el nombre del que se muestra actualmente Región de AWS. A continuación, elija la región `us-east-1` . Esta región es necesaria para que la `MoveAccount` EventBridge regla pueda detectar los AWS CloudTrail eventos asociados a los cambios en la organización. 4. Implemente la plantilla `iam-identitycenter-organization` . Asigne a la pila un nombre claro y descriptivo y actualice los parámetros según las instrucciones. Para obtener instrucciones, consulte Crear una pila en la CloudFormation documentación.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Finalizar la configuración del repositorio remoto.	Cambie el estado de la AWS CodeConnections conexión de `PENDING` a `AVAILABLE` . Esta conexión se creó al implementar la CloudFormation pila. Para obtener instrucciones, consulte Actualizar una conexión pendiente en la CodeConnections documentación.	DevOps ingeniero
Cargar archivos en el repositorio remoto.	Cargue todos los archivos que haya descargado del repositorio `aws-samples` y haya editado en los pasos anteriores al repositorio remoto. Los cambios en la ramificación `main` inician la canalización, que crea o actualiza los conjuntos de permisos y las asignaciones.	DevOps ingeniero

Actualización de los conjuntos de permisos y las asignaciones

Tarea	Descripción	Habilidades requeridas
Actualice los conjuntos de permisos y las asignaciones.	Cuando la EventBridge regla de `MoveAccount` Amazon detecta modificaciones en las cuentas de la organización, la CI/CD canalización se inicia automáticamente y actualiza los conjuntos de permisos. Por ejemplo, si añades una	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	cuenta a una unidad organizativa especificada en el archivo JSON de asignaciones, la CI/CD canalización aplicará el conjunto de permisos a la nueva cuenta. Si desea modificar los conjuntos de permisos y las asignaciones implementados, actualice los archivos JSON y, a continuación, confírmelos en el repositorio remoto. Tenga en cuenta lo siguiente cuando utilice la CI/CD canalización para administrar conjuntos de permisos y asociaciones implementados anteriormente: • Si cambias el nombre de un conjunto de permisos, la CI/CD canalización elimina el conjunto de permisos original y crea uno nuevo. • Esta canalización administra solo los conjuntos de permisos que tienen la etiqueta `SSOPipeline:true` . • Puede tener varios conjuntos de permisos y plantillas de asignación	

Tarea	Descripción	Habilidades requeridas
	en la misma carpeta del repositorio. • Si elimina una plantilla, la canalización eliminará la asignación o el conjunto de permisos. • Si elimina un bloque JSON de una asignación completa, la canalización eliminará la asignación del IAM Identity Center. • No puede eliminar un conjunto de permisos asignado a una Cuenta de AWS. En primer lugar, debe anular la asignación del conjunto de permisos.	

Resolución de problemas

Problema	Solución
Errores de acceso denegado	Confirme que tiene los permisos necesarios para implementar las CloudFormation plantillas y los recursos definidos en ellas. Para obtener más información, consulte Controlar el acceso en la CloudFormation documentación.
Errores de canalización en la fase de validación	Este error se muestra si hay algún error en el conjunto de permisos o en las plantillas de asignación. 1. En CodeBuild, consulte los detalles de la compilación.

Problema	Solución
	2. En el registro de compilación, busque el error de validación que proporciona más información sobre la causa del error de compilación. 3. Actualice el conjunto de permisos o las plantillas de asignación y, a continuación, consérvelos en el repositorio. 4. La CI/CD canalización reinicia el CodeBuild proyecto. Supervise el estado para confirmar que se ha resuelto el error de validación.

Recursos relacionados

- Conjuntos de permisos (documentación del IAM Identity Center)

Administrar credenciales mediante AWS Secrets Manager

Durga Prasad Cheepuri, Amazon Web Services

Resumen

Este patrón le guía en el uso de AWS Secrets Manager para obtener de forma dinámica las credenciales de bases de datos de una aplicación Java Spring.

En el pasado, cuando creaba una aplicación personalizada que recuperaba información desde una base de datos, normalmente tenía que incrustar las credenciales (el secreto) para obtener acceso a la base de datos directamente en la aplicación. Cuando llegaba el momento de cambiar las credenciales, había que invertir tiempo en actualizar la aplicación para utilizar las nuevas credenciales y, a continuación, distribuir la aplicación actualizada. Si tenía varias aplicaciones que compartían credenciales y se olvidaba de actualizar una de ellas, la aplicación dejaba de funcionar. Debido a este riesgo, muchos usuarios decidían no rotar sus credenciales periódicamente, lo que finalmente sustituye un riesgo por otro.

Secrets Manager le permite reemplazar las credenciales codificadas en el código (incluidas contraseñas), con una llamada a la API para recuperar el secreto mediante programación. Esto ayuda a garantizar la integridad del secreto si alguien examina el código, dado que el secreto sencillamente no está allí. Además, puede configurar Secrets Manager para rotar el secreto automáticamente de acuerdo con una programación especificada. Esto le permite reemplazar secretos a largo plazo con secretos a corto plazo, lo que contribuye a reducir significativamente el riesgo. Para obtener más información, consulte la documentación de AWS Secrets Manager.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS con acceso a Secrets Manager
- Una aplicación de Java Spring

Arquitectura

Pila de tecnología de origen

- Una aplicación Java Spring con código que acceda a una base de datos, con credenciales de base de datos administradas desde el archivo application.properties.

Pila de tecnología de destino

- Una aplicación Java Spring con código que acceda a una base de datos, con credenciales de base de datos administradas en Secrets Manager. El archivo application.properties contiene los secretos de Secrets Manager.

Integración de Secrets Manager en una aplicación

Tools (Herramientas)

- Secrets Manager: AWS Secrets Manager es un servicio de AWS que facilita la administración de los secretos. Los secretos pueden ser credenciales de base de datos, contraseñas, claves de API de terceros e incluso texto arbitrario. Puede almacenar y controlar el acceso a estos secretos de forma centralizada mediante la consola Secrets Manager, la interfaz de línea de comandos (CLI) de Secrets Manager o la API Secrets Manager y. SDKs

Epics

Almacenar el secreto en Secrets Manager

Tarea	Descripción	Habilidades requeridas
Almacene las credenciales como un secreto en Secrets Manager.	Almacene las credenciales de Amazon Relational Database Service (Amazon RDS) u otras credenciales de base de datos como un secreto en Secrets Manager; para ello, siga los pasos que se indican en Creating a secret (Crear un secreto) en la documentación de Secrets Manager.	Sys Admin
Establezca permisos para que la aplicación Spring acceda a Secrets Manager.	Establezca los permisos adecuados en función de cómo la aplicación	Sys Admin

Tarea	Descripción	Habilidades requeridas
	Java Spring utilice Secrets Manager. Para controlar el acceso al secreto, cree una política basada en la información proporcionada en la documentación de Secrets Manager, en las secciones Using identity-based policies (IAM Policies) and ABAC for Secrets Manager (Usar políticas basadas en identidad [políticas de IAM] y ABAC para Secrets Manager) y Using resource-based policies for Secrets Manager (Usar políticas basadas en recursos para Secrets Manager). Siga los pasos de la sección Retrieving the secret value (Recuperar el valor del secreto) de la documentación de Secrets Manager.	

Actualizar la aplicación Spring

Tarea	Descripción	Habilidades requeridas
Agregue dependencias JAR para usar Secrets Manager.	Para obtener más detalles, consulte la sección Información adicional.	Desarrollador de Java
Agregue los detalles del secreto a la aplicación Spring.	Actualice el archivo application.properties con el nombre del secreto, los puntos de conexión y la región de AWS.	Desarrollador de Java

Tarea	Descripción	Habilidades requeridas
	Para obtener ejemplos, consulte la sección Informaci ón adicional.	
Actualice el código de recuperación de credenciales de base de datos en Java.	En la aplicación, actualice el código Java que obtiene las credenciales de base de datos para obtener esos detalles de Secrets Manager. Para ver un código de ejemplo, consulte la sección Información adicional.	Desarrollador de Java

Recursos relacionados

- Documentación de AWS Secrets Manager
- Using identity-based policies (IAM Policies) and ABAC for Secrets Manager (Usar políticas basadas en identidad [políticas de IAM] y ABAC para Secrets Manager)
- Using resource-based policies for Secrets Manager (Usar políticas basadas en recursos para Secrets Manager)
- Código de muestra

Información adicional

Adding JAR dependencies for using Secrets Manager (Cómo agregar dependencias JAR para usar Secrets Manager)

Maven:

```
<groupId>com.amazonaws</groupId>
    <artifactId>aws-java-sdk-secretsmanager</artifactId>
    <version>1.11. 355 </version>
```

Gradle:

```
compile group: 'com.amazonaws', name: 'aws-java-sdk-secretsmanager', version:
 '1.11.355'
```

Updating the application.properties file with the details of the secret (Actualizar el archivo application.properties con los detalles del secreto)

```
spring.aws.secretsmanager.secretName=postgres-local
spring.aws.secretsmanager.endpoint=secretsmanager.us-east-1.amazonaws.com
spring.aws.secretsmanager.region=us-east-1
```

Updating the DB credentials retrieval code in Java (Actualizar el código de recuperación de credenciales de base de datos en Java.)

```
String  secretName  =  env.getProperty("spring.aws.secretsmanager.secretName");
String  endpoints  =  env.getProperty("spring.aws.secretsmanager.endpoint");
String  AWS Region  =  env.getProperty("spring.aws.secretsmanager.region");
AwsClientBuilder.EndpointConfiguration  config  =  new
  AwsClientBuilder.EndpointConfiguration(endpoints, AWS Region);
AWSSecretsManagerClientBuilder  clientBuilder  =
  AWSSecretsManagerClientBuilder.standard();
clientBuilder.setEndpointConfiguration(config);
AWSSecretsManager  client  =  clientBuilder.build();

ObjectMapper  objectMapper  =  new  ObjectMapper();

JsonNode  secretsJson  =  null;

ByteBuffer  binarySecretData;

GetSecretValueRequest  getSecretValueRequest  =  new
  GetSecretValueRequest().withSecretId(secretName);

GetSecretValueResult  getSecretValueResponse  =  null;

try  {
     getSecretValueResponse  =  client.getSecretValue(getSecretValueRequest);
    }

catch  (ResourceNotFoundException  e)  {
     log.error("The requested secret "  +  secretName  +  " was not found");
    }
```

```
catch  (InvalidRequestException  e)  {
     log.error("The request was invalid due to: "  +  e.getMessage());
     }

catch  (InvalidParameterException  e)  {
     log.error("The request had invalid params: "  +  e.getMessage());
     }
if  (getSecretValueResponse  ==  null)  {
     return  null;
     }  // Decrypted secret using the associated KMS key // Depending on whether the
 secret was a string or binary, one of these fields will be populated


String secret = getSecretValueResponse.getSecretString();

if (secret != null) {
     try {
                secretsJson  =  objectMapper.readTree(secret);
          }

     catch  (IOException  e)  {
                log.error("Exception while retrieving secret values: "  +
  e.getMessage());
          }
}

else  {
     log.error("The Secret String returned is null");

     return null;

     }
     String  host  =  secretsJson.get("host").textValue();
     String  port  =  secretsJson.get("port").textValue();
     String  dbname  =  secretsJson.get("dbname").textValue();
     String  username  =  secretsJson.get("username").textValue();
     String  password  =  secretsJson.get("password").textValue();
}
```

Supervise ElastiCache los clústeres de Amazon para comprobar el cifrado en reposo

Abhishek Agawane, Amazon Web Services

Resumen

Amazon ElastiCache es un servicio de Amazon Web Services (AWS) que proporciona una solución de almacenamiento en caché rentable, escalable y de alto rendimiento para distribuir un almacén de datos en memoria o un entorno de caché en la nube. Recupera datos de almacenes de datos en memoria de alto rendimiento y baja latencia. Esta funcionalidad lo convierte en una opción popular para casos de uso en tiempo real, como el almacenamiento en caché, los almacenes de sesiones, los juegos, los servicios geoespaciales, los análisis en tiempo real y las colas. ElastiCache ofrece los almacenes de datos de Redis y Memcached, los cuales ofrecen tiempos de respuesta inferiores a un milisegundo.

El cifrado de datos ayuda a evitar que usuarios no autorizados lean datos confidenciales disponibles en sus clústeres Redis y sus sistemas de almacenamiento en caché asociados. Esto incluye los datos guardados en medios persistentes, conocidos como datos en reposo y datos que pueden ser interceptados cuando recorren la red entre los clientes y los servidores de caché, conocidos como datos en tránsito.

Puede habilitar el cifrado en reposo para ElastiCache (Redis OSS) al crear un grupo de replicación configurando el parámetro en. `AtRestEncryptionEnabled` **`true`** Cuando este parámetro está habilitado, cifra el disco durante las operaciones de sincronización, copia de seguridad e intercambio, y cifra las copias de seguridad almacenadas en Amazon Simple Storage Service (Amazon S3). No puede habilitar el cifrado en reposo en un grupo de reproducción existente. Cuando cree un grupo de replicación, puede activar la encriptación en reposo de estas dos formas:

- Al seleccionar la opción Predeterminado, que utiliza el cifrado administrado por el servicio en reposo.
- Mediante una clave gestionada por el cliente y proporcionando el ID de clave o el nombre de recurso de Amazon (ARN) de AWS Key Management Service (AWS KMS).

Este patrón proporciona un control de seguridad que supervisa las llamadas a la API y genera un evento de Amazon EventBridge Events en la `CreateReplicationGroup` operación. Este evento llama a una AWS Lambda función que ejecuta un script de Python. La función obtiene el ID del

grupo de replicación de la entrada JSON del evento y realiza las siguientes comprobaciones para determinar si hay un clúster sin cifrar:

- Comprueba si la `AtRestEncryptionEnabled` clave existe.
- Si `AtRestEncryptionEnabled` existe, comprueba el valor para ver si existe`true`.
- Si el `AtRestEncryptionEnabled` valor está establecido en`false`, establece una variable que rastrea las infracciones y envía un mensaje de infracción a la dirección de correo electrónico que usted proporcione, mediante una notificación de Amazon Simple Notification Service (Amazon SNS).

Requisitos previos y limitaciones

Requisitos previos

- Una activa Cuenta de AWS.
- Un bucket de S3 para cargar el código de Lambda proporcionado.
- Una dirección de correo electrónico en la que desee recibir las notificaciones de infracciones.
- ElastiCache registro activado, para acceder a todos los registros de la API.

Limitaciones

- Este control de detección es regional y debe implementarse en todos los lugares Región de AWS que desee supervisar.
- El control es compatible con los grupos de replicación que se ejecutan en una nube privada virtual (VPC).
- El control admite grupos de replicación que ejecutan los siguientes tipos de nodos:
  - R7g, R6gd, R6g, R5, R4 y R3
  - M7g, M6g, M5, M4 y M3
  - T4g, T3, T2
  - C7gn

Versiones de producto

- Soporta ElastiCache (Redis OSS) la versión 3.2.6 o posterior y Valkey 7.2 o posterior

Arquitectura

Arquitectura de flujo de trabajo

1. El usuario lanza un grupo de ElastiCache replicación mediante una llamada a la API Consola de administración de AWS, la AWS Command Line Interface (AWS CLI) o una llamada a la API.
2. ElastiCache genera EventBridge eventos cuando se llama a la `CreateReplicationGroup` API.
3. Una EventBridge regla activa y llama a la función Lambda para comprobar el cumplimiento.
4. La función Lambda procesa el evento y comprueba si el cifrado en reposo está habilitado en el clúster. ElastiCache
5. Si se detecta una infracción de cifrado, la función Lambda publica un mensaje de notificación en un tema de SNS.
6. Amazon SNS envía una notificación por correo electrónico a los administradores sobre la infracción de conformidad con el cifrado.

Automatización y escala

- Si la está utilizando AWS Organizations, puede utilizarla AWS CloudFormation StackSetspara implementar esta plantilla en varias cuentas que desee supervisar.

Tools (Herramientas)

Servicios de AWS

- Amazon ElastiCache facilita la configuración, la administración y el escalado de los entornos de caché en memoria distribuidos en. Nube de AWS Proporciona una caché en memoria rentable, redimensionable y de alto rendimiento, a la vez que elimina la complejidad asociada a la implementación y la administración de un entorno de caché distribuida. ElastiCache funciona con los motores Redis y Memcached.
- AWS CloudFormationle ayuda a modelar y configurar sus AWS recursos, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Puede gestionar y aprovisionar pilas en varios Cuentas de AWS y. Regiones de AWS

- Amazon EventBridge ofrece un flujo casi en tiempo real de los eventos del sistema que describen los cambios en AWS los recursos. EventBridge se percata de los cambios operativos a medida que se producen y toma las medidas correctivas necesarias, enviando mensajes para responder al entorno, activando funciones, realizando cambios y recopilando información de estado.
- AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.
- Amazon SNS coordina y gestiona el envío de mensajes entre editores y clientes, incluidos los servidores web y las direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.

Código

El código de este patrón está disponible en el repositorio de cifrado GitHub Monitor Amazon ElastiCache Clusters for at-rest. Consulta la sección de Epics para obtener información sobre cómo usar los archivos del repositorio.

Prácticas recomendadas

Implementación

- Asegúrese de registrar las AWS CloudTrail llamadas a la ElastiCache API antes de implementar este control.
- Se trata de un control regional; despliega el control en cada Región de AWS lugar donde lo utilices ElastiCache.
- Valide la solución en dev/test los entornos antes de implementarla en producción.

Seguridad

- Para mejorar el control de las claves de cifrado, utilice las claves KMS administradas por el cliente.
- Revise los permisos AWS Identity and Access Management (IAM) para garantizar el acceso con privilegios mínimos para la función de ejecución de Lambda.
- Configure alertas para los mensajes que estén en la cola de mensajes muertos.

Operaciones

- Establezca una retención de registros adecuada para equilibrar las necesidades de cumplimiento con los costos.
- Ajuste la simultaneidad reservada de Lambda para ajustarla en función de ElastiCache su frecuencia de creación.
- Suscriba varias direcciones de correo electrónico a Amazon SNS para recibir notificaciones de equipo.

Supervisión

- Revisa CloudWatch las alarmas de Amazon para asegurarte de que los umbrales de alarma se ajustan a tus necesidades operativas.
- Supervise periódicamente la duración de la ejecución de las métricas Lambda y las tasas de error.
- Audite las infracciones con regularidad para revisar las notificaciones de conformidad con el cifrado.

Epics

Implementar el control de seguridad

Tarea	Descripción	Habilidades requeridas
Descarga el código de GitHub.	Clona o descarga el repositorio de código desde GitHub. El repositorio contiene los archivos `index.py` y `elasticache_encryption_at_rest.yml` .	Arquitecto de la nube
Cree paquetes de despliegue de Lambda.	Cree dos archivos.zip a partir del código de Python: • Crea `ElastiCache-EncryptionAtRest.zip` , que contiene `index.py`.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	• Utilice el siguiente comando : `zip ElastiCache-EncryptionAtRest.zip index.py`	
Cargue el código en un bucket de S3.	1. Cree un nuevo depósito de S3 o utilice un depósito de S3 existente para cargar el código Lambda. 2. Comprima el código Lambda (`index.py`) y asígnele un nombre. `ElastiCache-EncryptionAtRest.zip` 3. Cargue el archivo.zip en el bucket de S3. Este depósito debe estar en el Región de AWS mismo lugar que los recursos que desea evaluar.	Arquitecto de la nube
Implemente la CloudFormation plantilla.	Abre la CloudFormation consola en el Región de AWS mismo lugar que el bucket de S3 e implementa el `elasticache_encryption_at_rest.yml` archivo que se proporciona en el repositorio de código. En la siguiente Epic, proporcione los valores de los parámetros.	Arquitecto de la nube

Complete los parámetros de la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Proporcione el nombre del bucket de S3.	Escriba el nombre del bucket de S3 que ha creado o seleccionado en la primera Epic. Este bucket de S3 contiene el archivo.zip del código Lambda y debe estar en el Región de AWS mismo lugar que la plantilla y CloudFormation el recurso que se van a evaluar.	Arquitecto de la nube
Proporcione la clave de S3.	Proporcione la ubicación del archivo .zip del código de Lambda en su bucket de S3, sin barras diagonales iniciales (por ejemplo, `ElasticCache-EncryptionAtRest.zip` o `controls/ElasticCache-EncryptionAtRest.zip`).	Arquitecto de la nube
Proporcione una dirección de correo electrónico.	Proporcione una dirección de correo electrónico activa en la que desee recibir notificaciones de infracciones.	Arquitecto de la nube
Especifique un nivel de registro.	Especifique el nivel de registro y la verbosidad. • `Info`designa mensajes informativos detallados sobre el progreso de la aplicación y solo debe usarse para la depuración.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	• `Error`designa los eventos de error que aún podrían permitir que la aplicación siguiera ejecutándose. • `Warning`designa situacion es potencialmente dañinas.	

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirme la suscripción de correo electrónico.	Cuando la CloudFormation plantilla se implementa correctamente, envía un mensaje de suscripción a la dirección de correo electrónico que has proporcionado. Debe confirmar esta suscripción de correo electrónico para recibir notificaciones.	Arquitecto de la nube

Resolución de problemas

Problema	Solución
La función Lambda no se ha activado	Síntoma: no se inicia sesión CloudWatch después de crear o modificar ElastiCache los clústeres. Soluciones: • Compruebe el estado de la EventBridge regla:

Problema	Solución
	`aws events describe-rule --name <rule-name>` • Confirme que la política de Lambda basada en recursos permite la invocación. EventBridge • Confirme que el patrón de EventBridge eventos coincide con las llamadas a la API. ElastiCache
No hay notificaciones por correo electrónico	Síntoma: la función Lambda se ejecuta correctamente, pero no recibe ninguna notificación por correo electrónico. Soluciones: • Confirma tu suscripción a Amazon SNS a través del enlace de confirmación por correo electrónico. • Revisa las carpetas de spam o correo basura para ver si hay correos electrónicos de Amazon SNS. • Compruebe el nombre del recurso de Amazon (ARN) para el tema Amazon SNS en la variable de entorno Lambda: `OUTBOUND_TOPIC_ARN` • Pruebe Amazon SNS manualmente: `aws sns publish --topic-arn <arn> --message "Test"`

Problema	Solución
Problemas con los permisos	Síntoma: errores de acceso denegado en los registros de funciones Lambda. CloudWatch Soluciones: • Compruebe que la función de ejecución de Lambda tenga los permisos de ElastiCache lectura necesarios. • Confirme que la política AWS KMS clave incluye la función de ejecución de Lambda. • Asegúrese de que la política de temas de Amazon SNS permita a Lambda publicar.

Recursos relacionados

- Cree una pila desde la CloudFormation consola (documentación)CloudFormation
- Cifrado en reposo en ElastiCache (Redis OSS) (ElastiCache documentación)

Supervisar la actividad del usuario raíz de IAM

JJ Sung y Mostefa Brougui, Amazon Web Services

Resumen

Cada cuenta de Amazon Web Services (AWS) tiene un usuario raíz. Como práctica de seguridad recomendada para AWS Identity and Access Management (IAM), se aconseja utilizar el usuario raíz para realizar las tareas que solo este puede llevar a cabo. Para ver la lista completa, consulte Tareas que requieren credenciales de usuario raíz en Guía de referencia de administración de la cuenta de AWS. Como el usuario raíz tiene acceso absoluto a todos los recursos e información de facturación de AWS, recomendamos que no se utilice esta cuenta y que se supervise para detectar cualquier actividad, ya que podría indicar que las credenciales del usuario raíz se han visto comprometidas.

Con este patrón, se configura una arquitectura basada en eventos que supervisa al usuario raíz de IAM. Este patrón configura una hub-and-spoke solución que monitorea varias cuentas de AWS, las cuentas radiales, y centraliza la administración y los informes en una sola cuenta, la cuenta hub.

Cuando se utilizan las credenciales del usuario raíz de IAM, Amazon CloudWatch y AWS CloudTrail registran la actividad en el registro y en el registro, respectivamente. En la cuenta radial, una EventBridge regla de Amazon envía el evento al bus de eventos central de la cuenta hub. En la cuenta hub, una EventBridge regla envía el evento a una función de AWS Lambda. La función utiliza un tema de Amazon Simple Notification Service (Amazon SNS) que notifica la actividad del usuario raíz.

En este patrón, se utiliza una CloudFormation plantilla de AWS para implementar los servicios de supervisión y gestión de eventos en las cuentas radiales. Utiliza una plantilla de HashiCorp Terraform para implementar los servicios de notificación y gestión de eventos en la cuenta central.

Requisitos previos y limitaciones

Requisitos previos

1. Permisos para implementar recursos de AWS en el entorno de AWS.
2. Permisos para implementar conjuntos de pilas CloudFormation . Para obtener más información, consulte Requisitos previos para las operaciones de conjuntos de pilas (CloudFormation documentación).
3. Terraform instalado y listo para su uso. Para obtener más información, consulte Introducción - AWS (documentación de Terraform).

4. Un registro de seguimiento existente en cada cuenta spoke. Para obtener más información, consulte Introducción a AWS CloudTrail (CloudTrail documentación).
5. La ruta está configurada para enviar eventos a CloudWatch Logs. Para obtener más información, consulte Enviar eventos a CloudWatch los registros (CloudTrail documentación).
6. AWS Organizations debe administrar las cuentas hub y spoke.

Arquitectura

En el diagrama siguiente se muestran los componentes básicos de la implementación.

1. Cuando se utilizan las credenciales del usuario raíz de IAM, CloudWatch CloudTrail registre la actividad en el registro y en el registro, respectivamente.
2. En la cuenta radial, una EventBridge regla envía el evento al bus de eventos central de la cuenta central.
3. En la cuenta hub, una EventBridge regla envía el evento a una función Lambda.
4. La función de Lambda utiliza un tema de Amazon SNS que notifica la actividad del usuario raíz.

Tools (Herramientas)

Servicios de AWS

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS le CloudTrail ayuda a auditar la gobernanza, el cumplimiento y el riesgo operativo de su cuenta de AWS.
- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas, aplicaciones y servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, las funciones de AWS Lambda, los puntos de conexión de invocación HTTP que utilizan destinos de API o los buses de eventos de otras cuentas de AWS.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.

- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.

Otras herramientas y servicios

- Terraform es una aplicación de CLI para aprovisionar y administrar la infraestructura y los recursos de la nube mediante el uso de código, en forma de archivos de configuración.

Repositorio de código

El código fuente y las plantillas de este patrón están disponibles en un GitHub repositorio. Este patrón proporciona dos plantillas:

- Una plantilla de Terraform que contiene los recursos que se despliegan en la cuenta hub
- Una CloudFormation plantilla que se implementa como una instancia de conjunto de pilas en las cuentas de Spoke

El repositorio tiene la estructura siguiente.

```
.
 |__README.md
 |__spoke-stackset.yaml
 |__hub.tf
 |__root-activity-monitor-module
     |__main.tf  # contains Terraform code to deploy resources in the Hub account
     |__iam      # contains IAM policies JSON files
         |__ lambda-assume-policy.json          # contains trust policy of the IAM role
 used by the Lambda function
         |__ lambda-policy.json                 # contains the IAM policy attached to
 the IAM role used by the Lambda function
     |__outputs  # contains Lambda function zip code
```

La sección Epics proporciona step-by-step instrucciones para implementar las plantillas.

Epics

Implementar recursos en la cuenta hub

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código de muestra.	1. Abra el repositorio AWS IAM Root User Activity Monitor. 2. En la pestaña Code (Código), situada encima de la lista de archivos, seleccione Code y, a continuación, copie la URL HTTPS. 3. En una interfaz de la línea de comandos, cambie el directorio de trabajo a la ubicación en la que desee almacenar los archivos de muestra. 4. Introduzca el siguiente comando: `git clone <repoURL>`	AWS general
Actualice la plantilla de Terraform.	1. Recupere el ID de su organización. Para obtener instrucciones, consulte Viewing the details of an organization from the management account (Ver detalles de una organizac ión desde la cuenta de administración) (document	AWS general

Tarea	Descripción	Habilidades requeridas
	ación de AWS Organizat ions). 2. En el repositorio clonado, abra `hub.tf`. 3. Actualice lo siguiente con los valores adecuados para su entorno: • `OrganizationId` : Agregue el ID de su organización. • `SNSTopicName` : Agregue el nombre del tema de Amazon SNS. • `SNSSubscriptions` : Agregue el correo electrónico al que deben enviarse las notificac iones de Amazon SNS. • `Region`: Agregue el código de región de AWS en el que va a implement ar los recursos. Por ejemplo, `eu-west-1` . • `Tags`: Agregue sus etiquetas. Para obtener más información, consulte Etiquetado de recursos de AWS (Referencia general de AWS). 4. Guarde y cierre el archivo `hub.tf`.	

Tarea	Descripción	Habilidades requeridas

Implemente los recursos en la cuenta hub de AWS.	1. En la interfaz de la línea de comandos de Terraform, vaya hasta la carpeta raíz del repositorio clonado e ingrese el comando siguiente.
	`terraform init && terraform plan`
	2. Revise la salida y confirme que desea crear los recursos descritos.
	3. Escriba el siguiente comando.
	`terraform apply`
	4. Cuando se le solicite, especifique `yes` para confirmar la implement ación.
		AWS general

Implementar recursos en sus cuentas spoke

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla.	1. Inicie sesión en la consola de administración de AWS y abra la consola de CloudFormation . 2. En el panel de navegación, seleccione StackSets.	AWS general

Tarea	Descripción	Habilidades requeridas
	3. En la parte superior de la StackSetspágina, seleccion a Crear StackSet. 4. En Permisos, selecciona Permisos gestionados por el servicio. CloudFormation configura automáticamente los permisos necesarios para realizar la implement ación en las cuentas de destino administradas por AWS Organizations. 5. En Requisito previo - Preparación de la plantilla , seleccione Template is ready (La plantilla está lista). 6. En Especificar plantilla , seleccione Cargar un archivo de plantilla. 7. Seleccione Choose file (Elegir archivo) y, a continuación, en el repositor io clonado, seleccione `spoke-stackset.yam l` . 8. Elija Siguiente. 9. En la página Especific ar StackSet detalles, introduzca un nombre para el conjunto de pilas. 10. En Parameters, especifique el ID de cuenta de la cuenta	

Tarea	Descripción	Habilidades requeridas
	hub y, a continuación, seleccione Next (Siguiente). 11. En la página Configura r StackSet opciones, en Etiquetas, añada sus etiquetas. 12. En Execution configuration (Configuración de ejecución), seleccione Inactive y, a continuación, selecciona Next (Siguiente). 13. En la página Cómo establecer opciones de implementación, especifiq ue las unidades organizat ivas y las regiones en las que desea implementar el conjunto de pilas y, a continuación, seleccione Siguiente. 14. En la página de revisión, seleccione Acepto que AWS CloudFormation podría crear recursos de IAM y, a continuación, elija Enviar. CloudFormation comienza a implementar su conjunto de pilas. Para obtener más informaci ón e instrucciones, consulte Crear un conjunto de pilas	

Tarea	Descripción	Habilidades requeridas
	(CloudFormation documentación).	

(Opcional) Probar las notificaciones

Tarea	Descripción	Habilidades requeridas
Utilice las credenciales de usuario raíz.	1. Inicie sesión en una cuenta spoke o en la cuenta hub con las credenciales de usuario raíz. 2. Confirme que la cuenta de correo electrónico que especificó reciba la notificación de Amazon SNS.	AWS general

Recursos relacionados

- Prácticas recomendadas de seguridad (documentación de IAM)
- Trabajar con StackSets (CloudFormation documentación)
- Introducción (documentación de Terraform)

Información adicional

Amazon GuardDuty es un servicio de supervisión continua de la seguridad que analiza y procesa los registros para identificar actividades inesperadas y potencialmente no autorizadas en su entorno de AWS. Como alternativa a esta solución, si la tiene habilitada GuardDuty, puede avisarle cuando se hayan utilizado las credenciales del usuario raíz. El GuardDuty resultado es`Policy:IAMUser/RootCredentialUsage`, y la gravedad predeterminada es baja. Para obtener más información, consulta Cómo gestionar GuardDuty los hallazgos de Amazon.

Enviar una notificación cuando se cree un usuario de IAM

Mansi Suratwala y Sergiy Shevchenko, Amazon Web Services

Resumen

En Amazon Web Services (AWS), puede usar este patrón para implementar una CloudFormation plantilla de AWS para recibir notificaciones automáticamente cuando se creen usuarios de AWS Identity and Access Management (IAM).

Con IAM, puede administrar el acceso a los servicios y recursos de AWS de forma segura. Puede crear y administrar usuarios y grupos de AWS, y utilizar permisos para permitir y denegar a dichos usuarios y grupos el acceso a los recursos de AWS.

La CloudFormation plantilla crea un evento de Amazon CloudWatch Events y una función de AWS Lambda. El evento usa AWS CloudTrail para monitorear cualquier usuario de IAM que se esté creando en la cuenta de AWS. Si se crea un usuario, el evento CloudWatch Events inicia una función Lambda, que le envía una notificación de Amazon Simple Notification Service (Amazon SNS) informándole del nuevo evento de creación del usuario.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Creación e implementación de una CloudTrail ruta de AWS

Limitaciones

- La CloudFormation plantilla de AWS debe implementarse `CreateUser` únicamente para.

Arquitectura

Pila de tecnología de destino

- IAM
- AWS CloudTrail
- CloudWatch Eventos de Amazon

- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon SNS

Arquitectura de destino

Automatización y escala

Puede utilizar la CloudFormation plantilla de AWS varias veces para distintas regiones y cuentas de AWS. Debe ejecutarla solo una vez en cada región o cuenta. Para automatizar la implementación en varias cuentas, utilice AWS CloudFormation StackSets. La CloudFormation plantilla podrá implementar todos los recursos necesarios en cada cuenta.

Tools (Herramientas)

Herramientas

- IAM: AWS Identity and Access Management (IAM) es un servicio web que le ayuda a controlar de forma segura el acceso a los recursos de AWS. Utilice IAM para controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos.
- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar sus recursos de Amazon Web Services para que pueda dedicar menos tiempo a gestionar esos recursos y más a centrarse en las aplicaciones que se ejecutan en AWS. Cree una plantilla que describa todos los recursos de AWS que desee y CloudFormation se encarga de aprovisionar y configurar esos recursos por usted.
- AWS CloudTrail: AWS le CloudTrail ayuda a gestionar la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de su cuenta de AWS. Las acciones realizadas por un usuario, un rol o un servicio de AWS se registran como eventos en CloudTrail. Los eventos incluyen las acciones realizadas en la consola de administración de AWS, la interfaz de línea de comandos de AWS y AWS SDKs y APIs.
- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece una near-real-time secuencia de eventos del sistema que describen los cambios en los recursos de AWS.
- AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.

- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) es un servicio gestionado que proporciona la entrega de mensajes mediante Lambda, HTTP, correo electrónico, notificaciones push móviles y mensajes de texto móviles (SMS).

Código

El archivo .zip del proyecto está disponible como adjunto.

Epics

Cree el bucket de S3 para el script de Lambda

Tarea	Descripción	Habilidades requeridas
Defina el bucket de S3.	Abra la consola de Amazon S3 y elija o cree un bucket de S3. Este bucket de S3 alojará el archivo .zip de código de Lambda. El nombre del bucket de S3 no puede incluir barras diagonales iniciales.	Arquitecto de la nube

Cómo cargar el código de Lambda en el bucket de S3

Tarea	Descripción	Habilidades requeridas
Cargue el código de Lambda.	Cargue el archivo .zip de código de Lambda que se proporciona en la sección Adjuntos en el bucket de S3 que haya definido.	Arquitecto de la nube

Implemente la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla.	En la CloudFormation consola, implementa la CloudFormation `createIAMuser.yaml` plantilla que se proporcio na como adjunto a este patrón. En la siguiente Epic, proporcione los valores de los parámetros.	Arquitecto de la nube

Complete los parámetros de la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Proporcione el nombre del bucket de S3.	Escriba el nombre de bucket de S3 que ha creado o elegido en la primera Epic.	Arquitecto de la nube
Proporcione la clave de S3.	Proporcione la ubicación del archivo .zip del código de Lambda en su bucket de S3 sin barras diagonales iniciales (por ejemplo, `<directory>/<file-name>.zip`).	Arquitecto de la nube
Proporcione una dirección de correo electrónico.	Proporcione una dirección de correo electrónico activa en la que desea recibir las notificac iones de Amazon SNS.	Arquitecto de la nube
Defina el nivel de registro.	Defina el nivel y la frecuenci a de registro de la función de Lambda. `Info` designa mensajes informativos	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	detallados sobre el progreso de la aplicación. `Error` designa los eventos de error que aún podrían permitir que la aplicación siguiera ejecutándose. `Warning` designa situaciones potencial mente dañinas.	

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la plantilla se implementa correctamente, se envía un mensaje de correo electrónico de suscripción a la dirección de correo electróni co proporcionada. Debe confirmar esta suscripción de correo electrónico para recibir notificaciones.	Arquitecto de la nube

Recursos relacionados

- Creación de un registro de seguimiento
- Crear un bucket de S3
- Carga de archivos en un bucket de S3
- Implementación de una CloudFormation plantilla
- Creación de un usuario de IAM
- Crear una regla de CloudWatch eventos que se active en una llamada a la API de AWS mediante AWS CloudTrail

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Impedir el acceso a Internet de las cuentas mediante una política de control de servicios

Sergiy Shevchenko, Sean O'Sullivan y Victor Mazeo Whitaker, Amazon Web Services

Resumen

Con frecuencia, las organizaciones quieren limitar el acceso a Internet para los recursos de las cuentas que deben permanecer privados. En estas cuentas, los recursos de las nubes privadas virtuales (VPCs) no deberían acceder a Internet de ninguna manera. Muchas organizaciones eligen una arquitectura de inspección centralizada. En el caso del tráfico este-oeste (de VPC a VPC) en una arquitectura de inspección centralizada, debe asegurarse de que las cuentas radiales y sus recursos no tengan acceso a Internet. En el caso del tráfico norte-sur (salida a Internet y entornos en las instalaciones), se recomienda permitir el acceso a Internet únicamente a través de la VPC de inspección.

Este patrón utiliza una política de control de servicios (SCP) para evitar el acceso a Internet. Puede aplicar esta SCP a las cuentas o a las unidades organizativas (UO). La SCP limita la conectividad a Internet al impedir lo siguiente:

- Crear o adjuntar una puerta de enlace IPv6 a Internet IPv4 o una puerta de enlace que permita el acceso directo a Internet a la VPC
- Crear o aceptar una conexión de emparejamiento de VPC que pueda permitir el acceso indirecto a Internet a través de otra VPC
- Crear o actualizar una configuración de AWS Global Accelerator que pueda permitir que los recursos de la VPC tengan acceso directo a Internet.

Requisitos previos y limitaciones

Requisitos previos

- Una o varias Cuentas de AWS administradas como una organización en. AWS Organizations
- Todas las funciones están habilitadas en AWS Organizations.
- SCPs están habilitadas en la organización.
- Permisos para:
  - Acceda a la cuenta de administración de su organization.

- Crear SCPs. Para obtener más información sobre los permisos mínimos, consulte Creating an SCP.
- Adjunta el SCP a las cuentas o unidades organizativas de destino (OUs). Para obtener más información sobre los permisos mínimos, consulte Attaching and detaching service control policies.

Limitaciones

- SCPs no afectan a los usuarios ni a las funciones de la cuenta de administración. Afectan solo a las cuentas de miembro de su organización.
- SCPs afectan únicamente a los usuarios y roles AWS Identity and Access Management (de IAM) gestionados por las cuentas que forman parte de la organización. Para más información, consulte Efectos de las SCP en los permisos.

Tools (Herramientas)

Servicios de AWS

- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar múltiples cuentas Cuentas de AWS en una organización que puede crear y administrar de forma centralizada. En este patrón, se utilizan las políticas de control de servicios (SCPs) en AWS Organizations.
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Prácticas recomendadas

Tras establecer este SCP en su organización, asegúrese de actualizarlo con frecuencia para abordar cualquier novedad Servicios de AWS o función que pueda afectar al acceso a Internet.

Epics

Creación y conexión de la SCP

Tarea	Descripción	Habilidades requeridas
Cree la SCP.	1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión en la cuenta de administración de la organización. 2. En el panel izquierdo, elija Políticas. 3. En la pestaña de políticas , seleccione Políticas de control de servicios. 4. En la página Políticas de control de servicios, seleccione Crear política. 5. En la página Crear nueva política de control de servicios, ingrese un Nombre de la política y una Descripción de la política (opcional). 6. (Opcional) Agregue etiquetas de AWS a la política. 7. En el editor JSON, elimine la política de marcadores de posición. 8. Pegue la siguiente política de en el editor JSON. `{`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas

	<pre>{
	  "Version":
	 "2012-10-17",
	  "Statement": [
	  {
	  "Action": [
	  "ec2:Atta
	chInternetGateway",
	  "ec2:Crea
	teInternetGateway",
	
	  "ec2:Crea
	teVpcPeeringConnec
	tion",
	  "ec2:Acce
	ptVpcPeeringConnec
	tion",
	  "ec2:Crea
	teEgressOnlyIntern
	etGateway"
	  ],
	  "Resource":
	 "*",
	  "Effect": "Deny"
	  },
	  {
	  "Action": [
	  "globalac
	celerator:Create*",
	  "globalac
	celerator:Update*"
	  ],
	  "Resource":
	 "*",
	  "Effect": "Deny"
	  }
	  ]
	}</pre>
	9. Elija Crear política.	

Tarea	Descripción	Habilidades requeridas
Adjunte la SCP.	1. En la página Políticas de control de servicios, elija la política que creó. 2. En la pestaña Objetivos, seleccione Adjuntar. 3. Seleccione la cuenta o UO a la que desea adjuntar la política. Puede que tenga que ampliarlo OUs para encontrar la unidad organizativa o la cuenta que desee. 4. Elija Asociar política.	Administrador de AWS

Recursos relacionados

- AWS Organizations documentación
- Políticas de control de servicios (SCPs)
- Arquitectura de inspección centralizada con AWS Gateway Load Balancer y AWS Transit Gateway (entrada del AWS blog)

Exporte un informe de las identidades de AWS IAM Identity Center y sus asignaciones mediante PowerShell

Jorge Pava, Frank Allotta, Manideep Reddy Gillela y Chad Miles, Amazon Web Services

Resumen

Cuando utiliza AWS IAM Identity Center (sucesor de AWS Single Sign-On) para gestionar de forma centralizada el acceso de inicio de sesión único (SSO) a todas sus cuentas y aplicaciones en la nube de Amazon Web Services (AWS), informar y auditar esas asignaciones a través de la consola de administración de AWS puede resultar tedioso y llevar mucho tiempo. Esto es especialmente cierto si está informando sobre los permisos de un usuario o grupo en docenas o cientos de cuentas de AWS.

Para muchos, la herramienta ideal para ver esta información sería en una aplicación de hoja de cálculo, como Microsoft Excel. Esto puede ayudarle a filtrar, buscar y visualizar los datos de toda su organización, gestionados por AWS Organizations.

Este patrón describe cómo utilizar las herramientas de AWS PowerShell para generar un informe de las configuraciones de identidad de SSO en el Centro de identidades de IAM. El informe tiene el formato de un archivo CSV e incluye el nombre de la identidad (entidad principal), el tipo de identidad (usuario o grupo), las cuentas a las que la identidad puede acceder y los conjuntos de permisos. Tras generar este informe, puede abrirlo en la aplicación que prefiera para buscar, filtrar y auditar los datos según sea necesario. En la siguiente imagen se muestran datos de muestra en una aplicación de hoja de cálculo.

Importante: dado que este informe contiene información confidencial, le recomendamos encarecid amente que la almacene de forma segura y que la comparta solo de forma need-to-know puntual.

Requisitos previos y limitaciones

Requisitos previos

- IAM Identity Center y AWS Organizations, configurados y habilitados.
- PowerShell instalado y configurado Para obtener más información, consulte Instalación PowerShell (documentación de Microsoft).

- Herramientas de AWS para PowerShell, instaladas y configuradas. Por motivos de rendimiento, le recomendamos encarecidamente que instale la versión modularizada de las herramientas de AWS para PowerShell, llamada. `AWS.Tools` Cada servicio de AWS es compatible con su pequeño módulo propio. En el PowerShell shell, introduzca los siguientes comandos para instalar los módulos necesarios para este patrón:`AWS.Tools.Installer`, `OrganizationsSSOAdmin`, y. `IdentityStore`

```
Install-Module AWS.Tools.Installer
Install-AWSToolsModule -Name Organizations, SSOAdmin, IdentityStore
```

  Para obtener más información, consulte Instalar AWS.Tools en Windows o Instalar AWS.Tools en Linux o macOS (AWS Tools para obtener documentación). PowerShell Si recibe un error al instalar los módulos, consulte la sección de Solución de problemas de este patrón.

- Interfaz de la línea de comandos de AWS (AWS CLI) o AWS SDK se deben configurar previamente con credenciales de trabajo mediante una de las siguientes acciones:
  - Utilice `aws configure` de CLI de AWS. Para obtener más información, consulte Configuración rápida (documentación de la CLI de AWS).
  - Configure la CLI de AWS o el AWS Cloud Development Kit (AWS CDK) para obtener acceso temporal a través de un rol de AWS Identity and Access Management (IAM). Para obtener más información, consulte Obtener credenciales de rol de IAM para acceder a la CLI (documentación del IAM Identity Center).
- Un perfil con nombre para la AWS CLI que ha guardado las credenciales de una entidad principal de IAM que:
  - Tiene acceso a la cuenta de administración de AWS Organizations o a la cuenta de administrador delegado para IAM Identity Center
  - Tiene aplicadas las políticas administradas de AWS `AWSSSOReadOnly` y `AWSSSODirectoryReadOnly`

  Para obtener más información, consulte Uso de perfiles con nombre (documentación de CLI de AWS) y políticas administradas de AWS (documentación de IAM).

Limitaciones

- Las cuentas de AWS de destino deben administrarse como una organización en AWS Organizations.

Versiones de producto

- Para todos los sistemas operativos, se recomienda utilizar la PowerShell versión 7.0 o posterior.

Arquitectura

Arquitectura de destino

1. El usuario ejecuta el script en una línea de PowerShell comandos.
2. El script asume el perfil indicado para la CLI de AWS. Esto le da acceso al Centro de identidades de IAM.
3. El script recupera las configuraciones de identidad del SSO del IAM Identity Center.
4. El script genera un archivo CSV en el mismo directorio de la estación de trabajo en las instalaciones donde se guarda el script.

Tools (Herramientas)

Servicios de AWS

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- AWS IAM Identity Center le ayuda a gestionar de forma centralizada el acceso de inicio de sesión único (SSO) a todas sus cuentas y aplicaciones en la nube de AWS.
- Las herramientas de AWS PowerShell son un conjunto de PowerShell módulos que le ayudan a programar operaciones en sus recursos de AWS desde la línea de PowerShell comandos.

Otras herramientas

- PowerShelles un programa de administración de automatización y configuración de Microsoft que se ejecuta en Windows, Linux y macOS.

Epics

Genere el informe

Tarea	Descripción	Habilidades requeridas
Preparación del script.	1. Copie el PowerShell script en la sección de información adicional de este patrón. 2. En la sección `Param`, en su entorno de AWS, defina los valores de las siguientes variables: • `OutputFile` : el nombre de archivo del informe. • `ProfileName` : el perfil con nombre de la AWS CLI que desea utilizar para generar el informe. • `Region`: la Región de AWS en la que se implementa IAM Identity Center. Para obtener una lista completa de las regiones y sus códigos, consulte Puntos de conexión regionales. 3. Guarde el script con el nombre de archivo `SSO-Report.ps1` .	Administrador de la nube
Ejecute el script.	Se recomienda ejecutar el script personalizado en el PowerShell shell con el siguiente comando.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas

	`.\SSO-Report.ps1`
	
	Si lo desea, también puede ejecutar el script desde otro intérprete de comandos introduciendo el siguiente comando.
	
	`pwsh .\SSO-Report.ps1`
	
	El script genera un archivo CSV en el mismo directorio que el archivo de script.	

Analice los datos de los informes.	El archivo CSV de salida tiene los encabezados AccountNamePermissionSet, Principal y Tipo. Abra este archivo en la aplicación de hojas de cálculo que prefiera. Puede crear una tabla de datos para filtrar y ordenar la salida.	Administrador de la nube

Resolución de problemas

Problema	Solución
Error `The term 'Get-<parameter>' is not recognized as the name of a cmdlet, function, script file, or operable program.`	Las herramientas de AWS PowerShell o sus módulos no están instalados. En el PowerShell shell, introduzca los siguientes comandos para instalar las herramientas de AWS PowerShell y los módulos necesarios para este patrón: `AWS.Tools.Installer` `Organizations` ,`SSOAdmin`, `yIdentityStore` .

Problema	Solución
	`Install-Module AWS.Tools.Installer` `Install-AWSToolsModule -Name Organizations, SSOAdmin, IdentityStore`
Error `No credentials specified or obtained from persisted/shell defaults`	En la sección Preparación del script, en la sección Epics, confirme que ha introducido correctamente las variables `ProfileName` y `Region`. Asegúrese de que la configuración y las credenciales del perfil indicado tengan permisos suficientes para administrar el IAM Identity Center.
Error `Authenticode Issuer …` al instalar los módulos de AWS.Tools	Agregue el parámetro `-SkipPublisherCheck` al final del comando `Install-AWSToolsModule`.

Problema	Solución

Error `Get-ORGAccountList : Assembly AWSSDK.SSO could not be found or loaded.`	Este error puede producirse cuando se especifican perfiles de CLI de AWS con nombre, la CLI de AWS se configura para autenticar a los usuarios con el Centro de identidad de IAM y la CLI de AWS se configura para recuperar automáticamente los tokens de autenticación actualizados. Para corregir este error, haga lo siguiente:
	1. Introduzca el siguiente comando para confirmar que los módulos `SSO` y `SSOOIDC` están instalados.
	`Install-AWSToolsModule SSO, SSOOIDC`
	2. Inserte las siguientes líneas en el script situado debajo del bloque `param()`.
	`Import-Module AWS.Tools.SSO`
	`Import-Module AWS.Tools.SSOOIDC`

Recursos relacionados

- ¿Dónde se almacenan las opciones de configuración? (documentación de la CLI de AWS)
- Configurar la CLI de AWS para usar AWS IAM Identity Center (documentación de la CLI de AWS)
- Uso de perfiles con nombre (documentación de la CLI de AWS)

Información adicional

En el siguiente script, determine si necesita actualizar los valores de los siguientes parámetros:

- Si utiliza un perfil con nombre en la AWS CLI para acceder a la cuenta en la que está configurado el Centro de identidades de IAM, actualice el valor `$ProfileName`.

- Si el Centro de identidades de IAM se implementa en una región de AWS diferente a la región predeterminada para la configuración de AWS CLI o SDK de AWS, actualice el valor `$Region` para usar la región en la que está implementado el Centro de identidades de IAM.
- Si no se da ninguna de estas situaciones, no será necesario actualizar el script.

```
param (
    # The name of the output CSV file
    [String] $OutputFile  = "SSO-Assignments.csv",
    # The AWS CLI named profile
    [String] $ProfileName = "",
    # The AWS Region in which IAM Identity Center is configured
    [String] $Region      = ""
)
$Start = Get-Date; $OrgParams = @{}
If ($Region){ $OrgParams.Region = $Region}
if ($ProfileName){$OrgParams.ProfileName = $ProfileName}
$SSOParams   = $OrgParams.Clone(); $IdsParams = $OrgParams.Clone()
$AccountList = Get-ORGAccountList @OrgParams | Select-Object Id, Name
$SSOinstance = Get-SSOADMNInstanceList @OrgParams
$SSOParams['InstanceArn']       = $SSOinstance.InstanceArn
$IdsParams['IdentityStoreId']   = $SSOinstance.IdentityStoreId
$PSsets       = @{}; $Principals   = @{}
$Assignments  = @(); $AccountCount = 1; Write-Host ""
foreach ($Account in $AccountList) {
    $Duration = New-Timespan -Start $Start -End (Get-Date) | ForEach-Object
 {[Timespan]::New($_.Days, $_.Hours, $_.Minutes, $_.Seconds)}
    Write-Host "`r$Duration - Account $AccountCount of $($AccountList.Count)
 (Assignments:$($Assignments.Count))        " -NoNewline
    $AccountCount++
    foreach ($PS in Get-SSOADMNPermissionSetsProvisionedToAccountList -AccountId
 $Account.Id @SSOParams) {
        if (-not $PSsets[$PS]) {$PSsets[$PS] = (Get-SSOADMNPermissionSet @SSOParams -
PermissionSetArn $PS).Name;$APICalls++}
        $AssignmentsResponse = Get-SSOADMNAccountAssignmentList @SSOParams -
PermissionSetArn $PS -AccountId $Account.Id
        if ($AssignmentsResponse.NextToken) {$AccountAssignments =
 $AssignmentsResponse.AccountAssignments}
        else {$AccountAssignments = $AssignmentsResponse}
        While ($AssignmentsResponse.NextToken) {
            $AssignmentsResponse = Get-SSOADMNAccountAssignmentList @SSOParams -
PermissionSetArn $PS -AccountId $Account.Id -NextToken $AssignmentsResponse.NextToken
            $AccountAssignments += $AssignmentsResponse.AccountAssignments}
```

```
        foreach ($Assignment in $AccountAssignments) {
            if (-not $Principals[$Assignment.PrincipalId]) {
                $AssignmentType = $Assignment.PrincipalType.Value
                $Expression     = "Get-IDS"+$AssignmentType+" @IdsParams -"+
$AssignmentType+"Id "+$Assignment.PrincipalId
                $Principal      = Invoke-Expression $Expression
                if ($Assignment.PrincipalType.Value -eq "GROUP")
 { $Principals[$Assignment.PrincipalId] = $Principal.DisplayName }
                else { $Principals[$Assignment.PrincipalId] = $Principal.UserName }
            }
            $Assignments += [PSCustomObject]@{
                AccountName     = $Account.Name
                PermissionSet   = $PSsets[$PS]
                Principal       = $Principals[$Assignment.PrincipalId]
                Type            = $Assignment.PrincipalType.Value}
        }
    }
}
$Duration = New-Timespan -Start $Start -End (Get-Date) | ForEach-Object
 {[Timespan]::New($_.Days, $_.Hours, $_.Minutes, $_.Seconds)}
Write-Host "`r$($AccountList.Count) accounts done in $Duration. Outputting result to
 $OutputFile"
$Assignments | Sort-Object Account | Export-CSV -Path $OutputFile -Force
```

Restrinja el acceso en función de la dirección IP o la geolocalización mediante AWS WAF

Louis Hourcade, Amazon Web Services

Resumen

AWS WAFes un firewall de aplicaciones web que ayuda a proteger las aplicaciones web y APIs contra los exploits y bots web más comunes que pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos. Las listas de control de acceso a la web (web ACLs) AWS WAF le permiten controlar la forma en que el tráfico llega a sus aplicaciones. En una ACL web, se agregan reglas o grupos de reglas diseñados para permitir el tráfico legítimo, controlar el tráfico de bots y bloquear los patrones de ataque más comunes. Para obtener más información, consulte Cómo AWS WAF funciona.

Puede asociar los siguientes tipos de reglas a su AWS WAF web ACLs:

- Grupos de reglas AWS gestionadas: los equipos de reglas gestionadas y AWS Marketplace los vendedores ofrecen conjuntos de reglas preconfigurados. Algunos grupos de reglas administradas están diseñados para ayudar a proteger determinados tipos de aplicaciones web. Otros ofrecen una amplia protección contra amenazas conocidas o vulnerabilidades comunes.
- Reglas y grupos de reglas personalizados: también puede crear reglas y grupos de reglas que personalicen el acceso a sus aplicaciones web y APIs. Por ejemplo, puede restringir el tráfico en función de una lista específica de direcciones IP o de países.

Al usar este patrón y el repositorio de código asociado, puede usar la AWS WAF web AWS Cloud Development Kit (AWS CDK) ACLs para implementar reglas personalizadas. Estas reglas restringen el acceso a los recursos de la aplicación web según la dirección IP o la ubicación geográfica del usuario final. Si lo desea, también puede adjuntar varios grupos de reglas administrados.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Permisos para implementar AWS WAF recursos
- AWS CDKinstalado y configurado en su cuenta

- Git, instalado

Limitaciones

- Puede usar este patrón solo Regiones de AWS donde AWS WAF esté disponible. Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region.

Tools (Herramientas)

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir y aprovisionar la Nube de AWS infraestructura en el código.
- AWS WAF es un firewall de aplicación web que lo ayuda a supervisar las solicitudes HTTP y HTTPS que se reenvían a los recursos de su aplicación web protegida.

Repositorio de código

El código de este patrón está disponible en el repositorio de restricciones de GitHub IP y geolocalización. AWS WAF El código despliega dos web. AWS WAF ACLs La primera es una ACL web regional destinada a los recursos de Amazon API Gateway. La segunda es la ACL web global para CloudFront los recursos de Amazon. Ambas páginas ACLs contienen las siguientes reglas personalizadas:

- `IPMatch` bloquea las solicitudes de direcciones IP no permitidas.
- `GeoMatch` bloquea las solicitudes de países no permitidos.

Durante la implementación, si lo desea, puede adjuntar todos los siguientes grupos de reglas administradas a su web ACLs:

- Conjunto de reglas básicas (CRS): este grupo contiene reglas que son generalmente aplicables a las aplicaciones web. Brinda protección contra la explotación de una amplia gama de vulnerabilidades, incluyendo algunas de las vulnerabilidades de alto riesgo y más comunes descritas en publicaciones de OWASP tales como OWASP Top 10.
- Protección de administración: este grupo contiene reglas que permiten bloquear el acceso externo a las páginas administrativas expuestas.

- Entradas incorrectas conocidas: este grupo de reglas bloquea los patrones de solicitud que se conocen por no ser válidos y que están asociados a la explotación o el descubrimiento de vulnerabilidades.
- Lista de reputación de IP de Amazon: este grupo de reglas contiene reglas basadas en la inteligencia de amenazas interna de Amazon. Permite bloquear las direcciones IP que suelen estar asociadas a bots u otras amenazas.
- Grupo de reglas administradas en el sistema operativo Linux: este grupo de reglas bloquean los patrones de solicitud asociados a la explotación de vulnerabilidades específicas de Linux, como los ataques de inclusión de archivos locales (LFI) específicos de Linux.
- Grupo de reglas administradas de base de datos de SQL: este grupo de reglas permite bloquear los patrones de solicitud asociados a la explotación de bases de datos de SQL, como los ataques por inyección de código SQL.

Epics

Configure la AWS WAF web ACLs

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Introduzca el siguiente comando para clonar el repositorio Restricción de IP y geolocalización con AWS WAF en la estación de trabajo local: `git clone https://github.com/aws-samples/ip-and-geolocation-restriction-with-waf-cdk.git`	Git
Configure las reglas.	1. En el repositorio clonado, abra el archivo app.py.	AWS general, Python

Tarea	Descripción	Habilidades requeridas

	2. Modifique los valores de las siguientes variables para personalizar las reglas:
	
	`aws_acccount = "AWS_ACCOUNT"`
	`region = "AWS_REGION"`
	`ip_list = ["CIDR_RANGE_1", "CIDR_RANGE_2"]`
	`geo_list = ["COUNTRY_CODE_1", "COUNTRY_CODE_2"]`
	`aws_managed_rules = True`
	
	Donde:
	• `aws_account` es el ID del objetivo Cuenta de AWS.
	• `regiones` el destino Región de AWS de la ACL web para los recursos de API Gateway.
	
	Note
	La ACL web para CloudFront los recursos es global y se implementará en la `us-east-1` región.	

Tarea	Descripción	Habilidades requeridas
	• `ip_list` es la lista de rangos de CIDR a los que se permite el acceso. • `geo_list` es la lista de países a los que está permitido el acceso. Para obtener los valores válidos, consulte la documentación de AWS WAF. • `aws_managed_rules` controla si los grupos de reglas gestionados se agregan a la ACL web. Si este valor es `True`, se agregan. Si este valor es `False`, se excluyen. 3. Guarde y cierre el archivo app.py.	

Arranque e implementación del código

Tarea	Descripción	Habilidades requeridas
Inicie su AWS entorno.	Si aún no lo ha hecho, debe iniciar el AWS entorno antes de poder implementar la AWS CDK aplicación. 1. En la AWS CDK CLI, introduzca el siguiente comando para iniciar la `us-east-1` región:	AWS general

Tarea	Descripción	Habilidades requeridas

	`cdk bootstrap aws://<account-id>/us-east-1`
	2. Si va a implementar la ACL web para API Gateway en una región que no sea `us-east-1` , introduzca el siguiente comando para arrancar la región de destino:
	`cdk bootstrap aws://<account-id>/<region>`	

Implemente la AWS CDK aplicación.	1. Introduzca el siguiente comando para implementar la AWS CDK aplicación: `cdk deploy --all` 2. Espere hasta que se complete el despliegue de la AWS CloudFormation pila.	AWS general

Validación de la implementación

Tarea	Descripción	Habilidades requeridas
Confirme que la web se implementó ACLs correctam ente.	1. Inicie sesión en la AWS WAF consola y Consola de administración de AWS, a continuación, ábrala.	AWS general

Tarea	Descripción	Habilidades requeridas
	2. En el panel de navegación, elija Web ACLs. 3. En la lista de Regiones de AWS, elija Global (CloudFront). 4. Compruebe que se haya implementado la nueva ACL CloudFront web y confirme que tiene la dirección IP y las reglas de geolocalización que ha definido. El nombre predeterminado de esta ACL web es `WebACLCloudfront-<ID>` . 5. En la lista de Regiones de AWS, elija la región en la que desplegó la pila. 6. Compruebe que se haya implementado una nueva ACL web para los recursos de API Gateway. Confirme que tiene la dirección IP y las reglas de geolocalización que ha definido. El nombre predeterminado de esta ACL web es `WebACLApiGW-<ID>` .	

Tarea	Descripción	Habilidades requeridas
(Opcional) Asocie la web ACLs a sus recursos.	Asocie la AWS WAF web ACLs a sus AWS recursos, como un Application Load Balancer, una API Gateway o CloudFront una distribución. Para obtener instrucciones, consulte Asociar o desasociar una ACL web con un recurso de AWShttps://docs.aws.amazon.com/waf/latest/developerguide/web-acl-associating-aws-resource.html. Para ver un ejemplo, consulte class CfnWeb ACLAssociation (construcción) en la AWS CDK documentación.	AWS general

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Elimine las pilas.	1. Desasocie la ACL web de cualquier AWS recurso. Para obtener instrucciones, consulte la documentación de AWS WAF. 2. En la AWS CDK CLI, introduzca el siguiente comando para eliminar la AWS CDK aplicación. `cdk destroy --all`	AWS general

Recursos relacionados

- Referencia de la API (AWS CDK documentación)
- aws-cdk-libMódulo.aws_wafv2 (documentación)AWS CDK
- Trabajar con la web (documentación) ACLs AWS WAF
- Administrar sus propios grupos de reglas (AWS WAF documentación)
- Reglas (AWS WAF documentación)

Escanea los repositorios de Git en busca de información confidencial y problemas de seguridad mediante git-secrets

Saurabh Singh, Amazon Web Services

Resumen

Este patrón describe cómo usar la herramienta git-secrets de código abierto de AWS Labs para escanear los repositorios de código fuente de Git y encontrar código que podría incluir información confidencial, como contraseñas de usuario o claves de AWS acceso, o que tenga otros problemas de seguridad.

`git-secrets` escanea las confirmaciones, los mensajes de confirmación y las fusiones para evitar que se añada información confidencial, como secretos, a sus repositorios de Git. Por ejemplo, si una confirmación, un mensaje de confirmación o cualquier confirmación de un historial de fusiones coincide con uno de sus patrones de expresión regular prohibidos y configurados, la confirmación se rechaza.

Requisitos previos y limitaciones

Requisitos previos

- ¿Un activo Cuenta de AWS
- Un repositorio de Git que requiere un análisis de seguridad
- Un cliente Git (versión 2.37.1 y posteriores) instalado

Arquitectura

Arquitectura de destino

- Git
- `git-secrets`

Tools (Herramientas)

- git-secrets es una herramienta que evita que se guarde información confidencial en los repositorios de Git.
- Git es un sistema de control de versiones distribuido de código abierto.

Prácticas recomendadas

- Escanee siempre un repositorio de Git incluyendo todas las revisiones:

```
git secrets --scan-history
```

Epics

Conectarse a una EC2 instancia

Tarea	Descripción	Habilidades requeridas
Conéctate a una EC2 instancia mediante SSH.	Conéctese a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) mediante SSH y un archivo de key pair. Puede omitir este paso si escanea un repositorio en su equipo local.	AWS general

Instale Git

Tarea	Descripción	Habilidades requeridas
Instale Git	Instale Git mediante el comando:	AWS general

Tarea	Descripción	Habilidades requeridas
	`yum install git -y` Si utiliza su máquina local, puede instalar un cliente Git para una versión específica del sistema operativo. Para obtener más información, consulte el sitio web de Git.	

Clone el repositorio fuente e instale git-secrets

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código fuente de Git.	Para clonar el repositorio de Git que quiera escanear, seleccione el comando Git clone (Clonar Git) en su directorio principal.	AWS general
Clone git-secrets.	Clone el repositorio de Git `git-secrets` . `git clone https://github.com/awslabs/git-secrets.git` Coloque `git-secrets` en algún lugar de su `PATH` para que Git lo recoja cuando usted ejecute `git-secrets` .	AWS general
Instale git-secrets.	Para Unix y sus variantes (Linux/macOS):	AWS general

Tarea	Descripción	Habilidades requeridas

	Usted puede usar el destino `install` del `Makefile` (que se proporciona en el repositorio `git-secrets`) para instalar la herramienta. Usted puede personalizar la ruta de instalación mediante las variables `PREFIX` y `MANPREFIX` .
	`make install`
	Para Windows:
	Ejecute el PowerShell `install.ps1` script proporcionado en el `git-secrets` repositorio. Este script copia los archivos de instalación en un directorio de instalación (`%USERPROFILE%/.git-secrets` de forma predeterminada) y agrega el directorio al usuario actual `PATH`.
	`PS > ./install.ps1`
	Para Homebrew (usuarios de macOS):
	Ejecuta:
	`brew install git-secrets`	

Escanee el repositorio de código de git

Tarea	Descripción	Habilidades requeridas
Vaya al repositorio de origen.	Cambie al directorio del repositorio de Git que desee escanear: `cd my-git-repository`	AWS general
Registre el conjunto de reglas de AWS (enlaces de Git).	Para configurar `git-secrets` el escaneo de su repositorio de Git en cada confirmación, ejecute el comando: `git secrets --register-aws`	AWS general
Escanee el repositorio.	Ejecute el siguiente comando para comenzar a escanear su repositorio: `git secrets --scan`	AWS general

Revise el archivo de salida.	La herramienta genera un archivo de salida si encuentra una vulnerabilidad en su repositorio de Git. Por ejemplo:
	`example.sh:4:AWS_SECRET_ACCESS_KEY = *********`
	
	`[ERROR] Matched one or more prohibited patterns`
		AWS general

Tarea	Descripción	Habilidades requeridas
	Possible mitigations: - Mark false positives as allowed using: git config --add secrets.allowed ... - Mark false positives as allowed by adding regular expressions to .gitallowed at repository's root directory - List your configured patterns: git config --get-all secrets.patterns - List your configured allowed patterns: git config --get-all secrets.allowed - List your configured allowed patterns in .gitallowed at repository's root directory - Use --no-verify if this is a one-time false positive	

Recursos relacionados

- herramienta git-secrets

Proteja las transferencias de archivos mediante Transfer Family, Amazon Cognito y GuardDuty

Manoj Kumar, Amazon Web Services

Resumen

Esta solución le ayuda a transferir archivos de forma segura a través de un servidor SFTP mediante el uso de. AWS Transfer Family Incluye capacidades automatizadas de escaneo de malware a través de Malware Protection for S3, una función de Amazon GuardDuty. Está diseñada para organizaciones que necesitan intercambiar archivos de forma segura con terceros y validar que todos los archivos entrantes se analicen en busca de malware antes de procesarlos.

Las plantillas de infraestructura como código (IaC) que se proporcionan con este patrón le permiten implementar lo siguiente:

- Un servidor SFTP seguro con autenticación de Amazon Cognito mediante AWS Lambda
- Buckets de Amazon Simple Storage Service (Amazon S3) para archivos subidos y entrantes que se hayan analizado en busca de malware.
- Una arquitectura basada en nubes privadas virtuales (VPC) configurada con subredes públicas y privadas en varias zonas de disponibilidad.
- Control de acceso basado en IP para el tráfico de entrada y salida, con listas configurables de permisos y rechazos.
- Escaneo automatizado de malware mediante GuardDuty
- Enrutamiento inteligente de archivos basado en los resultados del escaneo a través de Amazon EventBridge y Lambda
- Notificaciones en tiempo real de incidentes de seguridad a través de Amazon Simple Notification Service (Amazon SNS).
- Cifrado de buckets de Amazon S3 y variables AWS Key Management Service de entorno Lambda mediante ()AWS KMS
- Puntos de conexión de Amazon Virtual Private Cloud (Amazon VPC) para acceso sin exposición a Internet.
- Registro integral a través de la CloudWatch integración de Amazon

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Permisos en AWS Identity and Access Management (IAM) para realizar las acciones descritas en este patrón, incluida la implementación de AWS CloudFormation plantillas que aprovisionen funciones de IAM
- GuardDuty, activado en la cuenta de destino
- Protección contra malware para S3, activada en la cuenta de destino.
- Service Quotas le permite crear lo siguiente en la cuenta de destino:
  - Una VPC
  - Una subred privada
  - Una subred pública
  - Tres direcciones IP elásticas
  - Límites de simultaneidad de Lambda suficientes
- Una dirección de correo electrónico válida para las notificaciones relacionadas con la seguridad
- (Opcional) Una lista de direcciones IP o rangos de CIDR que desee permitir o denegar
- (Opcional) AWS Command Line Interface (AWS CLI), instalado y configurado

Limitaciones

- Protección contra malware para S3 se rige por cuotas, como el tamaño máximo de los archivos. Para obtener más información, consulte Cuotas de protección contra malware para S3 y Compatibilidad de las funciones de Amazon S3 en la GuardDuty documentación.
- Esta solución utiliza únicamente la autenticación de nombre de usuario y contraseña de Amazon Cognito. Esta plantilla no admite métodos de autenticación basados en certificados ni de otro tipo. De forma predeterminada, esta solución no configura la autenticación multifactor (MFA).
- La solución implementa el control de acceso basado en IP únicamente a través de grupos de seguridad.

Arquitectura

El siguiente diagrama de arquitectura muestra los recursos que se implementan en este patrón. Esta solución utiliza Amazon Cognito para la autenticación y autorización de usuarios. Se utiliza un servidor AWS Transfer Family SFTP para la carga de archivos. Los archivos se almacenan en depósitos de Amazon S3 y Amazon los GuardDuty analiza en busca de malware. Amazon SNS envía una notificación por correo electrónico si se detecta malware.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario se conecta al punto final del servidor SFTP en. AWS Transfer Family Esto inicia el proceso de autenticación con el grupo de usuarios de Amazon Cognito.
2. Una función de Lambda inicia el proceso de autenticación y autorización y valida las credenciales del usuario con Amazon Cognito.
3. La función de Lambda devuelve el bucket `UploadBucket` de Amazon S3 como directorio principal. El usuario asume el rol de IAM para el servidor de Transfer Family, y la función de Lambda notifica al usuario que se ha autenticado correctamente.
4. El usuario sube un archivo al servidor SFTP de Transfer Family. El archivo se almacena en el bucket de Amazon S3 `UploadBucket`.
5. GuardDuty escanea el archivo en busca de malware. Los posibles resultados del análisis son `NO_THREATS_FOUND`, `THREATS_FOUND`, `UNSUPPORTED`, `ACCESS_DENIED` y `FAILED`. Para ver ejemplos de resultados, consulte el resultado del escaneo de objetos de S3 en la GuardDuty documentación.
6. Una EventBridge regla detecta el evento resultante del escaneo.
7. EventBridge inicia la función Lambda de enrutamiento de archivos.
8. La función de Lambda procesa el evento y filtra los archivos en función de los resultados del análisis de la siguiente manera:
   - Los archivos cuyo análisis devuelva el resultado `NO_THREATS_FOUND` se envían al bucket `CleanBucket` de Amazon S3.
   - Los archivos cuyo análisis devuelva el resultado `THREATS_FOUND` se envían al bucket `MalwareBucket` de Amazon S3.
   - Los archivos cuyo análisis devuelva el resultado `UNSUPPORTED` se envían al bucket `ErrorBucket` de Amazon S3.

- Los archivos cuyo análisis devuelva el resultado `ACCESS_DENIED` se envían al bucket `ErrorBucket` de Amazon S3.
- Los archivos cuyo análisis devuelva el resultado `FAILED` se envían al bucket `ErrorBucket` de Amazon S3.

Todos los archivos se cifran con un. AWS KMS key

9. Si se envió un archivo al bucket `MalwareBucket` de Amazon S3, la función de Lambda inicia un tema de Amazon SNS. El tema de Amazon SNS envía una notificación por correo electrónico a una dirección de correo electrónico que configure.

Tools (Herramientas)

Servicios de AWS

- Amazon le CloudWatch ayuda a supervisar las métricas de sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.
- Amazon Cognito ofrece autenticación, autorización y administración de usuarios para aplicaciones móviles y web.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, AWS Lambda funciones, puntos finales de invocación HTTP que utilizan destinos de API o buses de eventos en otros. Cuentas de AWS
- Amazon GuardDuty es un servicio de supervisión continua de la seguridad que analiza y procesa los registros para identificar actividades inesperadas y potencialmente no autorizadas en su AWS entorno.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Transfer Familyle ayuda a transferir archivos dentro y fuera de los servicios de AWS almacenamiento a través de los protocolos SFTP, FTPS o FTP.
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Repositorio de código

El código de este patrón está disponible en el GitHub AWS Transfer Family repositorio de soluciones de escaneo de GuardDuty malware.

Prácticas recomendadas

La CloudFormation plantilla proporcionada está diseñada para incorporar muchas de las AWS mejores prácticas, como los permisos con privilegios mínimos para las funciones y políticas de IAM, el cifrado en reposo y en tránsito y la rotación automática de claves. En el caso de los entornos de producción, considere implementar las siguientes recomendaciones adicionales:

- Habilite la autenticación multifactor (MFA) para los usuarios de Amazon Cognito.
- Se implementa AWS Shieldpara la protección distribuida contra la denegación de servicio DDo
- Configure AWS Config para supervisar continuamente el cumplimiento.
- Implemente AWS CloudTrail para un registro integral de API.
- Configura Amazon GuardDuty para la detección de amenazas más allá del escaneo de malware
- Implemente AWS Security Hub CSPM para administrar la seguridad de forma centralizada
- Use AWS Secrets Manager para administrar las credenciales.
- Implemente la supervisión del tráfico de red con Creación de reflejo de tráfico.
- Configure Amazon Macie para detectar información confidencial y protegerla en Amazon S3.
- Implemente evaluaciones de seguridad y pruebas de penetración periódicas.
- Defina plan formal de respuesta a incidentes.
- Implemente parches automatizados para todos los componentes.
- Imparta formación periódica sobre seguridad a los administradores.
- Configure AWS Organizations para administrar la seguridad de varias cuentas.

Epics

Implementación de recursos

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Introduce el siguiente comando para clonar el repositorio de soluciones de escaneo de GuardDuty malware AWS Transfer Family y colocarlo en tu estación de trabajo local: `git clone https://github.com/aws-samples/sample-secure-transfer-family-code.git`	Desarrollador de aplicaciones, ingeniero DevOps
Crea la CloudFormation pila.	1. Siga las instrucciones de la CloudFormation documentación para crear una pila a través de la CloudFormation consola o del AWS CLI. Configure los siguientes parámetros: • `UploadBucketName` : nombre del bucket de subida • `CleanBucketName` : nombre del bucket de archivos limpios • `MalwareBucketName` : nombre del bucket de archivos de malware	Administrador de la nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• `ErrorBucketName` : nombre del bucket de archivos de error • `SecurityTeamEmail` : dirección de correo electrónico para las alertas • `VpcCIDR`: intervalo de CIDR para la VPC • `PublicSubnet1CIDR` : intervalo de CIDR para la subred pública 1 • `PublicSubnet2CIDR` : intervalo de CIDR para la subred pública 2 • `PrivateSubnet1CIDR` : intervalo de CIDR para la subred privada 1 • `PrivateSubnet2CIDR` : intervalo de CIDR para la subred privada 2 • `AllowedIPAddresses` : direcciones IP o intervalos de CIDR permitidos • `EnableEgressRules` : si desea activar las reglas de salida para los grupos de seguridad, ingrese `true`. Si desea desactivar las reglas de salida, ingrese `false`.	

Tarea	Descripción	Habilidades requeridas
	2. Espere a que se complete la implementación de la pila. 3. En los resultados de creación de la pila, anote el punto de conexión del servidor SFTP. Necesitará este valor más tarde.	

Configuración de recursos

Tarea	Descripción	Habilidades requeridas
Active la protección contra malware.	1. Inicie sesión en la GuardDuty consola Consola de administración de AWS y ábrala. 2. En el panel de navegación, elija Protección contra malware para S3. 3. En la sección Buckets protegidos, seleccione Habilitar. 4. En Ingresar detalles del bucket de S3, ingrese el nombre del bucket de Amazon S3. O bien, seleccione Examinar S3 para seleccionar un bucket. Elija el bucket `UploadBucket` de Amazon S3.	Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	5. En Prefijo, seleccione Todos los objetos del bucket de S3. 6. En Etiquetar objetos analizados, seleccione Etiquetar objetos. 7. En la sección Acceso al servicio, elija Crear y usar un nuevo rol de servicio. 8. Seleccione Habilitar.	
Agregue usuarios al grupo de usuarios.	Agregue uno o más usuarios al grupo de usuarios de Amazon Cognito. Para obtener instrucciones, consulte Managing users in your user pool en la documentación de Amazon Cognito.	Administrador de la nube, administrador de AWS

Probar el servidor SFTP

Tarea	Descripción	Habilidades requeridas
Conéctese al punto de conexión del servidor SFTP.	1. Introduce el siguiente comando para obtener el punto final del servidor SFTP, donde `<stack-name>` está el nombre de tu CloudFormation pila: `TRANSFER_ENDPOINT=$(aws cloudformation describe-stacks \`	Desarrollador de aplicaciones, administrador de nube, arquitecto de nube, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas

	`--stack-name <stack-name> \ --query 'Stacks[0].Outputs[?OutputKey==`TransferServerEndpoint`].OutputValue' \ --output text)`
	2. Ingrese el siguiente comando para conectarse al servidor SFTP:
	`sftp user@company.com@$TRANSFER_ENDPOINT`
	3. Confirme que recibe la siguiente petición:
	`sftp>`
	Esto indica que ahora puede ingresar comandos para realizar transferencias de archivos.	

Resolución de problemas

Problema	Solución
Error en la autenticación del usuario	1. Compruebe que el usuario se encuentre en el grupo de usuarios de Amazon Cognito. 2. Valide que el usuario esté confirmado y activado.

Problema	Solución
	3. Asegúrese de que el usuario proporciona la contraseña correcta. 4. Compruebe si hay errores en CloudWatch los registros. Para obtener una lista de AWS CLI los comandos que pueden ayudarle a realizar estos pasos de solución de problemas, consulte Comandos útiles para la solución de problemas en la sección de información adicional.
Error en la autenticación del servidor SFTP	1. Compruebe que el usuario se encuentre en el grupo de usuarios de Amazon Cognito. 2. Valide que el usuario esté confirmado y activado. 3. Asegúrese de que el usuario proporciona la contraseña correcta. 4. Compruebe que la dirección IP esté permitida en el grupo de seguridad del AWS Transfer Family servidor. 5. Compruebe si hay errores en los registros de la función de Lambda de autenticación. 6. Compruebe que la función de IAM AWS Transfer Family tiene los permisos correctos. Para obtener una lista de AWS CLI los comandos que pueden ayudarle a realizar estos pasos de solución de problemas, consulte Comandos útiles para la solución de problemas en la sección de información adicional.

Problema	Solución
Acceso a la subida de archivos denegado	1. Compruebe que los permisos AWS KMS clave estén configurados correctamente. 2. Consulte las políticas de bucket de Amazon S3. 3. Confirme que los permisos del rol de IAM se hayan configurado correctamente. 4. Compruebe que los puntos de conexión de la VPC estén configurados correctamente. 5. Compruebe que la función de IAM AWS Transfer Family tiene los permisos correctos. Para obtener una lista de AWS CLI los comandos que pueden ayudarle a realizar estos pasos de solución de problemas, consulte Comandos útiles para la solución de problemas en la sección de información adicional.

Problema	Solución
No se analiza el malware	1. GuardDuty Actívalo en tu cuenta. 2. Active Protección contra malware para S3 3. Comprueba que la EventBridge regla de Amazon esté activa. 4. Compruebe si hay errores en los registros de la función de Lambda de enrutamiento de archivos. 5. Compruebe que las notificaciones estén configuradas correctamente en Amazon SNS. Para ver una lista de AWS CLI los comandos que pueden ayudarte a realizar estos pasos de solución de problemas, consulta la sección Comandos útiles para la solución de problemas en la sección de información adicional.

Problema	Solución
Errores de la función de Lambda	1. Compruebe la configuración de la VPC. 2. Compruebe que los puntos de conexión de la VPC estén configurados correctamente. 3. Compruebe que la función de IAM AWS Transfer Family tiene los permisos correctos. 4. Compruebe si hay errores en los CloudWatch registros. 5. Compruebe que los permisos AWS KMS clave estén configurados correctamente. Para obtener una lista de AWS CLI los comandos que pueden ayudarle a realizar estos pasos de solución de problemas, consulte Comandos útiles para la solución de problemas en la sección de información adicional.

Recursos relacionados

- Transfer Family web apps (documentación de Transfer Family)

Información adicional

Comandos útiles para solucionar problemas

Comprueba el estado de una CloudFormation pila:

```
aws cloudformation describe-stacks \
  --stack-name <STACK_NAME>
```

Haga una lista con todos los usuarios de un grupo de usuarios de Amazon Cognito:

```
aws cognito-idp list-users \
```

```
  --user-pool-id <USER_POOL_ID>
```

Vea los registros de funciones de Lambda:

```
aws logs describe-log-groups \
  --log-group-name-prefix /aws/lambda/
```

Compruebe el estado de GuardDuty:

```
aws guardduty list-detectors
```

Compruebe las reglas del grupo de seguridad:

```
aws ec2 describe-security-groups \
  --group-ids <SECURITY_GROUP_ID> \
  --output table
```

Compruebe el estado del AWS Transfer Family servidor:

```
aws transfer describe-server \
  --server-id <SERVER_ID>
```

Haga una lista con todos los archivos de un bucket de Amazon S3:

```
aws s3 ls s3://<BUCKET_NAME>/ \
  --recursive
```

Compruebe el estado de una EventBridge regla:

```
aws events describe-rule \
  --name <RULE_NAME>
```

Proteja los datos confidenciales de CloudWatch los registros con Amazon Macie

Anisha Salunkhe, Omar Franco y David Guardiola, Amazon Web Services

Resumen

Este patrón le muestra cómo utilizar Amazon Macie para detectar automáticamente los datos confidenciales en un grupo de CloudWatch registros de Amazon Logs mediante la implementación de un flujo de trabajo integral de supervisión de la seguridad. La solución utiliza Amazon Data Firehose para transmitir las entradas de CloudWatch Logs a Amazon Simple Storage Service (Amazon S3). Macie escanea periódicamente este depósito en busca de información de identificación personal (PII), datos financieros y otro contenido confidencial. La infraestructura se implementa a través de una AWS CloudFormation plantilla que proporciona todas las configuraciones Servicios de AWS y necesidades.

CloudWatch Los registros suelen contener datos de aplicaciones que, de forma inadvertida, pueden incluir información confidencial del usuario. Esto puede generar riesgos de conformidad y seguridad. Los enfoques tradicionales de monitoreo de registros carecen de capacidades automatizadas de detección de datos confidenciales. Esto puede dificultar la identificación y la respuesta a las posibles exposiciones de datos en tiempo real.

Este patrón ayuda a los equipos de seguridad y a los responsables de cumplimiento a mantener la confidencialidad de los datos, ya que permite detectar y alertar de forma automática los datos confidenciales en los sistemas de registro. Esta solución permite una respuesta proactiva a los incidentes mediante las notificaciones del Amazon Simple Notification Service (Amazon SNS) y aísla automáticamente los datos confidenciales en un bucket seguro de Amazon S3. Puede personalizar los patrones de detección e integrar el flujo de trabajo con sus procesos de operaciones de seguridad existentes.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Permisos para crear una CloudFormation pila
- Un grupo de CloudWatch registros que desee supervisar
- Una dirección de correo electrónico activa para recibir notificaciones de Amazon SNS

- Acceso a AWS CloudShell
- (Opcional) Acceso al AWS Command Line Interface (AWS CLI), instalado y configurado

Limitaciones

- Macie está sujeto a cuotas de servicio. Para obtener más información, consulte Cuotas para Macie en la documentación de Macie.

Arquitectura

Arquitectura de destino

El siguiente diagrama muestra el flujo de trabajo para usar Macie para examinar las entradas de registro de CloudWatch Logs en busca de datos confidenciales.

El flujo de trabajo muestra los siguientes pasos:

1. El grupo de CloudWatch registros genera los registros, que están sujetos al filtro de suscripción.
2. El filtro de suscripción reenvía los registros a Amazon Data Firehose.
3. Los registros se cifran con una clave AWS Key Management Service (AWS KMS) cuando pasan por el flujo de entrega de Amazon Data Firehose.
4. La transmisión de entrega entrega los registros al depósito de registros exportados en Amazon S3.
5. Todos los días, a las 4 de la mañana, Amazon EventBridge inicia una AWS Lambda función que inicia un escaneo de Macie en busca de datos confidenciales en el depósito de registros exportados.
6. Si Macie identifica datos confidenciales en el depósito, una función Lambda elimina el registro del depósito de registros exportado y lo cifra con un. AWS KMS key
7. La función Lambda aísla los registros que contienen datos confidenciales en el depósito de aislamiento de datos.
8. La identificación de datos confidenciales inicia un tema de Amazon SNS.
9. Amazon SNS envía una notificación por correo electrónico a una dirección de correo electrónico que usted configure con información sobre los registros que contienen datos confidenciales.

Recursos desplegados

La CloudFormation plantilla despliega los siguientes recursos en tu objetivo Cuenta de AWS y Región de AWS:

- Dos depósitos de Amazon S3:
  - Un depósito de registros exportado para almacenar los datos de CloudWatch Logs
  - Un depósito de aislamiento de datos para almacenar la información confidencial
- Una EventBridge regla de Amazon que responde a los hallazgos de Macie
- AWS Lambda funciones que inician eventos y exportan registros a buckets de Amazon S3
- Un tema y una suscripción de Amazon SNS
- Una transmisión de Amazon Data Firehose
- ¿Una sesión de Macie
- Un identificador de datos personalizado de Macie
- Un filtro de suscripción a CloudWatch Logs
- AWS KMS claves para cifrar los registros almacenados en los depósitos
- Las funciones y políticas AWS Identity and Access Management (de IAM) necesarias para la solución

Tools (Herramientas)

Servicios de AWS

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de su ciclo de vida en todo el mundo Cuentas de AWS . Regiones de AWS
- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas y aplicaciones Servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- Amazon Data Firehose le ayuda a entregar datos de streaming en tiempo real a otros Servicios de AWS puntos de enlace HTTP personalizados y puntos de enlace HTTP propiedad de proveedores de servicios externos compatibles.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, fuentes como AWS Lambda funciones, puntos finales de invocación HTTP que utilizan destinos de API o buses de eventos, entre otras. Cuentas de AWS

- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Macie lo ayuda a descubrir datos confidenciales, proporciona visibilidad de los riesgos de seguridad de los datos y permite la protección automática contra esos riesgos.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub sample-macie-for-securing-cloudwatch-logs.

Prácticas recomendadas

Siga las prácticas CloudFormation recomendadas de la documentación. CloudFormation

Epics

Implementar la solución

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código.	Introduzca el siguiente comando para clonar el repositorio en la estación de trabajo local: `git clone https://github.com/aws-samples/sample-macie-for-`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`securing-cloudwatch-logs`	
(Opcional) Edite la CloudFormation plantilla.	1. Abre el archivo main.yaml. 2. Personalice la plantilla mediante una de las siguientes acciones: • Puede cambiar el nombre de los recursos. • En la `parameter` sección, puede modificar los valores predeterminados. • Puede cambiar el patrón de filtro de suscripciones. Para obtener más información, consulte los filtros de suscripción a nivel de grupo de registros en la documentación de CloudWatch registros. 3. Guarda y cierra el archivo main.yaml.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

Opción 1: realizar la implementación mediante un script con parámetros de línea de comandos.	Introduzca el siguiente comando para implementar la solución mediante parámetros de línea de comandos, donde el valor de `enable-macie` es `true` solo si Amazon Macie aún no está habilitado:
	`./scripts/test-macie-solution.sh --deploy-stack \`
	`  --stack-name <stack name> \`
	`  --email <email address> \`
	`  --enable-macie <true or false> \`
	`  --region <region> \`
	`  --resource-name <prefix for all resources> \`
	`  --bucket-name <bucket name>`
		AWS general

Tarea	Descripción	Habilidades requeridas

Opción 2: Implemente mediante un script con variables de entorno.	1. Introduzca los siguientes comandos para definir las variables de entorno, donde el valor de `ENABLE_MACIE` es `true` solo si Amazon Macie aún no está activado:
	`export STACK_NAME=<stack name>`
	`export SNS_EMAIL=<email address>`
	`export ENABLE_MACIE=<true or false>`
	`export REGION=<region>`
	`export RESOURCE_NAME=<prefix for all resources>`
	`export BUCKET_NAME=<bucket name>`
	2. Introduzca el siguiente comando para validar los parámetros antes de la implementación:
	`./scripts/test-macie-solution.sh \`
	`--validate-params \`
	`--email <email address> \`
	`--region <region>`
	3. Introduzca el siguiente comando para implementar la solución:
		AWS general

Tarea	Descripción	Habilidades requeridas
	`./scripts/test-macie-solution.sh --deploy-stack`	

Tarea	Descripción	Habilidades requeridas
Opción 3: Implemente mediante AWS CLI.	Introduzca el siguiente comando para implementar la solución mediante AWS CLI, donde el valor de `EnableMacie` es `true` solo si Amazon Macie aún no está habilitado: `aws cloudformation create-stack \ --region us-east-1 \ --stack-name macie-for-securing-cloudwatch-logs \ --template-body file://app/main.yml \ --capabilities CAPABILITY_IAM \ --parameters \ ParameterKey=ResourceName,ParameterValue=<prefix for all resources> \ ParameterKey=BucketName,ParameterValue=<bucket name> \ ParameterKey=LogGroupName,ParameterValue=<path for log group> \ ParameterKey=SNSTopicEndpointEmail,ParameterValue=<email address> \ ParameterKey=EnableMacie,ParameterValue=<true or false>`	

Tarea	Descripción	Habilidades requeridas
Opción 4: Implementar mediante. Consola de administración de AWS	1. Abra la consola de AWS CloudFormation. 2. En la barra de navegación de la parte superior de la pantalla, selecciona la en la Región de AWS que quieres crear la pila. 3. En la página Pilas, elija Crear pila en la parte superior derecha y, a continuación, elija Con recursos nuevos (estándar). 4. En la página Crear pila, en Requisito previo: Preparar plantilla, elija Elegir una plantilla existente. 5. En Especificar plantilla, selecciona Cargar un archivo de plantilla y, a continuación, carga la plantilla main.yaml desde tu repositorio clonado. 6. Elija Siguiente. 7. En la página Especificar los detalles de la pila, en el cuadro Nombre de la pila, introduce un nombre de pila. 8. En la sección Parámetros, especifique los valores para los siguientes parámetros de la plantilla.	AWS general

Tarea	Descripción	Habilidades requeridas
	• `ResourceName` : prefijo para todos los recursos • `BucketName` : nombre exclusivo del bucket de Amazon S3 • `LogGroupName` : nombre del grupo de CloudWatch registros para Logs • `SNSTopicEndpointEmail` : Dirección de correo electrónico para las notificaciones • `EnableMacie` : Se establece en `true` si Macie aún no está activado • (Opcional)`Region`: el Región de AWS lugar en el que quieres desplegar la pila. • (Opcional)`TemplatePath` : ruta a la CloudFormation plantilla 9. Elija Siguiente. 10. En Capacidades, seleccione Acepto que esta plantilla puede crear recursos de IAM para especificar que desea utilizar los recursos de IAM en la plantilla. 11. Elija Siguiente.	

Tarea	Descripción	Habilidades requeridas
	12. En la página Revisar y crear, revise los detalles de la pila. 13. Seleccione Enviar para lanzar su stack.	

Tarea	Descripción	Habilidades requeridas
Supervise el estado del despliegue y confirme el despliegue.	1. Introduzca el siguiente comando para supervisar el estado de la implement ación: `./scripts/test-mac ie-solution.sh \ --deployment-statu s \ --stack-name <stack name>` **Note** También puedes supervisar el progreso y el estado de la creación de la pila en la pestaña Eventos de la nueva pila. Para obtener más información, consulta Supervisa r el progreso de la pila. 2. Cuando el estado cambie a CREATE_COMPLETE, revise los resultados de la pila para ver la información sobre los recursos.	AWS general

Tarea	Descripción	Habilidades requeridas
Confirme la suscripción a Amazon SNS.	Siga las instrucciones de Confirme su suscripción a Amazon SNS en la documentación de Amazon SNS para confirmar su suscripción a Amazon SNS.	Desarrollador de aplicaciones

Pruebe la solución

Tarea	Descripción	Habilidades requeridas

Opción 1: Realice la prueba con informes automatizados.	Si utilizó el nombre de pila predeterminado, introduzca el siguiente comando para probar la solución:
	`./scripts/test-macie-solution.sh \ --full-test`
	Si utilizó un nombre de pila personalizado, introduzca el siguiente comando para probar la solución:
	`./scripts/test-macie-solution.sh \ --full-test \ --stack-name <stack name>`
	Si ha utilizado un nombre de pila y parámetros personalizados, introduzca el siguiente
		AWS general

Tarea	Descripción	Habilidades requeridas

	comando para probar la solución:
	
	`./scripts/test-macie-solution.sh --full-test \`
	`  --stack-name <stack name> \`
	`  --region <region> \`
	`  --log-group <log group path>`	

Tarea	Descripción	Habilidades requeridas
Opción 2: realizar la prueba con una validación específica.	1. Introduzca el siguiente comando para generar datos de prueba con información confidencial: `./scripts/test-macie-solution.sh \ --generate-test-data \ --stack-name <stack name>` Este comando hace lo siguiente: • Crea entradas de CloudWatch registro que contienen patrones de datos confidenciales realistas, como números de empleados IDs, patentes IDs, tarjetas de crédito, números de seguro social y direcciones de correo electrónico • Genera entradas de registro confidenciales y no confidenciales para realizar pruebas exhaustivas • Proporciona un registro detallado del proceso de generación de datos de prueba	AWS general

Tarea	Descripción	Habilidades requeridas
	2. Introduzca el siguiente comando para verificar el flujo de la canalización de datos: `./scripts/test-macie-solution.sh \ --verify-pipeline \ --stack-name <stack name>` Este comando hace lo siguiente: • Confirma que las entradas de CloudWatch los registros se transmiten a Amazon Data Firehose • Valida que los datos de registro se entregaron al bucket de Amazon S3 con el cifrado adecuado • Comprueba que el almacenamiento de objetos de Amazon S3 tenga la estructura de prefijos correcta • Verifica el estado de cifrado de los objetos almacenados • Supervisa el tiempo del flujo de datos y proporciona períodos de espera para el procesamiento	

Tarea	Descripción	Habilidades requeridas
	3. Introduzca el siguiente comando para iniciar el trabajo de clasificación de Macie: `./scripts/test-macie-solution.sh \ --trigger-macie-job \ --stack-name <stack name>` Este comando hace lo siguiente: • Activa manualmente el trabajo de clasificación de Macie mediante una función Lambda • Supervisa el estado de ejecución del trabajo y proporciona comentarios • Valida la disponibilidad del servicio de Macie antes de la ejecución • Gestiona los casos en los que Macie no está habilitada en la cuenta • Proporciona resultados detallados de la ejecución del trabajo 4. Introduzca el siguiente comando para validar las alertas y el aislamiento de los datos:	

Tarea	Descripción	Habilidades requeridas
	`./scripts/test-macie-solution.sh \ --verify-alerts \ --stack-name <stack name>` Este comando hace lo siguiente: • Confirma que EventBridge las reglas estén correctamente configuradas y activas • Valida la configuración del tema Amazon SNS y el estado de la suscripción • Comprueba la configuración y los permisos del depósito de aislamiento de datos • Supervisa el movimiento de datos confidenciales al depósito de aislamiento • Verifica la funcionalidad completa del flujo de trabajo de alertas	

Limpieza

Tarea	Descripción	Habilidades requeridas
Opción 1: realizar una limpieza automática.	Si ha utilizado el nombre de pila predeterminado, introduzc	AWS general

Tarea	Descripción	Habilidades requeridas

	a el siguiente comando para eliminar la pila:
	`./scripts/cleanup-macie-solution.sh \ --full-cleanup`
	Si ha utilizado un nombre de pila personalizado, introduzc a el siguiente comando para eliminar la pila:
	`./scripts/cleanup-macie-solution.sh \ --full-cleanup \ --stack-name <stack name>`
	Si ha utilizado un nombre de pila y parámetros personali zados, introduzca el siguiente comando para eliminar la pila:
	`./scripts/cleanup-macie-solution.sh \ --full-cleanup \ --stack-name <stack name> \ --region <region> \ --disable-macie <true or false>`	

Tarea	Descripción	Habilidades requeridas
Opción 2: Realizar la step-by-step limpieza.	1. Introduzca el siguiente comando para detener los procesos activos: `./scripts/cleanup-macie-solution.sh \ --stop-processes \ --stack-name <stack name>` Este comando hace lo siguiente: • Desactiva EventBridge las reglas para impedir la ejecución de nuevos trabajos • Detiene cualquier trabajo de clasificación de Macie que se esté ejecutando actualmente • Cancela las ejecuciones de trabajos pendientes de Macie • Borra todos los mensajes pendientes de Amazon SNS de la cola • Proporciona actualizaciones de estado para cada proceso detenido 2. Introduzca el siguiente comando para vaciar los depósitos de Amazon S3:	AWS general

Tarea	Descripción	Habilidades requeridas

	``
	./scripts/cleanup-
	macie-solution.sh \
	  --empty-buckets \
	  --stack-name <stack
	 name>
	``
	Este comando hace lo siguiente:
	• Elimina todos los objetos del depósito para Logs CloudWatch
	• Elimina todos los objetos del bucket de aislamiento de datos de Amazon S3
	• Elimina cualquier carga multiparte incompleta
	• Gestiona los objetos versionados si el control de versiones de Amazon S3 está activado
	• Proporciona actualiza ciones sobre el recuento de objetos y el progreso de la eliminación
	3. Introduzca el siguiente comando para eliminar la CloudFormation pila:
	``
	./scripts/cleanup-
	macie-solution.sh \
	  --delete-stack \
	  --stack-name <stack
	 name>
	``	

Tarea	Descripción	Habilidades requeridas
	Este comando hace lo siguiente: • Inicia el proceso de eliminación de la CloudFormation pila • Supervisa el progreso de la eliminación con actualizaciones de estado en tiempo real • Gestiona los errores de eliminación con informes de errores detallados • Espera a que se elimine por completo la pila antes de continuar • Proporciona el historial de eventos de la pila para la resolución de problemas 4. Introduzca el siguiente comando para limpiar los recursos de Macie: `./scripts/cleanup-macie-solution.sh \ --cleanup-macie \ --stack-name <stack name>` Esta pila hace lo siguiente: • Elimina los identific adores de datos personali	

Tarea	Descripción	Habilidades requeridas
	zados creados por la solución • Limpia cualquier resto de artefactos y hallazgos relacionados con el trabajo de Macie • Desactiva la sesión de Macie si la ha activado la pila • Maneja los casos en los que los recursos de Macie se comparten con otras aplicaciones • Proporciona el estado de limpieza detallado de cada componente de Macie	

Tarea	Descripción	Habilidades requeridas

Verifique la limpieza.	1. Ingresa el siguiente comando para comprobar que la pila se ha eliminado:
	`aws cloudformation describe-stacks \ --stack-name <stack name> \ --region <region>`
	2. Introduzca el siguiente comando para comprobar que se han eliminado los buckets de Amazon S3:
	`aws s3 ls | grep macie`
	3. Introduzca el siguiente comando para comprobar que se han eliminado los identificadores de datos personalizados de Macie:
	`aws macie2 list-custom-data-identifiers \ --region <region>`
	4. Introduzca el siguiente comando para comprobar si hay recursos restantes:
	`./scripts/cleanup-macie-solution.sh \ --verify-cleanup \ --stack-name <stack name>`
		AWS general

Resolución de problemas

Problema	Solución
CloudFormation el estado de la pila muestra CREATE_FAILED.	La CloudFormation plantilla está configurada para publicar registros en Logs. CloudWatch Puedes ver los registros en el Consola de administración de AWS para no tener que conectarte a tu EC2 instancia de Amazon. Para obtener más información, consulta Ver CloudFormation los registros en la consola (AWS entrada del blog).
CloudFormation `delete-stack` el comando falla.	Algunos recursos deben estar vacíos para poder eliminarlos. Por ejemplo, debe eliminar todos los objetos de un bucket de Amazon S3 o eliminar todas las instancias de un grupo de EC2 seguridad de Amazon antes de poder eliminar el bucket o el grupo de seguridad. Para obtener más información, consulte Fallos al eliminar la pila en la documentación de Amazon S3.
Error al analizar un parámetro.	Cuando utilice la consola AWS CLI o la CloudFormation consola para introducir un valor, añada las comillas.

Recursos relacionados

- Mejores prácticas de arquitectura para el almacenamiento (AWS sitio web)
- Sintaxis de patrones de filtrado para filtros métricos, filtros de suscripción, eventos de registro de filtros y Live Tail (documentación de CloudWatch registros)
- Diseño e implementación del registro y la supervisión con Amazon CloudWatch (guía AWS prescriptiva)
- Solución de problemas CloudFormation (CloudFormation documentación)

Asegurar AWS IAM Roles Anywhere con un certificado privado

Barnali Singh, Amazon Web Services

Resumen

Este patrón demuestra cómo implementar AWS IAM Roles Anywhere with AWS Private Certificate Authority (Autoridad de certificación privada de AWS) para permitir una autenticación segura y basada en certificados para las cargas de trabajo externas que acceden a los recursos. AWS La solución elimina la necesidad de claves de acceso a largo plazo mediante el uso de X.509 certificados para obtener credenciales temporales. AWS Se trata de un patrón de seguridad nativo de la nube que incluye una automatización completa mediante AWS CloudFormation plantillas y scripts de shell, lo que permite a las organizaciones implementar rápidamente la autenticación híbrida segura para aplicaciones locales, CI/CD canalizaciones y sistemas externos.

Requisitos previos y limitaciones

Requisitos previos

Para AWS el despliegue de infraestructuras:

- AWS CLI instalado y configurado con permisos administrativos
- Permisos administrativos para IAM IAM Roles Anywhere y servicios Autoridad de certificación privada de AWS

Para la configuración del sistema cliente:

- AWS CLI instalado en el sistema cliente con los siguientes permisos:
  - `acm-pca:IssueCertificate`
  - `acm-pca:GetCertificate`
- OpenSSL instalado en el sistema cliente
- AWS Signing Helper está instalado en cada sistema cliente
- Comprensión básica de los conceptos de X.509 certificados y PKI

> **Note**
>
> La CloudFormation plantilla gestiona automáticamente la creación AWS de recursos. OpenSSL solo es necesario en los sistemas externos que utilizarán certificados para acceder a los recursos. AWS

Limitaciones

- El período de validez del certificado está limitado a un máximo de 10 años para la CA raíz
- Cambie los certificados de los clientes con regularidad. Le recomendamos que lo haga al menos una vez al año.
- Limitación regional: confíe en las anclas y Autoridad de certificación privada de AWS debe estar en la misma AWS región
- Tamaño máximo del certificado: 16 KB para los certificados de clientes

Versiones de producto

- AWS CLI versión 2.0 o posterior
- OpenSSL 1.1.1 o posterior
- AWS Signing Helper 1.4.0 o posterior
- Autoridad de certificación privada de AWS, versión actual
- IAM Roles Anywhere e, versión actual

Arquitectura

Pila de tecnología de destino

• Autoridad de certificación privada de AWS - CA raíz para la emisión de certificados

• IAM Roles Anywhere - servicio de asunción de Certificate-based roles

• Funciones y políticas de IAM: control de acceso y permisos

• AWS Signing Helper: herramienta de recuperación de Client-side credenciales

• OpenSSL: generación de certificados y claves

• CloudFormation - Automatización de infraestructuras

Arquitectura de destino

Figura 1: Autenticación basada en IAM Roles Anywhere certificados

La arquitectura se compone de:

1. Certificado actual: el sistema externo presenta el X.509 certificado a AWS
2. Autenticar: IAM Roles Anywhere recibe el certificado e inicia la autenticación
3. Verificar: Trust Anchor verifica el certificado con las autoridades certificadoras confiables
4. Validar: Autoridad de certificación privada de AWS valida la autenticidad y el estado del certificado
5. Certificado válido: Autoridad de certificación privada de AWS confirma que el certificado es válido y confiable
6. Asumir el rol: IAM Roles Anywhere permite que el sistema externo asuma el rol de IAM configurado
7. Otorgar acceso: el sistema externo recibe credenciales temporales para acceder a los recursos AWS

Automatización y escala

Este patrón incluye la automatización completa mediante:

• CloudFormation plantilla para el aprovisionamiento AWS de recursos con permisos de IAM configurables

• Secuencia de comandos de shell para la generación de certificados y la configuración del cliente

• Configuración parametrizada para múltiples entornos y políticas de IAM personalizadas

• Generación de certificados por lotes para varios clientes

• Instalación y configuración automatizadas del asistente de credenciales

Flujo de trabajo

1. Establezca los AWS servicios básicos necesarios para utilizar la autenticación basada en certificados. IAM Roles Anywhere

2. Cree y configure certificados y herramientas de autenticación del lado del cliente para un acceso seguro. AWS
3. Verifique la funcionalidad de autenticación basada en certificados y establezca la supervisión de las operaciones en curso.

Tools (Herramientas)

• CloudFormation - Automatiza la creación de PCA, Trust Anchor, IAM Role y Profile

• AWS CLI - Command-line interfaz para la interacción de servicios AWS

• OpenSSL: genera solicitudes de firma de certificados y administra los certificados

• Asistente de AWS firma: intercambia certificados por credenciales temporales AWS

• Bash/shell Secuencias de comandos: automatiza todo el proceso de configuración

Repositorio de código

Funciones de AWS IAM en cualquier lugar con una autoridad de certificación privada

Prácticas recomendadas

- Configure las políticas de IAM según el principio del mínimo privilegio mediante el `--iam-policies parameter`
- Cambie los certificados de los clientes con regularidad. Le recomendamos que lo haga anualmente.
- Utilice una sólida validación de certificados en las políticas de confianza
- Implemente procedimientos de revocación de certificados
- Controle las fechas de vencimiento de los certificados

Epics

Configure la AWS infraestructura

Tarea	Descripción	Habilidades requeridas
Implemente CloudFormation la infraestructura	Cree e implemente la CloudFormation plantilla que aprovisione todos los AWS recursos necesarios Autoridad de certificación privada de AWS, incluidos Trust Anchor, la función de IAM, con las políticas y el IAM Roles Anywhere perfil adecuados. Configure los parámetros para la denominación del proyecto, los períodos de validez de los certificados, la duración de las sesiones y los anexos a las políticas de IAM para establecer la base de la infraestructura principal.	Arquitecto e ingeniero de nube DevOps
Configure la configuración de la autoridad de certificación	Autoridad de certificación privada de AWS Para inicializarla, instale el certificado raíz, configure las plantillas de certificados y establezca la cadena de confianza de los certificados. Configure los períodos de validez de los certificados, los algoritmos clave y las extensiones de certificado necesarios para la IAM Roles Anywhere autenticación a fin de garantizar	Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	una infraestructura de PKI adecuada.	
Validar la configuración de recursos de &AWS;	Realice una validación exhaustiva de todos los AWS recursos desplegados para garantizar una configuración y conectividad adecuadas. Compruebe que Trust Anchor esté correctamente vinculada a Autoridad de certificación privada de AWS, que la función de IAM tenga los permisos adecuados, que el perfil esté correctamente configurado y que todos los recursos estén en buen active/ready estado para los flujos de trabajo de autenticación basados en certificados.	Administrador de sistemas de AWS, ingeniero de pruebas

Genere e implemente certificados de cliente

Tarea	Descripción	Habilidades requeridas
Prepare el entorno del cliente	Configure el entorno del cliente haciendo que los scripts de despliegue sean ejecutables y garantizando los permisos adecuados. Configure el sistema local con las herramientas y dependencias necesarias, compruebe la accesibilidad de los scripts y establezca las bases para	DevOps ingeniero, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	los procesos de generación e implementación de certifica dos.	
Genere una solicitud de firma de certificado	Cree una solicitud de firma de certificado (CSR) para el sistema cliente mediante OpenSSL o herramientas equivalentes. Configure los parámetros del certificado, incluida la información del asunto, los algoritmos clave y las extensiones del certifica do. Asegúrese de que la CSR cumpla con Autoridad de certificación privada de AWS los requisitos y contenga los metadatos adecuados para la IAM Roles Anywhere autentica ción.	Administrador de la nube, ingeniero DevOps
Emita el certificado de cliente a través de Autoridad de certificación privada de AWS	Procese la CSR Autoridad de certificación privada de AWS para emitir un certifica do de cliente válido. Configure los períodos de validez de los certificados y las plantilla s de certificados y garantice el establecimiento adecuado de la cadena de certifica dos. Verifique la emisión del certificado y descargue el certificado firmado para su implementación en el cliente.	Administrador de AWS, arquitecto de la nube

Pruebe y valide la autenticación

Tarea	Descripción	Habilidades requeridas
Obtenga AWS credenciales temporales	Ejecute el script auxiliar de credenciales para recuperar AWS las credenciales temporales mediante el certificado de cliente y la clave privada configurados. Compruebe que el proceso de recuperación de credenciales funciona correctamente, valide el formato de las credencia les y las fechas de caducidad y garantice una integración adecuada con el IAM Roles Anywhere servicio para lograr flujos de trabajo de autentica ción fluidos.	DevOps ingeniero, administr ador de sistemas de AWS
Pruebe el acceso a AWS los recursos	Realice pruebas exhaustiv as del acceso a los AWS recursos utilizando las credenciales temporales obtenidas. Ejecute varios AWS CLI comandos y llamadas a la API para verificar la conectividad con los servicios de destino, como Amazon S3, Amazon EC2 y. AWS Lambda Valide que los permisos se ajusten a las políticas de funciones de IAM configuradas y documente los patrones de acceso correctos.	Ingeniero de pruebas, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Compruebe la asunción de funciones y los permisos	Realice una validación exhaustiva del proceso de asunción de funciones de IAM y de los límites de los permisos. Pruebe tanto las operaciones permitidas como las restringidas para confirmar que el acceso con privilegios mínimos se aplica correctam ente. Verifique los límites de duración de las sesiones y los mecanismos de actualización de credenciales y asegúrese de que la asunción del rol cumpla con las mejores prácticas de seguridad.	Administrador de AWS, ingeniero de pruebas
Implemente la supervisión y el registro	Configure una supervisión y un registro exhaustivos para el sistema de autentica ción basado en certifica dos. Configure el CloudTrai l registro para los registros de auditoría, implemente la supervisión de la caducidad de los certificados, configure alertas para los errores de autenticación y establezc a paneles de control para rastrear los patrones de uso y los eventos de seguridad en toda la infraestructura. IAM Roles Anywhere	DevOps ingeniero, arquitecto de nube

Resolución de problemas

Problema	Solución
Fallos en la validación de los certificados: «La validación del certificado ha fallado» o InvalidCertificate «» errores al intentar la autenticación.	Pasos de resolución: • Compruebe las fechas de validez del certifica do mediante openssl x509 -en certificate.pem -dates -no out • Compruebe que la configuración de Trust Anchor apunta a la CA privada correcta • Asegúrese de que la clave privada correspon de al certificado • Regenere el certificado si lo emitió la CA incorrecta
Errores de permiso de IAM denegado: «Acceso denegado» o «UnauthorizedOpera tion» al acceder a AWS los recursos a pesar de la autenticación correcta	Pasos de resolución: • Revise y amplíe las políticas de funciones de IAM para incluir los permisos necesarios • Compruebe que la política de confianza incluye a rolesanywhere.amazonaws.com como entidad de confianza • Compruebe que la configuración del ARN del perfil coincide con los recursos desplegados • Implemente un mecanismo de actualización de credenciales para procesos de ejecución prolongada

Recursos relacionados

- IAM Roles Anywhere Guía del usuario

- AWS Private Certificate Authority Guía del usuario
- AWS Documentación auxiliar para firmar

Información adicional

Este patrón es ideal para organizaciones con arquitecturas de nube híbrida, CI/CD canalizaciones externas AWS o cualquier sistema externo que requiera un acceso seguro. AWS El enfoque basado en certificados proporciona una mayor seguridad que las claves de acceso a largo plazo y permite la administración centralizada de los certificados mediante. Autoridad de certificación privada de AWS

Permisos de IAM configurables: la solución admite una configuración flexible de políticas de IAM mediante: `--iam-policies parameter`

- Predeterminado: `ReadOnlyAccess` para una implementación inicial segura
- Personalizado: especifique los ARN de política separados por comas para casos de uso específicos. Por ejemplo, `S3ReadOnlyAccessEC2ReadOnlyAccess`, o políticas personalizadas. Admite múltiples políticas para requisitos de permisos complejos.

Ejemplos de uso:

```
# Default read-only access
./deploy.sh

# S3-only access
./deploy.sh --iam-policies "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess"

# Multiple services
./deploy.sh --iam-policies "arn:aws:iam::aws:policy/
AmazonS3ReadOnlyAccess,arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess"
```

Enviar alertas desde AWS Network Firewall a un canal de Slack

Venki Srivatsav y Aromal Raj Jayarajan, Amazon Web Services

Resumen

Este patrón describe cómo implementar un firewall mediante el Firewall de red de Amazon Web Services (AWS) con el modelo de implementación distribuida y cómo propagar las alertas generadas por AWS Network Firewall a un canal de Slack configurable.

Los estándares de conformidad, como el Estándar de seguridad de datos del sector de pagos con tarjeta (PCI DSS), requieren que instale y mantenga un firewall para proteger los datos de los clientes. En la nube de AWS, una nube privada virtual (VPC) se considera igual que una red física en el contexto de estos requisitos de conformidad. Puede usar Network Firewall para monitorear el tráfico de red entre VPCs y proteger las cargas de trabajo que se ejecutan según VPCs un estándar de cumplimiento. Network Firewall bloquea el acceso o genera alertas cuando detecta un acceso no autorizado desde otra VPCs persona de la misma cuenta. Sin embargo, Network Firewall admite un número limitado de destinos para enviar las alertas. Estos destinos incluyen depósitos de Amazon Simple Storage Service (Amazon S3), grupos de registros de CloudWatch Amazon y transmisiones de entrega de Amazon Data Firehose. Cualquier otra acción relacionada con estas notificaciones requiere un análisis fuera de línea mediante Amazon Athena o Amazon Kinesis.

Este patrón proporciona un método para propagar las alertas generadas por Network Firewall a un canal de Slack configurable para tomar medidas adicionales casi en tiempo real. También puede ampliar la funcionalidad a otros mecanismos de alerta PagerDuty, como Jira y el correo electrónico. (Esas personalizaciones quedan fuera del alcance de este patrón).

Requisitos previos y limitaciones

Requisitos previos

- Canal de Slack (consulte Primeros pasos en el centro de ayuda de Slack)
- Privilegios necesarios para enviar un mensaje al canal
- La URL del punto de conexión de Slack con un token de API (seleccione su aplicación y elija un webhook entrante para ver su URL; para obtener más información, consulte Cómo crear un webhook entrante en la documentación de la API de Slack)
- Una instancia de prueba de Amazon Elastic Compute Cloud (Amazon EC2) en las subredes de carga de trabajo

- Reglas de prueba en Network Firewall
- Tráfico real o simulado para activar las reglas de prueba
- Un bucket de S3 para almacenar los archivos fuente que se van a implementar

Limitaciones

- Actualmente, esta solución solo admite un rango de enrutamiento entre dominios sin clase (CIDR) como filtro para el origen y el destino. IPs

Arquitectura

Pila de tecnología de destino

- Una VPC
- Cuatro subredes (dos para el firewall y dos para las cargas de trabajo)
- Puerta de enlace de Internet
- Cuatro tablas de enrutamiento con reglas
- El bucket de S3 se utiliza como destino de alertas y se configura con una política de bucket y una configuración de eventos para ejecutar una función de Lambda
- Función de Lambda con un rol de ejecución, para enviar notificaciones de Slack
- El secreto de AWS Secrets Manager para almacenar la URL de Slack
- Firewall de red con configuración de alertas
- Canal de Slack

Todos los componentes, excepto el canal de Slack, se aprovisionan mediante las CloudFormation plantillas y la función Lambda que se proporcionan con este patrón (consulta la sección Código).

Arquitectura de destino

Este patrón configura un firewall de red descentralizado con integración con Slack. Esta arquitectura consta de una VPC con dos zonas de disponibilidad. La VPC incluye dos subredes protegidas y dos subredes de firewall con puntos de conexión del firewall de red. Todo el tráfico que entra y sale de las subredes protegidas se puede supervisar mediante la creación de políticas y reglas de firewall. El firewall de la red está configurado para colocar todas las alertas en un bucket de S3. Este bucket de S3 está configurado para llamar a una función de Lambda cuando recibe un evento `put`. La

función de Lambda obtiene la URL de Slack configurada de Secrets Manager y envía el mensaje de notificación al espacio de trabajo de Slack.

Para obtener más información sobre esta arquitectura, consulte la entrada del blog de AWS sobre modelos de implementación para AWS Network Firewall.

Tools (Herramientas)

Servicios de AWS

- AWS Network Firewall es un servicio de detección y prevención de intrusiones y firewall de red gestionado y con estado para la VPCs nube de AWS. Puede utilizar el firewall de red para filtrar el tráfico en el perímetro de su VPC y proteger sus cargas de trabajo en AWS.
- AWS Secrets Manager es un servicio de almacenamiento y recuperación de credenciales. Con Secrets Manager puede reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación. Este patrón usa Secrets Manager para almacenar la URL de Slack.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web. Este patrón utiliza Amazon S3 para almacenar las CloudFormation plantillas y el script de Python para la función Lambda. También utiliza un bucket de S3 como el destino de alerta del firewall de red.
- AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Este patrón utiliza AWS CloudFormation para implementar automáticamente una arquitectura distribuida para Firewall Manager.

Código

El código de este patrón está disponible en el GitHub repositorio Network Firewall Slack Integration. En la carpeta `src` del repositorio, encontrará:

- Conjunto de CloudFormation archivos en formato YAML. Estas plantillas se utilizan para aprovisionar los componentes de este patrón.
- Un archivo fuente de Python (`slack-lambda.py`) para crear la función de Lambda.

- Un paquete de implementación de archivos .zip (`slack-lambda.py.zip`) para cargar el código de la función de Lambda.

Para usar el código de muestra, siga las instrucciones de la siguiente sección.

Epics

Configuración del bucket de S3

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/. 2. Elija o cree un bucket de S3 para alojar el código. Un nombre de bucket de S3 es globalmente único y todas las cuentas de AWS comparten el espacio de nombres. El nombre de bucket de S3 no puede incluir barras a la izquierda . Se recomienda utilizar un prefijo para organizar el código de este patrón. Para más información, consulte Crear un bucket en la documentación de Amazon S3.	Desarrollador de aplicaciones, propietario de la aplicación, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cargue las CloudFormation plantillas y el código Lambda.	1. Descargue los siguientes archivos del GitHub repositorio para este patrón: • `base.yml` • `igw-ingress-route.yml` • `slack-lambda.py` • `slackLambda.yml` • `decentralized-deployment.yml` • `protected-subnet-route.yml` • `slack-lambda.py.zip` 2. Cargue los archivos en el bucket de S3 que ha creado.	Desarrollador de aplicaciones, propietario de la aplicación, administrador de la nube

Implemente la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Lanza la CloudFormation plantilla.	Abra la CloudFormation consola de AWS en la misma región de AWS que su bucket de S3 e implemente la plantilla `base.yml`. Esta plantilla crea los recursos de AWS y las funciones de Lambda necesarios para que las alertas se transmitan al canal de Slack.	Desarrollador de aplicaciones, propietario de la aplicación, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	Para obtener más informaci ón sobre la implementación de CloudFormation plantillas, consulte Crear una pila en la CloudFormation consola de AWS en la CloudFormation documentación.	
Complete los parámetros de la plantilla.	Especifique el nombre de la pila y configure los valores de los parámetros. Para obtener una lista de los parámetros, sus descripciones y valores predeterminados, consulte CloudFormation los parámetro s en la sección de información adicional.	Desarrollador de aplicaciones, propietario de la aplicación, administrador de la nube
Cree la pila.	1. Revise los detalles de la pila y actualice los valores en función de los requisitos de su entorno. 2. Elija Crear pila para implementar la plantilla.	Desarrollador de aplicaciones, propietario de la aplicación, administrador de la nube

Verificación de la solución

Tarea	Descripción	Habilidades requeridas
Probar la implementación.	Utilice la CloudFormation consola de AWS o la interfaz de línea de comandos de AWS (AWS CLI) para comprobar que se han creado los recursos que figuran en la	Desarrollador de aplicaciones, propietario de la aplicación, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	sección Pila de tecnologías de destino. Si la CloudFormation plantilla no se implementa correctamente, compruebe los valores que proporcionó para los `pAvailabilityZone2` parámetros `pAvailabilityZone1` y. Deberían ser adecuados para la región de AWS en la que vaya a implementar la solución. Para obtener una lista de las zonas de disponibilidad de cada región, consulta Regiones y zonas en la EC2 documentación de Amazon.	

Tarea	Descripción	Habilidades requeridas

Pruebe la funcionalidad.	1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
	
	2. Cree una EC2 instancia en una de las subredes protegidas. Elija una AMI (HVM) de Amazon Linux 2 para usarla como servidor HTTPS. Para obtener instrucciones, consulta Cómo lanzar una instancia en la EC2 documentación de Amazon.
	
	Note
	Se acerca el fin de la compatibilidad de Amazon Linux 2. Para obtener más información, consulte Amazon Linux 2 FAQs.
	
	3. Utilice los siguientes datos de usuario para instalar un servidor web en la EC2 instancia:
	
	`#!/bin/bash`
	`yum install httpd -y`
	`systemctl start httpd`
	`systemctl stop`
	`firewalld`
	`cd /var/www/html`
		Desarrollador de aplicaciones, propietario de la aplicación, administrador de la nube

Tarea	Descripción	Habilidades requeridas

	`echo "Hello!! this is a NFW alert test page, 200 OK" > index.html`
	
	4. Cree las siguientes reglas de firewall de red:
	
	Regla sin estado:
	
	`Source: 0.0.0.0/0`
	`Destination 10.0.3.65 /32 (private IP of the EC2 instance)`
	`Action: Forward`
	
	Regla con estado:
	
	`Protocol: HTTP`
	`Source ip/port: Any / Any`
	`Destination ip/port: Any /Any`
	
	5. Obtenga la IP pública del servidor web que creó en el paso 3.
	
	6. Acceda a la IP pública en un navegador. Debería ver el siguiente mensaje en el navegador:
	
	`Hello!! this is a NFW alert test page, 200 OK`
	
	También recibirá una notificación en el canal de Slack. Es	

Tarea	Descripción	Habilidades requeridas
	posible que la notificación se retrase en función del tamaño del mensaje. Para realizar pruebas, considere la posibilidad de proporcionar un filtro CIDR que no sea demasiado estrecho (por ejemplo, un valor CIDR con /32 se consideraría demasiado estrecho y /8 sería demasiado ancho). Para obtener más información, consulte la sección Comportamiento del filtro en Información adicional.	

Recursos relacionados

- Deployment models for AWS Network Firewall (entrada del blog de AWS)
- Políticas de AWS Network Firewall (documentación de AWS)
- Integración de Network Firewall con Slack (GitHub repositorio)
- Crear un espacio de trabajo de Slack (centro de ayuda de Slack)

Información adicional

CloudFormation parameters

Parámetro	Description (Descripción)	Valor predeterminado o de muestra
`pVpcName`	Nombre del VPC que se va a crear.	Inspección

pVpcCidr	El rango CIDR que debe crear la VPC.	10.0.0.0/16
pVpcInstanceTenancy	Cómo se distribuyen las EC2 instancias en el hardware físico. Las opciones son default (arrendamiento compartido) o dedicated (arrendamiento único).	predeterminado
pAvailabilityZone1	La primera zona de disponibilidad de la infraestructura.	us-east-2a
pAvailabilityZone2	La segunda zona de disponibilidad de la infraestructura.	us-east-2b
pNetworkFirewallSubnet1Cidr	El rango CIDR de la primera subred del firewall (mínimo /28).	10.0.1.0/24
pNetworkFirewallSubnet2Cidr	El rango CIDR de la segunda subred del firewall (mínimo /28).	10.0.2.0/24
pProtectedSubnet1Cidr	El rango CIDR de la primera subred protegida (carga de trabajo).	10.0.3.0/24
pProtectedSubnet2Cidr	El rango CIDR de la segunda subred protegida (carga de trabajo).	10.0.4.0/24
pS3BucketName	El nombre del bucket de S3 existente en el que cargó el código fuente de Lambda.	us-w2- yourname-lambda-functions
pS3KeyPrefix	El prefijo del bucket de S3 en el que cargó el código fuente de Lambda.	aod-test

pAWSSecretName4Slack	El nombre del secreto que contiene la URL de Slack.	SlackEnpoint-Cfn
pSlackChannelName	El nombre del canal de Slack que creó.	somename-notifications
pSlackUserName	Nombre de usuario de Slack.	Usuario de Slack
pSecretKey	Puede ser cualquier clave. Se recomienda usar la configura ción predeterminada.	webhookUrl
pWebHookUrl	El valor de la URL de Slack.	https://hooks.slack.com/ser vices/¿T?? ¿9T? /A031885 JRM7 /9D4Y?????
pAlertS3Bucket	El nombre del bucket de S3 que se utilizará como el destino de la alerta del firewall de red. Este bucket se creará automáticamente.	us-w2- yourname-security-aod-alerts
pSecretTagName	El nombre de la etiqueta del secreto.	AppName
pSecretTagValue	El valor de la etiqueta para el nombre de etiqueta indicado.	LambdaSlackIntegration
pdestCidr	El filtro para el rango CIDR de destino. Para obtener más información, consulte la siguiente sección, Filtro comportamiento.	10.0.0.0/16

`pdestCondition`	Un indicador que indica si se debe excluir o incluir la coincidencia de destino. Para obtener más informaci ón, consulte la siguiente sección. Los valores válidos son `include` y `exclude`.	incluir
`psrcCidr`	El filtro del rango de CIDR de origen al que se debe alertar. Para obtener más información, consulte la siguiente sección.	118.2.0.0/16
`psrcCondition`	El indicador para excluir o incluir la coincidencia de origen. Para obtener más información, consulte la siguiente sección.	incluir

Comportamiento del filtro

Si no ha configurado ningún filtro en AWS Lambda, todas las alertas generadas se envían a su canal de Slack. El origen y el destino IPs de las alertas generadas coinciden con los rangos de CIDR que configuró al implementar la plantilla. CloudFormation Si hay una coincidencia, se aplica la condición. Si el origen o el destino se encuentran dentro del rango CIDR configurado y al menos uno de ellos está configurado con la condición `include`, se genera una alerta. Las siguientes tablas proporcionan ejemplos de valores, condiciones y resultados del CIDR.

	CIDR configura do	IP de alerta	Configured	Alerta
Origen	10.0.0.0/16	10.0.0.25	incluir	Sí
Destino	100.0.0.0/16	202.0.0.13	incluir	

	CIDR configurado	IP de alerta	Configured	Alerta
Origen	10.0.0.0/16	10,00,25	excluya	No
Destino	100.0.0.0/16	202.0.0.13	incluir	

	CIDR configurado	IP de alerta	Configured	Alerta
Origen	10.0.0.0/16	10,00,25	incluir	Sí
Destino	100.0.0.0/16	100,0.0,13	incluir	

	CIDR configurado	IP de alerta	Configured	Alerta
Origen	10.0.0.0/16	90,0,25	incluir	Sí
Destino	Nulo	202,0,0,13	incluir	

	CIDR configurado	IP de alerta	Configured	Alerta
Origen	10.0.0.0/16	90,0,25	incluir	No
Destino	100.0.0.0/16	202.0.0.13	incluir	

Envío de atributos personalizados a Amazon Cognito e ingesta en los tokens

Carlos Alessandro Ribeiro y Mauricio Mendoza, Amazon Web Services

Resumen

El envío de atributos personalizados a un proceso de autenticación de Amazon Cognito puede proporcionar contexto adicional a una aplicación, permitir controles de acceso más detallados y facilitar la administración de los perfiles de usuario y los requisitos de autenticación. Estas características son útiles en una amplia gama de aplicaciones y escenarios, y pueden ser de ayuda para mejorar la seguridad y la funcionalidad generales de una aplicación.

Este patrón muestra cómo enviar atributos personalizados a un proceso de autenticación de Amazon Cognito cuando una aplicación necesita proporcionar contexto adicional al token de acceso o al token de identidad (ID). Debe usar Node.js como aplicación de backend. La aplicación autentica a un usuario de un grupo de usuarios de Amazon Cognito y transfiere los atributos personalizados necesarios para la generación de los tokens. Puede utilizar los desencadenadores de AWS Lambda de Amazon Cognito para personalizar el proceso de autenticación sin necesidad de una personalización importante del código ni un esfuerzo significativo.

> **Important**
>
> El código y los ejemplos de este patrón no se recomiendan para las cargas de trabajo de producción porque están destinados únicamente a fines de demostración. Para las cargas de trabajo de producción, se requiere una configuración adicional del cliente. Utilice este patrón como referencia únicamente con fines piloto o proof-of-concept con fines específicos.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Permisos para crear y gestionar grupos de usuarios y funciones de Amazon Cognito AWS Lambda
- AWS Command Line Interface (AWS CLI), instalado y configurado
- Un entorno de desarrollo integrado (IDE) que admita Node.js.

- La versión 18 o posterior de Node.js instalada.
- La versión 8 o posterior de npm instalada.
- TypeScript instalado

Limitaciones

- Este patrón no se aplica a la integración de aplicaciones a través del flujo de autenticación de credenciales de cliente.
- El desencadenador previo a la generación del token puede agregar o cambiar solo algunos atributos del token de acceso y del token de identidad. Para obtener más información, consulte Pre token generation Lambda trigger en la documentación de Amazon Cognito.

Arquitectura

Arquitectura de destino

El siguiente diagrama muestra la arquitectura de destino para este patrón. También muestra cómo podría funcionar la aplicación Node.js con un backend para actualizar las bases de datos. Sin embargo, las actualizaciones de la base de datos de backend quedan fuera del alcance de este patrón.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. La aplicación Node.js emite un token de acceso con atributos personalizados para el grupo de usuarios de Amazon Cognito.
2. El grupo de usuarios de Amazon Cognito inicia la función de Lambda previa a la generación del token, que personaliza los tokens de acceso e ID.
3. La aplicación Node.js realiza una llamada a la API a través de Amazon API Gateway.

> **Note**
>
> Los demás componentes arquitectónicos que se muestran en esta arquitectura son solo de ejemplo y están fuera del alcance de este patrón.

Automatización y escala

Puede automatizar el aprovisionamiento de grupos de usuarios AWS Lambda , funciones, instancias de bases de datos y otros recursos de Amazon Cognito AWS CloudFormationmediante Terraform o cualquier herramienta de infraestructura como código (IaC) compatible. AWS Cloud Development Kit (AWS CDK)HashiCorp Si desea escalar sus implementaciones, utilice canalizaciones de integración y entrega continuas (CI/CD), que ayudan a evitar los errores asociados con las implementaciones manuales.

Tools (Herramientas)

Servicios de AWS

- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket APIs a cualquier escala.
- Amazon Cognito ofrece autenticación, autorización y administración de usuarios para aplicaciones móviles y web.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores escalable y rápido que ayuda a ejecutar, detener y administrar contenedores en un clúster.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS SDK para JavaScriptproporciona una JavaScript API para Servicios de AWS. Puede usarla para crear bibliotecas o aplicaciones para Node.js o el navegador.

Otras herramientas

- Node.js es un entorno de JavaScript ejecución basado en eventos que está diseñado para crear aplicaciones de red escalables.
- npm es un registro de software que se ejecuta en un entorno Node.js y se utiliza para compartir o tomar prestados paquetes y administrar la implementación de paquetes privados.

Prácticas recomendadas

Recomendamos que siga las siguientes prácticas recomendadas:

- Secretos e información confidencial: no almacene secretos ni información confidencial en la aplicación. Utilice un sistema externo del que la aplicación pueda extraer los datos, como AWS AppConfig, AWS Secrets Manager o Almacén de parámetros de AWS Systems Manager.
- Implementación estandarizada: utilice CI/CD canalizaciones para implementar sus aplicaciones. Puede utilizar servicios como AWS CodeBuild y AWS CodePipeline.
- Caducidad del token: establezca una fecha de caducidad corta para el token de acceso.
- Uso de una conexión segura: todas las comunicaciones entre la aplicación cliente y el backend deben cifrarse mediante SSL/TLS. Utilice AWS Certificate Manager (ACM) para generar y gestionar SSL/TLS certificados, y utilice Amazon CloudFront o Elastic Load Balancing para gestionar la SSL/TLS rescisión.
- Validación de las entradas del usuario: asegúrese de que todas las entradas del usuario estén validadas para evitar ataques por inyección de código y otras vulnerabilidades de seguridad. Utilice bibliotecas y servicios de validación de entradas, como Amazon API Gateway y AWS WAF para evitar los vectores de ataque más comunes.
- Utilice funciones de IAM: utilice funciones AWS Identity and Access Management (IAM) para controlar el acceso a AWS los recursos y asegurarse de que solo los usuarios autorizados tengan acceso. Siga el principio de privilegio mínimo y asegúrese de que cada usuario tenga los permisos necesarios para realizar su rol.
- Uso de una política de contraseñas: configure una política de contraseñas que cumpla con sus requisitos de seguridad, como la longitud mínima, la complejidad y la caducidad. Utilice Secrets Manager o AWS Systems Manager Parameter Store para almacenar y gestionar las contraseñas de forma segura.
- Activación de la autenticación multifactor (MFA): habilite la MFA para todos los usuarios a fin de proporcionar una capa adicional de seguridad y reducir el riesgo de acceso no autorizado. Utilice AWS IAM Identity Center o Amazon Cognito para habilitar la MFA y otros métodos de autenticación.
- Almacenamiento seguro de la información confidencial: almacene la información confidencial, como contraseñas y tokens de acceso, de forma segura mediante AWS Key Management Service (AWS KMS) u otros servicios de cifrado.
- Uso de métodos de autenticación sólidos: para aumentar la seguridad del proceso de autenticación, utilice métodos de autenticación sólidos, como la autenticación biométrica o la autenticación multifactor.
- Supervisión de la actividad sospechosa: utilice AWS CloudTrail y otras herramientas de supervisión para detectar actividades sospechosas y posibles amenazas a la seguridad. Configura

alertas automatizadas para detectar actividades inusuales y utiliza Amazon GuardDuty o AWS Security Hub CSPMpara detectar posibles amenazas.

- Revisión y actualización periódicas de las políticas de seguridad: revise y actualice periódicamente sus políticas y procedimientos de seguridad para asegurarse de que cumplan con los cambiantes requisitos de seguridad y sus prácticas recomendadas. Úselo AWS Config para realizar un seguimiento y auditar los cambios en sus políticas y procedimientos de seguridad.
- Registro automático: no habilite el registro automático en un grupo de usuarios de Amazon Cognito. Para obtener más información, consulte Reducir los riesgos de fraude en el registro de usuarios y la transferencia de SMS con los grupos de usuarios de Amazon CognitoAWS (entrada del blog).

Para obtener más información sobre las prácticas recomendadas, consulte Security best practices for Amazon Cognito user pools en la documentación de Amazon Cognito.

Epics

Configure los recursos AWS

Tarea	Descripción	Habilidades requeridas
Cree un grupo de usuarios.	1. En una terminal de CLI, ingrese el siguiente comando para crear un grupo de usuarios de Amazon Cognito: `aws cognito-idp create-user-pool \ --pool-name <MyUserPool>` 2. Ingresa el siguiente comando para crear un ID de cliente y un secreto que se usarán con el SDK para JavaScript:	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas

	<pre>aws cognito-idp
	 create-user-pool-c
	lient \
	   --user-pool-id
	 <UserPoolID> \
	   --client-name
	 <MyNewClient> \
	   --no-generate-secr
	et \
	   --explicit-auth-
	flows "USER_PAS
	SWORD_AUTH"
	 "ADMIN_NO_SRP_AUTH"</pre>
	Para obtener más informaci ón e instrucciones sobre cómo configurar un grupo de usuarios en el Consola de administración de AWS, consulte Introducción a los grupos de usuarios y Añadir más funciones y opciones de seguridad a su grupo de usuarios.
	Tip
	Para reducir los costos, utilice el plan Essentials o el plan Lite para probar este patrón. Para obtener más información,	

Tarea	Descripción	Habilidades requeridas
	consulte Precios de Amazon Cognito.	
Agregue un usuario al grupo de usuarios.	Ingrese el siguiente comando para crear un usuario en el grupo de usuarios de Amazon Cognito: `aws cognito-idp sign-up \ --client-id <ClientID> \ --username <jane@example.com> \ --password <PASSWORD> \ --user-attributes Name="email",Value="<jane@example.com>" Name="name",Value="<Jane>"`	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Agregue el cliente de la aplicación al grupo de usuarios.	1. Vaya a la consola de Amazon Cognito. 2. Elija User pools (Grupos de usuarios). 3. Elija el grupo de usuarios que creó anteriormente. 4. En Defina su aplicación, elija el tipo de aplicación que mejor se adapte al escenario de aplicación para el que desea crear los servicios de autenticación y autorización. 5. En Poner un nombre a la aplicación, ingrese un nombre descriptivo o continúe con el nombre predeterminado. 6. En Agregar una URL de retorno, ingrese una ruta de redireccionamiento a su aplicación para que los usuarios completen la autenticación. 7. Elija Cree su aplicación. Puede configurar las opciones avanzadas después de crear el cliente de la aplicación.	Administrador de sistemas de AWS, administrador de AWS DevOps, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Cree un desencadenador de Lambda anterior a la generación de tokens.	1. Abra la página de Functions (Funciones) en la consola de Lambda. 2. Elija Crear función. 3. Seleccione Crear desde cero. 4. En el panel Información básica, ingrese `myPreTokenGenerationLambdaFunction` en Nombre de la función. 5. En Tiempo de ejecución, elija Node.js 22. 6. Deje la arquitectura establecida en x86_64. 7. Elija Crear función. 8. En la pestaña Código, en Código fuente, ingrese la función de Lambda de ejemplo de la sección Recursos adicionales de este patrón. Esta función de Lambda inyecta los atributos personalizados en el token de ID y el token de acceso.	AWS DevOps, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Personalice el flujo de trabajo del grupo de usuarios.	1. Vaya a la consola de Amazon Cognito. 2. Elija User pools (Grupos de usuarios). 3. Elija el grupo de usuarios que creó anteriormente. 4. En el panel de navegación izquierdo, en Autenticación, elija Extensiones. 5. Elija Agregar desencade nador de Lambda. 6. Agregue o edite un desencadenador previo a la generación de tokens. 7. En Tipo de desencade nador, elija Autenticación. 8. En Autenticación, seleccion e Desencadenador anterior a la generación del token. 9. En Asignar una función de Lambda, elija `myPreToke nGenerationLambdaF unction` . 10. Elija Agregar desencade nador de Lambda. 11. Elija una opción de Versión del evento desencadenante de Características básicas con personalización del token de acceso para las identidades de los usuarios o Características básicas	AWS DevOps, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	con personalización del token de acceso para las identidades de usuario y máquina. Esta configuración actualiza los parámetros de solicitud que Amazon Cognito envía a la función para incluir campos para la personalización del token de acceso. Para obtener más información, consulte Customizing user pool workflows with Lambda triggers en la documentación de Amazon Cognito.	

Creación de la aplicación Node.js

Tarea	Descripción	Habilidades requeridas

Cree la aplicación Node.js.	1. En una ventana de la terminal, ingrese los siguientes comandos:
	
	`mkdir my-app`
	`cd my-app`
	`npm init -y`
	`npm install --save-dev typescript`
	`npm i --save-dev @types/node`
	`npm i amazon-cognito-identity-js`
	`npx tsc --init`
	`mkdir src`
		Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	`touch src/index.ts`
	2. Modifique el `package.json` archivo para incluir los scripts de TypeScript compilación:
	`"scripts": { "start": "node src/index.js", "build": "tsc" },`	

Implemente la lógica de autenticación.	1. Abra el archivo `index.ts`. 2. Pegue el ejemplo de Typescript que se proporciona en la sección recursos adicionales de este patrón. 3. Guarde y cierre el archivo `index.ts`. **Note** Puede crear su propio TypeScript archivo o modificar la muestra proporcionada según sea necesario para su caso de uso.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Configure las variables de entorno y el archivo de configuración.	En una terminal, ingrese los siguientes comandos para crear las variables de entorno: `export USERNAME= "<COGNITO_USER_NAME>" export PASSWORD= "<COGNITO_USER_PAS SWORD>" export USER_POOL _ID="<COGNITO_USER _ID>" export CLIENT_ID ="<COGNITO_CLIENT_ ID>"` **Important** No codifique los secretos ni exponga sus credenciales.	Desarrollador de aplicaciones
Ejecute la aplicación .	Ingrese los siguientes comandos para poner en marcha la aplicación y confirmar que funciona: `npm run build npm start`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Confirme que los atributos personalizados estén insertados en los tokens.	Utilice las características de depuración de su IDE para ver los tokens de acceso e ID. Confirme que se hayan agregado los atributos personalizados. Para ver ejemplos de tokens, consulte la sección Información adicional de este patrón.	Desarrollador de aplicaciones

Resolución de problemas

Problema	Solución
El ID de cliente no es válido al intentar autenticar al usuario	Este error suele producirse cuando se utiliza un ID de cliente con un secreto de cliente generado. Debe crear un ID de cliente sin ningún secreto adjunto. Para obtener más información, consulte Application-specific settings with app clients.

Recursos relacionados

- Customizing user pool workflows with Lambda triggers (documentación de Amazon Cognito)
- Pre token generation Lambda trigger (documentación de Amazon Cognito)
- CognitoIdentityProviderClient(AWS SDK para JavaScript documentación)
- cognito-idp (documentación)AWS CLI

Información adicional

Archivo de TypeScript muestra

El siguiente ejemplo de código es un TypeScript archivo que invoca el proceso de autenticación mediante un AWS SDK para enviar atributos personalizados a Amazon Cognito:

```
import * as AmazonCognitoIdentity from "amazon-cognito-identity-js";

const userPoolId: string = process.env.USER_POOL_ID ?? '';
const clientId: string = process.env.CLIENT_ID ?? '';

const poolData = {
  UserPoolId: userPoolId,
  ClientId: clientId
};
const userPool = new AmazonCognitoIdentity.CognitoUserPool(poolData);

export const loginWithCognitoSDK = function (userName: string, password: string) {
  const authenticationDetails = new AmazonCognitoIdentity.AuthenticationDetails({
    Username: userName,
    Password: password,
    ClientMetadata: {
        customGroup: "MyCustomGroup",
        customApplicationData: "Custom data from a custom application"
    }
  });
  const userData = {
    Username: userName,
    Pool: userPool
  };

  const cognitoUser = new AmazonCognitoIdentity.CognitoUser(userData);

  // Authenticate the user using the authenticationDetails object
  cognitoUser.authenticateUser(authenticationDetails, {
    onSuccess: function (result: any) {},
    onFailure: function (err: any) {},
  });
}
loginWithCognitoSDK(process.env.USERNAME ?? '', process.env.PASSWORD ?? '');
```

En el ejemplo se utiliza el `AuthenticationDetails` modelo del SDK JavaScript para proporcionar el nombre de usuario, la contraseña y el. `ClientMetadada` Tras la autenticación en Amazon Cognito, los metadatos del cliente se pueden recuperar de los tokens de acceso e ID.

Función de Lambda de ejemplo

El siguiente código de ejemplo es una función de Lambda vinculada al token de pregeneración de Amazon Cognito. Le permite personalizar el token de acceso y el token de ID que utiliza Amazon Cognito. Los tokens se transfieren a través de las integraciones entre su arquitectura. Este ejemplo incluye un atributo de notificación personalizado denominado `customApplicationData` y un nombre de grupo personalizado denominado `MyCustomGroup`:

```
export const handler = async(event, context, callback) => {
    event.response = {
        claimsOverrideDetails: {
            claimsToAddOrOverride: { customApplicationData:
 event.request.clientMetadata.customApplicationData },
            groupOverrideDetails: { groupsToOverride:
 [event.request.clientMetadata.customGroup] }
        }
    };
    callback(null, event);
};
```

Ejemplo de token de acceso

Puede decodificar el token de acceso para visualizar los atributos personalizados que se agregaron. El siguiente es un ejemplo de token de acceso:

```
{
  "sub": "6daf331f-4451-48b4-abde-774579299204",
  "cognito:groups": [
    "MyCustomGroup"
  ],
  "iss": "https://cognito-idp.<REGION>.amazonaws.com/<USERPOOL_ID>",
  "client_id": "<YOUR_CLIENT_ID>",
  "origin_jti": "acff7e91-09f9-4fde-8eec-38b0f8c47cdc",
  "event_id": "c5113a9c-1f01-435b-9b73-a5cd3e88514e",
  "token_use": "access",
  "scope": "aws.cognito.signin.user.admin",
  "auth_time": 1677979246,
  "exp": 1677982846,
  "iat": 1677979246,
  "jti": "5c9c2708-a871-4428-bd9b-18ad261bea90",
  "username": "<USER_NAME>"
}
```

Ejemplo de token de identificación

Puede decodificar el token de acceso para visualizar los atributos personalizados que se agregaron. El siguiente es un ejemplo de token de acceso:

```
{
  "sub": "6daf331f-4451-48b4-abde-774579299204",
  "cognito:groups": [
    "MyCustomGroup"
  ],
  "iss": "https://cognito-idp.<REGION>.amazonaws.com/<USERPOOL_ID>",
  "cognito:username": "<USER_NAME>",
  "origin_jti": "acff7e91-09f9-4fde-8eec-38b0f8c47cdc",
  "customApplicationData": "Custom data from a custom application",
  "aud": "<YOUR_CLIENT_ID>",
  "event_id": "c5113a9c-1f01-435b-9b73-a5cd3e88514e",
  "token_use": "id",
  "auth_time": 1677979246,
  "exp": 1677982846,
  "iat": 1677979246,
  "jti": "f7ca006b-f25b-44d2-a7a4-6e6423f4201f",
  "email": "<USER_EMAIL>"
}
```

Simplifique la administración de certificados privados mediante AWS Private CA y AWS RAM

Everett Hinckley y Vivek Goyal, Amazon Web Services

Resumen

Puede usar AWS Private Certificate Authority (AWS Private CA) para emitir certificados privados para autenticar los recursos internos y firmar el código informático. Este patrón proporciona una CloudFormation plantilla de AWS para la implementación rápida de una jerarquía de CA de varios niveles y una experiencia de aprovisionamiento coherente. Si lo desea, puede usar AWS Resource Access Manager (AWS RAM) para compartir de forma segura la CA dentro de sus organizaciones o unidades organizativas (OUs) en AWS Organizations y centralizar la CA mientras usa la RAM de AWS para administrar los permisos. No es necesario tener una CA privada en cada cuenta, por lo que este enfoque le permite ahorrar dinero. Además, puede utilizar Amazon Simple Storage Service (Amazon S3) para almacenar la lista de revocación de certificados (CRL) y los registros de acceso.

Esta implementación ofrece los siguientes beneficios y características:

- Centraliza y simplifica la administración de la jerarquía de CA privadas mediante AWS Private CA.
- Exporta certificados y claves a dispositivos gestionados por el cliente en AWS y en las instalaciones.
- Utiliza una CloudFormation plantilla de AWS para una implementación rápida y una experiencia de aprovisionamiento coherente.
- Crea una CA raíz privada junto con una jerarquía de 1, 2, 3 o 4 CA subordinadas.
- Si lo desea, utiliza la RAM de AWS para compartir la CA subordinada de la entidad final con otras cuentas a nivel de organización o unidad organizativa.
- Ahorra dinero al eliminar la necesidad de una CA privada en cada cuenta mediante el uso de AWS RAM.
- Crea un bucket de S3 opcional para la CRL.
- Crea un bucket de S3 opcional para los registros de acceso a la CRL.

Requisitos previos y limitaciones

Requisitos previos

Si desea compartir la CA dentro de una estructura de AWS Organizations, identifique o configure lo siguiente:

- Una cuenta de seguridad para crear la jerarquía de CA y compartirla.
- Una unidad organizativa o cuenta independiente para realizar pruebas.
- El uso compartido está habilitado en la cuenta de administración de AWS Organizations. Para obtener más información, consulte Habilitar el uso compartido con AWS Organizations en la documentación de AWS RAM.

Limitaciones

- CAs son recursos regionales. Todos CAs residen en una sola cuenta de AWS y en una sola región de AWS.
- No se admiten los certificados y las claves generados por los usuarios. Para este caso de uso, le recomendamos que personalice esta solución para utilizar una CA raíz externa.
- No se admite un bucket de CRL público. Le recomendamos que utilice la CRL como privada. Si se requiere acceso a Internet a la CRL, consulte la sección sobre el uso de Amazon CloudFront para habilitar la función S3 Block Public Access (BPA) en la documentación de AWS Private CA. CRLs
- Este patrón implementa un enfoque de una sola región. Si necesita una autoridad de certificación multirregional, puede implementar subordinadas en una segunda región de AWS o de forma en las instalaciones. Esta complejidad queda fuera del ámbito de este patrón, ya que la implementación depende del caso de uso específico, del volumen de carga de trabajo, de las dependencias y de los requisitos.

Arquitectura

Pila de tecnología de destino

- CA
- AWS RAM
- Amazon S3
- AWS Organizations
- AWS CloudFormation

Arquitectura de destino

Este patrón ofrece dos opciones para compartir con AWS Organizations:

Opción 1: Crear el recurso compartido a nivel de la organización. Todas las cuentas de la organización pueden emitir los certificados privados mediante la CA compartida, como se muestra en el siguiente diagrama.

Opción 2 : Crear el recurso compartido a nivel de unidad organizativa (OU). Solo las cuentas de la OU especificada pueden emitir los certificados privados mediante la CA compartida. Por ejemplo, en el siguiente diagrama, si el recurso compartido se crea en el nivel de unidad en un entorno aislado, tanto el desarrollador 1 como el desarrollador 2 pueden emitir certificados privados mediante la CA compartida.

Tools (Herramientas)

Servicios de AWS

- AWS Private CA: AWS Private Certificate Authority (AWS Private CA) es un servicio de CA privada alojado para emitir y revocar certificados digitales privados. Le ayuda a crear jerarquías de entidades de certificación privadas, incluidas las principales y las subordinadas CAs, sin los costes de inversión y mantenimiento que supone operar una entidad de certificación local.
- AWS RAM: AWS Resource Access Manager (AWS RAM) le ayuda a compartir sus recursos de forma segura entre las cuentas de AWS y dentro de su organización o OUs en AWS Organizations. Para reducir la sobrecarga operativa en un entorno de varias cuentas, puede crear un recurso y utilizar la RAM de AWS para compartir ese recurso entre cuentas.
- AWS Organizations: AWS Organizations es un servicio de administración de cuentas que le permite unificar varias cuentas de AWS en una organización que crea y administra de forma centralizada.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web. Este patrón utiliza Amazon S3 para almacenar la lista de revocación de certificados (CRL) y los registros de acceso.
- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Este patrón

utiliza AWS CloudFormation para implementar automáticamente una jerarquía de CA de varios niveles.

Código

El código fuente de este patrón está disponible en el GitHub repositorio jerárquico de CA privadas de AWS. El repositorio incluye:

- La CloudFormation plantilla de AWS`ACMPCA-RootCASubCA.yaml`. Puede utilizar esta plantilla para implementar la jerarquía de CA para esta implementación.
- Pruebe los archivos para casos de uso, como la solicitud, la exportación, la descripción y la eliminación de un certificado.

Para utilizar estos archivos, siga las instrucciones de la sección Epics.

Epics

Diseñe la jerarquía de CA

Tarea	Descripción	Habilidades requeridas
Recopile la información sobre el tema del certificado.	Recopile la información sobre el titular del certificado: nombre de la organización, unidad organizativa, país, estado, en las instalaciones y nombre común.	Arquitecto de la nube, arquitecto de seguridad e ingeniero de PKI
Recopile información opcional sobre AWS Organizations.	Si la CA formará parte de una estructura de AWS Organizations y desea compartir la jerarquía de CA dentro de esa estructura, recopile el número de cuenta de administración, el Identificador de la organización y, opcionalmente, el Identificador	Arquitecto de la nube, arquitecto de seguridad e ingeniero de PKI

Tarea	Descripción	Habilidades requeridas
	de la OU (si desea compartir la jerarquía de CA solo con una OU específica). Además, determine las cuentas de AWS Organizations o OUs, si las hay, con las que quiere compartir la CA.	
Diseñe la jerarquía de CA.	Determine qué cuenta alojará a la cuenta raíz y a la subordinada. CAs Determine cuántos niveles subordina dos requiere la jerarquía entre los certificados raíz y de entidad final. Para obtener más información, consulte Diseñar una jerarquía de CA en la documentación de CA privadas de AWS.	Arquitecto de la nube, arquitecto de seguridad e ingeniero de PKI
Determine las convenciones de nomenclatura y etiquetado para la jerarquía de CA.	Determine los nombres de los recursos de AWS: la CA raíz y cada CA subordina da. Determine qué etiquetas deben asignarse a cada CA.	Arquitecto de la nube, arquitecto de seguridad e ingeniero de PKI

Tarea	Descripción	Habilidades requeridas
Determine los algoritmos de cifrado y firma necesarios.	Determine lo siguiente: • Los requisitos del algoritmo de cifrado de su organizac ión para las claves públicas que la CA utiliza cuando emite un certificado. El valor predeterminado es RSA_2048. • El algoritmo clave que utiliza su CA para la firma de certificados. El valor predeterminado es SHA256 WITHRSA.	Arquitecto de la nube, arquitecto de seguridad e ingeniero de PKI
Determine los requisitos de revocación de certificados para la jerarquía de CA.	Si se requieren capacidades de revocación de certificados, establezca una convención de nomenclatura para el bucket de S3 que contiene la lista de revocación de certificados (CRL).	Arquitecto de la nube, arquitecto de seguridad e ingeniero de PKI
Determine los requisitos de registro para la jerarquía de CA.	Si se requieren capacidad es de registro de acceso, establezca una convenció n de nomenclatura para el bucket de S3 que contiene los registros de acceso.	Arquitecto de la nube, arquitecto de seguridad e ingeniero de PKI

Tarea	Descripción	Habilidades requeridas
Determine los períodos de caducidad de los certificados.	Determine la fecha de caducidad del certificado raíz (el valor predeterminado es de 10 años), los certificados de la entidad final (el valor predeterminado es de 13 meses) y los certificados de CA subordinados (el valor predeterminado es de 3 años). Los certificados de CA subordinados deben caducar antes que los certificados de CA de los niveles superiores de la jerarquía. Para obtener más información, consulte Administrar el ciclo de vida de las CA privadas en la documentación de las CA privadas de AWS.	Arquitecto de la nube, arquitecto de seguridad e ingeniero de PKI

Implemente la jerarquía de CA

Tarea	Descripción	Habilidades requeridas
Completar los requisitos previos.	Complete los pasos de la sección de requisitos previos de este patrón.	Administrador de la nube, ingenieros de seguridad e ingenieros de PKI
Cree funciones de CA para varias personas.	1. Determine los tipos de funciones o usuarios de AWS Identity and Access Management (IAM) en AWS IAM Identity Center (sucesor de AWS Single	Administrador de la nube, ingenieros de seguridad e ingenieros de PKI

Tarea	Descripción	Habilidades requeridas
	Sign-On) necesarios para administrar los distintos niveles de la jerarquía de CA, CAAdmin como Root, Subordinate y. CAAdmin CertificateConsumer 2. Determine la granularidad de las políticas necesarias para separar las funciones. 3. Cree los roles o usuarios de IAM necesarios en el Centro de Identidad de IAM en la cuenta en la que reside la jerarquía de CA.	

Tarea	Descripción	Habilidades requeridas
Implemente la pila. CloudFormation	1. Desde el GitHub repositorio de este patrón, descarga la plantilla AWSPCA-RootCASubCA .yaml. 2. Implemente la plantilla desde la CloudFormation consola de AWS o desde la interfaz de línea de comandos de AWS (AWS CLI). Para obtener más información, consulte Cómo trabajar con pilas en la CloudFormation documentación. 3. Complete los parámetros de la plantilla, incluidos el nombre de la organización, el nombre de la OU, el algoritmo clave, el algoritmo de firma y otras opciones.	Administrador de la nube, ingenieros de seguridad e ingenieros de PKI

Tarea	Descripción	Habilidades requeridas
Diseñe una solución para actualizar los certificados utilizados por los recursos administrados por los usuarios.	Los recursos de los servicios integrados de AWS, como Elastic Load Balancing, actualizan los certificados automáticamente antes de que caduquen. Sin embargo, los recursos administrados por los usuarios, como los servidores web que se ejecutan en instancias de Amazon Elastic Compute Cloud (Amazon EC2), requieren otro mecanismo. 1. Determine qué recursos administrados por el usuario requieren certificados de entidad final de la entidad emisora de certificados privada. 2. Planifique un proceso para recibir notificaciones sobre la caducidad de los recursos y certificados administrados por los usuarios. Para ver ejemplos, consulte los siguientes: • Uso de una regla gestionada por AWS Config • Uso de Amazon CloudWatch y Amazon EventBridge	Administrador de la nube, ingenieros de seguridad e ingenieros de PKI

Tarea	Descripción	Habilidades requeridas
	3. Escriba scripts personalizados para actualizar los certificados en los recursos administrados por los usuarios e intégrelos con los servicios de AWS para automatizar las actualizaciones. Para obtener más información sobre los servicios de AWS integrados, consulte Servicios integrados con AWS Certificate Manager en la documentación de ACM.	

Valide y documente la jerarquía de CA

Tarea	Descripción	Habilidades requeridas
Valide el uso compartido opcional de RAM en AWS.	Si la jerarquía de CA se comparte con otras cuentas de AWS Organizations, inicie sesión en una de esas cuentas desde la consola de administración de AWS, navegue hasta la consola de CA privada de AWS y confirme que la CA recién creada se comparte con esta cuenta. Solo estará visible la CA de nivel inferior de la jerarquía, ya que es la CA que genera los certificados de	Administrador de la nube, ingenieros de seguridad e ingenieros de PKI

Tarea	Descripción	Habilidades requeridas
	la entidad final. Repita este procedimiento para ver una muestra de las cuentas con las que se comparte la CA.	
Valide la jerarquía de las entidades de certificación con pruebas del ciclo de vida de los certificados.	En el GitHub repositorio de este patrón, localice las pruebas del ciclo de vida. Ejecute las pruebas desde la AWS CLI para solicitar un certificado, exportarlo, describirlo y eliminarlo.	Administrador de la nube, ingenieros de seguridad e ingenieros de PKI
Importe la cadena de certifica dos a almacenes fiduciarios.	Para que los navegadores y otras aplicaciones confíen en un certificado, el emisor del certificado debe estar incluido en el almacén de confianza del navegador, que es una lista de certificados de confianza CAs. Añada la cadena de certificados de la nueva jerarquía de CA al almacén de confianza del navegador y de la aplicació n. Confirme que los certifica dos de la entidad final son de confianza.	Administrador de la nube, ingenieros de seguridad e ingenieros de PKI

Tarea	Descripción	Habilidades requeridas
Cree un manual de procedimientos para documentar la jerarquía de las CA.	Cree un manual de procedimientos preliminar para describir la arquitectura de la jerarquía de las entidades de certificación, la estructura contable que puede solicitar los certificados de la entidad final, el proceso de creación y las tareas de administración básicas, como la emisión de certificados de la entidad final (a menos que desee permitir el autoservicio por parte de las cuentas secundarias), el uso y el seguimiento.	Administrador de la nube, ingenieros de seguridad e ingenieros de PKI

Recursos relacionados

- Diseño de una jerarquía de CA (documentación de CA privada de AWS)
- Creación de una CA privada (documentación de CA privada de AWS)
- Cómo usar la RAM de AWS para compartir su cuenta cruzada de CA privada de AWS (entrada del blog de AWS)
- Prácticas recomendadas para las CA privadas de AWS (entrada del blog de AWS)
- Habilite el uso compartido de recursos en AWS Organizations (documentación de AWS RAM)
- Administración del ciclo de vida de las CA privadas (documentación de las CA privadas de AWS)
- acm-certificate-expiration-check para AWS Config (documentación de AWS Config)
- AWS Certificate Manager ahora monitorea la caducidad de los certificados a través de Amazon CloudWatch (anuncio de AWS)
- Servicios integrados con AWS Certificate Manager (documentación de ACM)

Información adicional

Cuando exporte certificados, utilice una contraseña que sea segura desde el punto de vista criptográfico y que se ajuste a la estrategia de prevención de pérdidas de datos de su organización.

Optimice la gestión EC2 del cumplimiento de Amazon con los agentes de Amazon Bedrock y AWS Config

Anand Bukkapatnam Tirumala, Amazon Web Services

Resumen

Este patrón describe cómo integrar Amazon Bedrock con AWS Config las reglas para facilitar la gestión del cumplimiento de las instancias de Amazon Elastic Compute Cloud (Amazon EC2). El enfoque utiliza funcionalidades avanzadas de IA generativa para proporcionar recomendaciones personalizadas que están alineadas con el Marco de AWS Well-Architected, a fin de garantizar una selección óptima del tipo de instancia y la eficiencia del sistema. Entre las características clave de este patrón se incluyen las siguientes:

- Supervisión automatizada del cumplimiento: AWS Config las reglas evalúan continuamente las EC2 instancias según criterios predefinidos para los tipos de instancias deseados.
- Recomendaciones basadas en la IA: los modelos de IA generativa de Amazon Bedrock analizan los patrones de infraestructura. Estos modelos proporcionan sugerencias inteligentes de mejora basadas en las mejores prácticas que se describen en el AWS Well-Architected Framework.
- Remediación: los grupos de acción de Amazon Bedrock permiten tomar medidas de remediación automatizadas para abordar con rapidez los casos que no cumplen la normativa y minimizar las posibles ineficiencias en el rendimiento o los costos.
- Escalabilidad y adaptabilidad: la solución está diseñada para ampliarse con la infraestructura y adaptarse a las necesidades de arquitectura de nube cambiantes.
- Recomendaciones de seguridad mejoradas: el cumplimiento de los principios de AWS Well-Architected contribuye a mejorar la postura de seguridad y el rendimiento del sistema.

Puede utilizar este patrón como modelo para implementar su propia infraestructura generativa basada en la IA en varios entornos con cambios mínimos, utilizando las prácticas necesarias. DevOps

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS

- Un rol AWS Identity and Access Management (IAM) con permisos para crear y gestionar recursos en los buckets, AWS Lambda funciones AWS Config, Amazon Bedrock, IAM, Amazon Logs y Amazon de Amazon Simple Storage Service (Amazon S3). CloudWatch EC2
- Una EC2 instancia para marcar como no conforme. No utilice el tipo `t2.small` para esta instancia.
- Los modelos Amazon Titan Text Embeddings V2 y Anthropic Claude 3 Haiku están habilitados en su. Cuenta de AWS Para habilitar el acceso a los modelos en el Región de AWS lugar en el que vaya a implementar la solución, consulte Añadir o eliminar el acceso a los modelos básicos de Amazon Bedrock en la documentación de Amazon Bedrock.
- Terraform, instalado y configurado.
- AWS Command Line Interface (AWS CLI) v2 se instaló y configuró en el entorno de implementación.
- Revisión completa de la política de IA responsable de Amazon.

Limitaciones

- Algunos Servicios de AWS no están disponibles en todos. Regiones de AWS Para obtener información sobre la disponibilidad en regiones, consulte Servicios de AWS by Region. Para ver los puntos de conexión específicos, consulte Service endpoints and quotas y elija el enlace del servicio.
- Esta solución se probó con los modelos Amazon Titan Text Embeddings V2 y Claude 3 Haiku. Si prefiere utilizar otros modelos, puede personalizar el código de Terraform, que está parametrizado para facilitar los cambios.
- Esta solución no incluye una característica de historial de chat y el chat no se almacena.

Arquitectura

En el siguiente diagrama se muestran los componentes de la arquitectura y el flujo de trabajo de esta aplicación.

El flujo de trabajo consta de los pasos siguientes:

1. El usuario interactúa con el modelo a través de la consola de chat de Amazon Bedrock. El usuario hace preguntas como las siguientes:

- `What can you help me with?`
- `List non-complaint resources`
- `Suggest security best practices`

2. Si el modelo se entrenó anteriormente, responde a las peticiones directamente a partir de sus conocimientos actuales. De lo contrario, la petición se dirige al grupo de acción de Amazon Bedrock.
3. El grupo de acción llega a los puntos de conexión de VPC mediante AWS PrivateLink para lograr una comunicación de servicio segura.
4. La solicitud llega a la función de Lambda a través de los puntos de conexión de VPC para los servicios de Amazon Bedrock.
5. La función de Lambda es el motor de ejecución principal. Según la solicitud, la función llama a la API para realizar acciones en los Servicios de AWS. También gestiona el enrutamiento y la ejecución de las operaciones.
6. La función Lambda llama AWS Config para determinar los recursos no conformes (la EC2 instancia no conforme que creó como requisito previo).
7. AWS Config marca el recurso que no cumple con las normas. Este patrón implementa la AWS Config desired-instance-typeregla para encontrar el tamaño de EC2 instancia ideal.
8. AWS Config pide al usuario que detenga o corrija la instancia y que tome las medidas correspondientes en la instancia. EC2 Amazon Bedrock comprende esta carga útil de devoluciones.
9. El usuario recibe una respuesta en la consola de chat de Amazon Bedrock.

Automatización y escala

Esta solución utiliza Terraform como una herramienta de infraestructura como código (IaC) para permitir una fácil implementación Cuentas de AWS y funcionar como una utilidad independiente en varias cuentas. Este enfoque simplifica la administración y mejora la coherencia de las implementaciones.

Tools (Herramientas)

Servicios de AWS

- AWS Configle permite evaluar, auditar y evaluar las configuraciones de sus AWS recursos para comprobar su conformidad y los ajustes deseados.

- Amazon Bedrock es un servicio de IA totalmente administrado que proporciona acceso a muchos modelos fundacionales de alto rendimiento a través de una API unificada.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus recursos de AWS al controlar quién está autenticado y autorizado a usarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

Otras herramientas

- Git es un sistema de control de versiones distribuido y de código abierto.
- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.

Repositorio de código

El código de este patrón está disponible en el GitHub sample-awsconfig-bedrock-compliance repositorio -manager.

Prácticas recomendadas

- Siga el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Conceder privilegios mínimos y Prácticas recomendadas de seguridad y casos de uso en la documentación de IAM.
- Supervise los registros de ejecución de Lambda con regularidad. Para obtener más información, consulte Supervisión, depuración y solución de problemas de funciones de Lambda y Prácticas recomendadas para trabajar AWS Lambda con funciones en la documentación de Lambda.

Epics

Implementar la solución

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Para clonar el repositorio para este patrón, utilice el comando siguiente: `git clone "git@github.com:aws-samples/sample-awsconfig-bedrock-compliance-manager.git"`	AWS DevOps, jefe de construcción, DevOps ingeniero, administrador de la nube
Edite las variables de entorno.	En el directorio raíz del repositorio clonado en su máquina local, edite el archivo `terraform.tfvars` . Revise los marcadores de posición marcados con `[XXXXX]` y edítelos según su entorno.	Administrador de sistemas de AWS DevOps, DevOps ingeniero, administrador de AWS

Cree la infraestructura.	1. Para crear la infraestructura para esta solución, ejecute los comandos siguientes:
	`terraform init`
	`terraform plan`
	2. Revise el plan de ejecución y, a continuación, ejecute el comando:
	`terraform apply --auto-approve`
		AWS DevOps, DevOps ingeniero, administrador de sistemas de AWS, administrador de la nube

Uso del agente

Tarea	Descripción	Habilidades requeridas

Chatee con el agente.	La implementación de la solución en el paso anterior implementa `security-bot-agent` , que es un agente de Amazon Bedrock con una consola de chat.
	
	Para usar el agente:
	
	1. Inicie sesión Consola de administración de AWS con una identidad de IAM que tenga permisos para usar la consola Amazon Bedrock. A continuación, abra la consola de Amazon Bedrock.
	2. En el panel de navegación, elija Crear, Agentes. Seleccione security-bot-agent.
	3. Comience la conversación con el agente. Por ejemplo:
	
	`List non-complaint EC2 instances`
	
	y:
	
	`Replace these non-complaint EC2 instances with compliant instances`
		AWS DevOps, DevOps ingeniero, administrador de sistemas de AWS, administrador de la nube

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Configure la infraestructura y los recursos.	Cuando haya completado su trabajo con esta solución, puede eliminar la infraestr uctura creada por este patrón; para ello, ejecute el comando siguiente: `terraform destroy -- auto-approve`	AWS DevOps, DevOps ingeniero, administrador de sistemas de AWS, administr ador de la nube

Resolución de problemas

Problema	Solución
Problemas de comportamiento del agente	Para obtener información sobre la resolució n de problemas, consulte Test and troublesh oot agent behavior en la documentación de Amazon Bedrock.
AWS Lambda problemas de red	Para más información, consulte Troubleshoot networking issues in Lambda en la documenta ción de Lambda.
Permisos de IAM	Para más información, consulte Troubleshoot IAM en la documentación de IAM.

Recursos relacionados

- Agentes de Amazon Bedrock
- Use action groups to define actions for your agent to perform (documentación de Amazon Bedrock)
- desired-instance-type regla (AWS Config documentación)

- Cómo AWS Config funciona (AWS Config documentación)

Actualice las credenciales de la CLI de AWS desde el centro de identidad de IAM de AWS mediante PowerShell

Chad Miles y Andy Bowen, Amazon Web Services

Resumen

Si desea utilizar las credenciales de AWS IAM Identity Center (sucesoras de AWS Single Sign-On) con la interfaz de línea de comandos de AWS (AWS CLI), AWS o el kit de desarrollo en la nube de SDKs AWS (AWS CDK), normalmente tiene que copiar y pegar las credenciales de la consola del IAM Identity Center en la interfaz de línea de comandos. Este proceso puede llevar un tiempo considerable, y debe repetirse en cada cuenta a la que se desea acceder.

Una solución habitual consiste en usar el comando `aws sso configure` de la CLI de AWS. Este comando añade un perfil habilitado para el IAM Identity Center a su CLI o SDK de AWS. Sin embargo, la desventaja de esta solución es que debe ejecutar el comando `aws sso login` para cada perfil o cuenta de CLI de AWS que haya configurado de esta manera.

Como solución alternativa, este patrón describe cómo utilizar los perfiles con nombre de la CLI de AWS y las herramientas de AWS PowerShell para almacenar y actualizar las credenciales de varias cuentas desde una única instancia del IAM Identity Center de forma simultánea. El script también almacena los datos de sesión del IAM Identity Center en memoria para poder actualizar las credenciales sin tener que volver a iniciar sesión en el IAM Identity Center.

Requisitos previos y limitaciones

Requisitos previos

- PowerShell instalado y configurado Para obtener más información, consulte Instalación PowerShell (documentación de Microsoft).
- Herramientas de AWS para PowerShell, instaladas y configuradas. Por motivos de rendimiento, le recomendamos encarecidamente que instale la versión modularizada de las herramientas de AWS para PowerShell, llamada. `AWS.Tools` Cada servicio de AWS es compatible con su pequeño módulo propio. En el PowerShell indicador, introduzca los siguientes comandos para instalar los módulos necesarios para este patrón: `AWS.Tools.InstallerSSO`, y. `SSOIDC`

```
Install-Module AWS.Tools.Installer
Install-AWSToolsModule SSO, SSOOIDC
```

Para obtener más información, consulte Instalar AWS.Tools en Windows o Instalar AWS.Tools en Linux o macOS.

- La CLI de AWS o el SDK de AWS deben configurarse previamente con credenciales de trabajo mediante una de las siguientes acciones:
  - Utilice el comando `aws configure` de la CLI de AWS. Para más información, consulte Configuración rápida (documentación de AWS CLI).
  - Configure la CLI de AWS o el CDK de AWS para obtener acceso temporal a través de un rol de IAM. Para obtener más información, consulte Obtener credenciales de rol de IAM para acceder a la CLI (documentación del IAM Identity Center).

Limitaciones

- Este script no se puede usar en un proceso ni en una solución totalmente automatizada. Al implementar este script, deberá autorizar manualmente el acceso desde el IAM Identity Center. El script continuará automáticamente.

Versiones de producto

- Para todos los sistemas operativos, se recomienda utilizar la PowerShell versión 7.0 o posterior.

Arquitectura

Puede usar el script de este patrón para actualizar simultáneamente varias credenciales del centro de identidad de IAM y puede crear un archivo de credenciales para usarlo con AWS CLI SDKs, AWS o AWS CDK.

Tools (Herramientas)

Servicios de AWS

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- AWS IAM Identity Center le ayuda a gestionar de forma centralizada el acceso de inicio de sesión único (SSO) a todas sus cuentas y aplicaciones en la nube de AWS.

- Las herramientas de AWS PowerShell son un conjunto de PowerShell módulos que le ayudan a programar operaciones en sus recursos de AWS desde la línea de PowerShell comandos.

Otras herramientas

- PowerShelles un programa de administración de automatización y configuración de Microsoft que se ejecuta en Windows, Linux y macOS.

Prácticas recomendadas

Conserve una copia de este script para cada instancia de IAM Identity Center. No es posible usar un script en múltiples instancias.

Epics

Ejecutar el script SSO

Tarea	Descripción	Habilidades requeridas
Personalice el script de SSO.	1. Copie el script de SSO en la sección de Información adicional. 2. En la sección `Param`, en su entorno de AWS, defina los valores de las siguientes variables: • `DefaultRoleName` – El rol de IAM o conjunto de permisos que se va a usar de forma predeterminada. • `Region`: la Región de AWS en la que se implementa IAM Identity Center. Para obtener una lista completa de las	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	regiones y sus códigos, consulte Puntos de conexión regionales. • `StartUrl` – La URL utilizada para acceder a la página de inicio de sesión de IAM Identity Center. Use el mismo formato que el valor de ejemplo del script. • `EnvironmentName` – Un nombre abreviado para hacer referencia a esta copia del script. Se usará cuando se ejecuten varias copias del script en la misma sesión. 3. En la línea 10, en `# Add your Account Information` , edite los siguientes valores de las tablas hash para que reflejen su entorno: • `Profile` – El nombre del perfil de CLI de AWS en el que se van a almacenar las credencia les temporales. • `AccountId` – La ID de la cuenta de AWS de la que está recuperando las credenciales.	

Tarea	Descripción	Habilidades requeridas
	• `RoleName` – El nombre del rol o conjunto de permisos de IAM Identity Center que desea usar. Puede dejarlo como `$DefaultRoleName` si desea usar el mismo rol que definió en la sección `Param`. Cada línea de la tabla de hash debe terminar con una coma, excepto la última.	

Ejecutar el script SSO.	Se recomienda ejecutar el script personalizado en el PowerShell shell con el siguiente comando.
	
	`./Set-AwsCliSsoCredentials.ps1`
	
	Si lo desea, también puede ejecutar el script desde otro intérprete de comandos introduciendo el siguiente comando.
	
	`pwsh Set-AwsCliSsoCredentials.ps1`
		Administrador de la nube

Resolución de problemas

Problema	Solución
Error `No Access`	El rol de IAM que está usando no tiene permisos para acceder a la función o al conjunto de permisos que ha definido en el parámetro `RoleName`. Actualice los permisos del rol que está usando o defina un rol o conjunto de permisos diferente en el script.

Recursos relacionados

- ¿Dónde se almacenan las opciones de configuración? (documentación de la CLI de AWS)
- Configurar la CLI de AWS para usar AWS IAM Identity Center (documentación de la CLI de AWS)
- Uso de perfiles con nombre (documentación de la CLI de AWS)

Información adicional

Script de SSO

En el siguiente script, sustituya los marcadores de posición de los corchetes angulares (**<>**) por su propia información y elimine los corchetes angulares.

```
Set-AwsCliSsoCredentials.ps1
Param(
    $DefaultRoleName = '<AWSAdministratorAccess>',
    $Region          = '<us-west-2>',
    $StartUrl        = "<https://d-12345abcde.awsapps.com/start/>",
    $EnvironmentName = "<CompanyName>"
)
Try {$SsoAwsAccounts = (Get-Variable -name "$($EnvironmentName)SsoAwsAccounts" -Scope
 Global -ErrorAction 'SilentlyContinue').Value.Clone()}
Catch {$SsoAwsAccounts = $False}
if (-not $SsoAwsAccounts) { $SsoAwsAccounts = @(
# Add your account information in the list of hash tables below, expand as necessary,
 and do not forget the commas
```

```
    @{Profile = "<Account1>"      ; AccountId = "<012345678901 >"; RoleName =
 $DefaultRoleName },
    @{Profile = "<Account2>"      ; AccountId = "<123456789012>"; RoleName =
 "<AWSReadOnlyAccess>" }
)}
$ErrorActionPreference = "Stop"
if (-not (Test-Path ~\.aws))      { New-Item ~\.aws -type Directory }
if (-not (Test-Path ~\.aws\credentials)) { New-Item ~\.aws\credentials -type File }
$CredentialFile = Resolve-Path ~\.aws\credentials
$PsuedoCreds    = @{AccessKey =
 'AKAEXAMPLE123ACCESS';SecretKey='PsuedoS3cret4cceSSKey123PsuedoS3cretKey'} # Pseudo
 Creds, do not edit.
Try {$SSOTokenExpire = (Get-Variable -Scope Global -Name
 "$($EnvironmentName)SSOTokenExpire" -ErrorAction 'SilentlyContinue').Value} Catch
 {$SSOTokenExpire = $False}
Try {$SSOToken       = (Get-Variable -Scope Global -Name "$($EnvironmentName)SSOToken"
 -ErrorAction 'SilentlyContinue').Value }      Catch {$SSOToken       = $False}
if ( $SSOTokenExpire -lt (Get-Date) ) {
    $SSOToken = $Null
    $Client   = Register-SSOOIDCClient -ClientName cli-sso-client -ClientType public -
Region $Region @PsuedoCreds
    $Device   = $Client | Start-SSOOIDCDeviceAuthorization -StartUrl $StartUrl -Region
 $Region @PsuedoCreds
    Write-Host "A Browser window should open. Please login there and click ALLOW." -
NoNewline
    Start-Process $Device.VerificationUriComplete
    While (-Not $SSOToken){
        Try {$SSOToken = $Client | New-SSOOIDCToken -DeviceCode $Device.DeviceCode -
GrantType "urn:ietf:params:oauth:grant-type:device_code" -Region $Region @PsuedoCreds}
        Catch {If ($_.Exception.Message -notlike "*AuthorizationPendingException*")
{Write-Error $_.Exception} ; Start-Sleep 1}
    }
    $SSOTokenExpire = (Get-Date).AddSeconds($SSOToken.ExpiresIn)
    Set-Variable -Name "$($EnvironmentName)SSOToken" -Value $SSOToken -Scope Global
    Set-Variable -Name "$($EnvironmentName)SSOTokenExpire" -Value $SSOTokenExpire -
Scope Global
}
$CredsTime     = $SSOTokenExpire - (Get-Date)
$CredsTimeText = ('{0:D2}:{1:D2}:{2:D2} left on SSO Token' -f $CredsTime.Hours,
 $CredsTime.Minutes, $CredsTime.Seconds).TrimStart("0 :")
for ($i = 0; $i -lt $SsoAwsAccounts.Count; $i++) {
    if (([DateTimeOffset]::FromUnixTimeSeconds($SsoAwsAccounts[$i].CredsExpiration /
 1000)).DateTime -lt (Get-Date).ToUniversalTime()) {
```

```
        Write-host "`r
    `rRegistering Profile $($SsoAwsAccounts[$i].Profile)" -NoNewline
        $TempCreds = $SSOToken | Get-SSORoleCredential -AccountId
 $SsoAwsAccounts[$i].AccountId -RoleName $SsoAwsAccounts[$i].RoleName -Region $Region
 @PsuedoCreds
        [PSCustomObject]@{AccessKey = $TempCreds.AccessKeyId; SecretKey =
 $TempCreds.SecretAccessKey; SessionToken = $TempCreds.SessionToken
        } | Set-AWSCredential -StoreAs $SsoAwsAccounts[$i].Profile -ProfileLocation
 $CredentialFile
        $SsoAwsAccounts[$i].CredsExpiration = $TempCreds.Expiration
    }
}
Set-Variable -name "$($EnvironmentName)SsoAwsAccounts" -Value $SsoAwsAccounts.Clone() -
Scope Global
Write-Host "`r$($SsoAwsAccounts.Profile) Profiles registered, $CredsTimeText"
```

Uso de Network Firewall para capturar los nombres de dominio de DNS de la indicación del nombre del servidor para el tráfico saliente

Kirankumar Chandrashekar, Amazon Web Services

Resumen

Este patrón le muestra cómo utilizar AWS Network Firewall para recopilar los nombres de dominio DNS que proporciona la indicación del nombre del servidor (SNI) en el encabezado HTTPS del tráfico de red saliente. Network Firewall es un servicio gestionado que facilita la implementación de protecciones de red críticas para Amazon Virtual Private Cloud (Amazon VPC), incluida la capacidad de proteger el tráfico saliente con un firewall que bloquea los paquetes que no cumplen determinados requisitos de seguridad. Proteger el tráfico saliente dirigido a nombres de dominio DNS específicos se denomina filtrado de salida, que consiste en monitorear y, potencialmente, restringir el flujo de información saliente de una red a otra.

Tras capturar los datos del SNI que pasan por Network Firewall, puede utilizar Amazon CloudWatch Logs y AWS Lambda para publicar los datos en un tema del Amazon Simple Notification Service (Amazon SNS) que genere notificaciones por correo electrónico. Las notificaciones por correo electrónico incluyen el nombre del servidor y otra información relevante sobre el SNI. Además, puede utilizar el resultado de este patrón para permitir o restringir el tráfico saliente por nombre de dominio en el SNI mediante reglas de firewall. Para obtener más información, consulte Trabajo con grupos de reglas con estado en AWS Network Firewall en la documentación de Network Firewall.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- La versión 2 de la Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada en Linux, macOS o Windows.
- Network Firewall, instalado y configurado en Amazon VPC y utilizado para inspeccionar el tráfico saliente. Puede configurar Network Firewall para utilizar cualquiera de las siguientes configuraciones de VPC:
  - Arquitectura simple de una sola zona con una puerta de enlace de Internet
  - Arquitectura de un varias zonas con una puerta de enlace de Internet

- Arquitectura con una puerta de enlace de Internet y una puerta de enlace NAT

Arquitectura

El siguiente diagrama muestra cómo usar Network Firewall para recopilar datos de SNI del tráfico de red saliente y, a continuación, publicar esos datos en un tema de SNS mediante Logs CloudWatch y Lambda.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Network Firewall recopila los nombres de dominio de los datos del SNI del encabezado HTTPS del tráfico de red saliente.
2. CloudWatch Logs supervisa los datos del SNI e invoca una función Lambda cada vez que el tráfico de red saliente pasa a través de Network Firewall.
3. La función Lambda lee los datos del SNI capturados por los CloudWatch registros y, a continuación, los publica en un tema de SNS.
4. El tema de SNS le envía una notificación por correo electrónico que incluye los datos del SNI.

Automatización y escala

- Puede usar AWS CloudFormation para crear este patrón mediante el uso de la infraestructura como código.

Pila de tecnología

- Amazon CloudWatch Logs
- Amazon SNS
- Amazon VPC
- AWS Lambda
- AWS Network Firewall

Tools (Herramientas)

Servicios de AWS

- Amazon CloudWatch Logs: puede usar Amazon CloudWatch Logs para monitorear, almacenar y acceder a sus archivos de registro desde instancias de Amazon Elastic Compute Cloud (Amazon EC2) CloudTrail, AWS, Amazon Route 53 y otras fuentes.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio administrado con el que se ofrece la entrega de mensajes de los publicadores a los suscriptores (también conocido como productores y consumidores).
- Amazon VPC: Amazon Virtual Private Cloud (Amazon VPC) le permite aprovisionar una sección aislada de forma lógica de la nube de AWS donde puede lanzar recursos de AWS en una red virtual que haya definido. Dicha red virtual es prácticamente idéntica a las redes tradicionales que se utilizan en sus propios centros de datos, con los beneficios que supone utilizar la infraestructura escalable de AWS.
- AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores.
- AWS Network Firewall: AWS Network Firewall es un servicio gestionado que facilita la implementación de las protecciones de red esenciales para todo su Amazon VPCs.

Epics

Crear un grupo de CloudWatch registros para Network Firewall

Tarea	Descripción	Habilidades requeridas
Cree un grupo de CloudWatch registros.	1. Inicie sesión en la consola de administración de AWS y abra la consola de CloudWatch . 2. En el panel de navegació n, selecione Grupos de registro. 3. Elija Actions (Acciones) y, a continuación, elija Create log group (Crear grupo de registro). 4. Escriba el nombre del grupo de registro y, a continuac	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	ión, seleccione Crear grupo de registro. Para obtener más informaci ón, consulte Trabajar con grupos de registros y flujos de registros en la CloudWatch documentación.	

Crear un tema de SNS y una suscripción

Tarea	Descripción	Habilidades requeridas
Cree un tema de SNS.	Para crear un tema de SNS, siga las instrucciones de la documentación de Amazon SNS.	Administrador de la nube
Suscriba un punto de conexión a un tema SNS.	Para suscribir una dirección de correo electrónico como punto de conexión al tema de SNS que ha creado, siga las instrucciones de la documentación de Amazon SNS. En Protocolo, elija Email/Email-JSON. **Note** También puede elegir un punto de conexión diferente en función de sus requisitos.	Administrador de la nube

Configurar el registro en Network Firewall

Tarea	Descripción	Habilidades requeridas
Habilite el registro de firewall.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon VPC. 2. En el panel de navegación, en NETWORK FIREWALL, elija Firewalls. 3. En la sección Firewalls, elija el firewall en el que desee capturar el nombre del servidor del SNI para el tráfico saliente. 4. Seleccione la pestaña de Detalles del firewall y, a continuación, elija Editar en la sección Registro. 5. En Tipo de registro, seleccione Alerta. En el destino del registro para las alertas, selecciona el grupo de CloudWatch registros. 6. Para el grupo de CloudWatch registros, busque y elija el grupo de registros que creó anteriormente y, a continuación, elija Guardar. Para obtener más información sobre el uso de CloudWatch Logs como destino de	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	registro para Network Firewall, consulte Amazon CloudWatch Logs en la documentación de Network Firewall.	

Configurar una regla con estado en Network Firewall

Tarea	Descripción	Habilidades requeridas
Crear un grupo de reglas con estado.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon VPC. 2. En el panel de navegación, en NETWORK FIREWALL, seleccione Grupos de regla de Network Firewall. 3. Elija Crear grupo de reglas de Network Firewall. 4. En la página de grupo Crear grupo de reglas de Network Firewall, para el Tipo de grupo de reglas, elija Grupo de reglas con estado. Nota: Para obtener más información, consulte Trabajar con grupos de reglas con estado en AWS Network Firewall. 5. En la sección Grupo de reglas con estado, introduzca un nombre y una	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	descripción para el grupo de reglas. 6. En Capacidad, defina la capacidad máxima que desea permitir para el grupo de reglas con estado (hasta un máximo de 30 000). Nota: No puede cambiar esta configura ción después de crear el grupo de reglas. Para obtener información sobre cómo calcular la capacidad , consulte Configuración de la capacidad de los grupos de reglas en AWS Network Firewall. Para obtener información sobre la configuración máxima, consulte Cuotas de AWS Network Firewall. 7. Para Opciones de grupos de reglas con estado, seleccione 5-tuple. 8. En la sección Orden de reglas con estado, seleccione Predeterminado. 9. En la sección Variables de regla, mantenga los valores predeterminados. 10. En la sección Agregar regla, elija TLS para Protocolo. En Origen, elija Cualquiera. En Puerto	

Tarea	Descripción	Habilidades requeridas
	de origen, elija Cualquier puerto. En Destino, seleccione Cualquier a. En Puerto de destino, seleccione Cualquier puerto. En Dirección del tráfico, seleccione Adelante. En Acción, seleccione Alerta. Seleccione Agregar regla. 11 Elija Crear grupo de reglas con estado.	

Tarea	Descripción	Habilidades requeridas
Asocie la regla con estado a Network Firewall.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon VPC. 2. En el panel de navegación, en NETWORK FIREWALL, elija Firewalls. 3. Elija el firewall en el que desee capturar el nombre del servidor del SNI para el tráfico saliente. 4. En la sección Grupos de reglas con estado, elija Acciones y, a continuac ión, elija Agregar grupos de reglas con estado no administrados. 5. En la página Agregar grupos de reglas con estado no administrados, seleccione el grupo de reglas con estado que creó anteriormente y, a continuación, elija Agregar grupo de reglas con estado.	Administrador de la nube

Cree una función de Lambda para leer los registros

Tarea	Descripción	Habilidades requeridas
Crear el código para la función de Lambda.	En un entorno de desarroll o integrado (IDE) que pueda leer el evento CloudWatch	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas

	Logs de Network Firewall para el tráfico saliente, pegue el siguiente código de Python 3 y <SNS-topic-ARN> sustitúyalo por su valor:
	
	`import json`
	`import gzip`
	`import base64`
	`import boto3`
	`sns_client = boto3.client('sns')`
	`def lambda_handler(event, context):`
	`  decoded_event = json.loads(gzip.decompress(base64.b64decode(event['awslogs']['data'])))`
	`  body = '''`
	`  {filtermatch}`
	`  '''.format(`
	`  loggroup=decoded_event['logGroup'],`
	`  logstream=decoded_event['logStream'],`
	`  filtermatch=decoded_event['logEvents'][0]['message'],`
	`  )`
	`  print(body)`
	`  filterMatch = json.loads(body)`
	`  data = []`
	`  if 'http' in filterMatch['event']:`
	`  data.append(filterMatch['ev`	

Tarea	Descripción	Habilidades requeridas
	ent']['http']['hos tname']) elif 'tls' in filterMatch['event']: data.appe nd(filterMatch['ev ent']['tls']['sni']) result = 'Domain accessed ' + 1*' ' + (data[0]) + 1*' ' 'via AWS Network Firewall ' + 1*' ' + (filterMa tch['firewall_name']) print(result) message = {'ServerN ame': result} send_to_sns = sns_client.publish(TargetArn=<SNS-topic-ARN>, #Replace with the SNS topic ARN Message=j son.dumps({'default': json.dumps(message), 'sms': json.dump s(message), 'email': json.dump s(message)}), Subject='Server Name passed through the Network Firewall', MessageSt ructure='json') Este ejemplo de código analiza el contenido de CloudWatch los registros y	

Tarea	Descripción	Habilidades requeridas
	captura el nombre del servidor proporcionado por el SNI en el encabezado HTTPS.	
Crear la función de Lambda.	Para crear la función de Lambda, siga las instrucciones de la documentación de Lambda y elija Python 3.9 para el Tiempo de ejecución.	Administrador de la nube
Añada el código a la función de Lambda.	Para añadir el código Python a la función de Lambda que creó anteriormente, siga las instrucciones de la documentación de Lambda.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Agregue CloudWatch registros como activador a la función Lambda.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Lambda. 2. En el panel de navegación, seleccione Funciones y, a continuación, elija la función que creó anteriormente. 3. En la sección Informaci ón general de la función, seleccione Agregar desencadenador. 4. En la página Agregar activador, en la sección Configuración del disparado r, elija CloudWatch Registros y, a continuación, elija Agregar. 5. En Grupo de registros, elija el grupo de CloudWatch registros que creó anteriorm ente. 6. En Nombre del filtro, especifique un nombre para el filtro. 7. Seleccione Agregar. 8. En la pestaña Configura ción de la página de la función, en la sección Activadores, seleccione el activador que acabas de añadir y, a continuación, seleccione Activar.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte Uso de Lambda con CloudWatch registros en la documentación de Lambda.	

Tarea	Descripción	Habilidades requeridas
Agregue permisos de publicación de SNS.	Agregue el permiso sns:Publish a la función de ejecución de Lambda para que Lambda pueda realizar llamadas a la API para publicar mensajes en SNS. 1. Busque el rol de ejecución de la función de Lambda que creó anteriormente. 2. Agregue la siguiente política a su AWS Identity and Access Management (rol de IAM): `{ "Version": "2012-10-17", "Statement": [ { "Sid": "AllowSNSPublish", "Effect": "Allow", "Action": [ "sns:GetTopicAttributes", "sns:Subscribe", "sns:Unsubscribe", "sns:Publish" ], "Resource": "*" }`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	<pre>] }</pre>	

Pruebe la funcionalidad de su notificación de SNS

Tarea	Descripción	Habilidades requeridas

Envíe tráfico a través de Network Firewall.	1. Envíe o espere a que el tráfico HTTPS pase a través de Network Firewall.
	2. Compruebe el correo electrónico de notificación de SNS que recibe de AWS cuando el tráfico pasa a través de Network Firewall. El correo electrónico incluye los detalles del SNI del tráfico saliente. Por ejemplo, el correo electrónico generado a partir del código Lambda anterior tendrá el siguiente contenido si el nombre de dominio al que se ha accedido es EMAIL-JSON https://aws.amazon.comy el protocolo de suscripción es EMAIL-JSON:
	<pre>{
	    "Type": "Notification",
	    "MessageId": "<messageID>",</pre>
		Ingeniero de pruebas

Tarea	Descripción	Habilidades requeridas
	<pre>"TopicArn": "arn:aws:sns:us-west-2:123456789:testSNSTopic", "Subject": "Server Name passed through the Network Firewall", "Message": "{\"ServerName\": \"Domain 'aws.amazon.com' accessed via AWS Network Firewall 'AWS-Network-Firewall-Multi-AZ-firewall\"}", "Timestamp": "2022-03-22T04:10:04.217Z", "SignatureVersion": "1", "Signature": "<Signature>", "SigningCertURL": "<SigningCertUrl>", "UnsubscribeURL": "<UnsubscribeURL>" }</pre> A continuación, consulte el registro de alertas de Network Firewall en Amazon CloudWatch siguiendo las instrucciones de la CloudWatch documentación de Amazon. El registro de alerta muestra el siguiente resultado: <pre>{</pre>	

Tarea	Descripción	Habilidades requeridas
	"firewall_name": "AWS-Network-Firewall-Multi-AZ-firewall", "availability_zone": "us-east-2b", "event_timestamp": "<event timestamp>", "event": { "timestamp": "2021-03-22T04:10:04.214222+0000", "flow_id": <flow ID>, "event_type": "alert", "src_ip": "10.1.3.76", "src_port": 22761, "dest_ip": "99.86.59.73", "dest_port": 443, "proto": "TCP", "alert": { "action": "allowed", "signature_id": 2, "rev": 0, "signature": "", "category": "", "severity": 3 }, "tls": { "subject": "CN=aws.amazon.com",	

Tarea	Descripción	Habilidades requeridas
	"issuerdn ": "C=US, O=Amazon, OU=Server CA 1B, CN=Amazon", "serial": "<serial number>", "fingerpr int": "<fingerprint ID>", "sni": "aws.amazon.com", "version": "TLS 1.2", "notbefor e": "2020-09-30T00:00: 00", "notafter ": "2021-09-23T12:00: 00", "ja3": {}, "ja3s": {} }, "app_proto": "tls" } }	

Usa Terraform para habilitar Amazon automáticamente GuardDuty para una organización

Aarthi Kannan, Amazon Web Services

Resumen

Amazon supervisa GuardDuty continuamente sus cuentas de Amazon Web Services (AWS) y utiliza información sobre amenazas para identificar actividades inesperadas y potencialmente maliciosas en su entorno de AWS. La activación manual GuardDuty de varias cuentas u organizaciones, en varias regiones de AWS o a través de la consola de administración de AWS puede resultar engorrosa. Puede automatizar el proceso mediante una herramienta de infraestructura como código (IaC) como Terraform, capaz de aprovisionar y administrar servicios y recursos de múltiples cuentas y regiones en la nube.

AWS recomienda usar AWS Organizations para configurar y administrar varias cuentas en GuardDuty. Este patrón sigue dicha recomendación. Una de las ventajas de este enfoque es que, cuando se creen o agreguen nuevas cuentas a la organización, se GuardDuty habilitarán automáticamente en estas cuentas para todas las regiones compatibles, sin necesidad de intervención manual.

Este patrón muestra cómo usar HashiCorp Terraform para habilitar Amazon GuardDuty para tres o más cuentas de Amazon Web Services (AWS) en una organización. El código de ejemplo proporcionado en este patrón hace lo siguiente:

- Se habilita GuardDuty para todas las cuentas de AWS que son miembros actuales de la organización objetivo en AWS Organizations
- Activa la función de activación automática en GuardDuty, que se habilita automáticamente GuardDuty para cualquier cuenta que se añada a la organización de destino en el futuro
- Te permite seleccionar las regiones en las que quieres activarlas GuardDuty
- Utiliza la cuenta de seguridad de la organización como GuardDuty administrador delegado
- Crea un depósito de Amazon Simple Storage Service (Amazon S3) en la cuenta de registro y se GuardDuty configura para publicar los resultados agregados de todas las cuentas de este depósito
- Asigna una política de ciclo de vida que, de forma predeterminada, transfiere los resultados del bucket de S3 al almacenamiento de Amazon S3 Glacier Flexible Retrieval después de 365 días

Puede ejecutar manualmente este código de ejemplo o bien integrarlo en su proceso de integración y entrega continuas (CI/CD).

Público objetivo

Este patrón se recomienda para los usuarios que tengan experiencia con Terraform GuardDuty, Python y AWS Organizations.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una organización configurada en AWS Organizations que contenga, al menos, las tres cuentas siguientes:
  - Una cuenta de administración: esta es la cuenta desde la que se implementa el código de Terraform, ya sea de forma independiente o como parte del proceso. CI/CD El estado de Terraform también se almacena en esta cuenta.
  - Una cuenta de seguridad: esta cuenta se usa como administrador GuardDuty delegado. Para obtener más información, consulte Consideraciones importantes para los administradores GuardDuty delegados (GuardDuty documentación).
  - Una cuenta de registro: esta cuenta contiene el depósito de S3, donde se GuardDuty publican los resultados agregados de todas las cuentas de los miembros.

  Para obtener más información sobre cómo configurar la organización con los ajustes requeridos, consulte Crear una estructura de cuentas (AWS Well-Architected Labs).
- Un bucket de Amazon S3 y una tabla de Amazon DynamoDB que sirvan como backend remoto para almacenar el estado de Terraform en la cuenta de administración. Para obtener más información sobre el uso de backends remotos para el estado de Terraform, consulte los backends de S3 (documentación de Terraform). Para ver un ejemplo de código que configura la administración remota del estado con un backend de S3, consulte remote-state-s3-backend (Terraform Registry). Tenga en cuenta los siguientes requisitos:
  - El bucket de S3 y la tabla de DynamoDB deben estar en la misma región.
  - Al crear la tabla de DynamoDB, la clave de partición debe ser `LockID` (distingue entre mayúsculas y minúsculas), y el tipo de clave de partición debe ser String. Todos los demás valores de la tabla deben estar en sus valores predeterminados. Para obtener más información,

consulte Acerca de las claves principales y Creación de una tabla (documentación de DynamoDB).

- Un depósito de S3 que se utilizará para almacenar los registros de acceso del depósito de S3 en el que GuardDuty se publicarán los resultados. Para obtener más información, consulte Habilitar el registro de acceso al servidor de Amazon S3 (documentación de Amazon S3). Si va a realizar la implementación en una zona de aterrizaje de AWS Control Tower, puede reutilizar el bucket de S3 de la cuenta del archivo de registros para este fin.
- Terraform version 0.14.6 o versión posterior, instalada y configurada. Para obtener más información, consulte Introducción - AWS (documentación de Terraform).
- Python versión 3.9.6 o una versión posterior, instalada y configurada. Para obtener más información, consulte Versiones de origen (sitio web de Python).
- AWS SDK para Python (Boto3) instalado. Para obtener más información, consulte Instalación (documentación de Boto3).
- jq está instalado y configurado. Para obtener más información, consulte Descargar jq (documentación de jq).

Limitaciones

- Este patrón es compatible con los sistemas operativos macOS y Amazon Linux 2. No se ha probado el uso de este patrón en sistemas operativos Windows.

> **Note**
>
> Se acerca el fin de la compatibilidad de Amazon Linux 2. Para obtener más información, consulte Amazon Linux 2 FAQs.

- GuardDuty no debe estar ya activado en ninguna de las cuentas ni en ninguna de las regiones de destino.
- La solución IaC de este patrón no implementa los requisitos previos.
- Este patrón ha sido diseñado para una AWS Landing Zone que satisfaga las siguientes prácticas recomendadas:
  - Zona de aterrizaje creada mediante AWS Control Tower.
  - Cuentas de AWS independientes para la seguridad y el registro.

Versiones de producto

- Versión de Terraform 0.14.6 o posterior. El código de ejemplo se ha probado en la versión 1.2.8.
- Python, versión 3.9.6 o posterior.

Arquitectura

En esta sección se ofrece información general de alto nivel sobre esta solución y la arquitectura establecida en el código de ejemplo. El siguiente diagrama muestra los recursos implementados en las distintas cuentas de la organización, dentro de una única región de AWS.

1. Terraform crea el rol GuardDutyTerraformOrgRoleAWS Identity and Access Management (IAM) en la cuenta de seguridad y en la cuenta de registro.
2. Terraform crea un bucket de S3 en la región de AWS predeterminada de la cuenta de registro. Este segmento se usa como destino de publicación para agregar todos los GuardDuty hallazgos de todas las regiones y de todas las cuentas de la organización. Terraform también crea una clave de AWS Key Management Service (AWS KMS) en la cuenta de seguridad usada para cifrar los resultados del bucket de S3, y configura el archivo automático de los resultados del bucket de S3 en el almacenamiento de S3 Glacier Flexible Retrieval.
3. Desde la cuenta de administración, Terraform designa la cuenta de seguridad como la administradora delegada. GuardDuty Esto significa que la cuenta de seguridad ahora administra el GuardDuty servicio para todas las cuentas de los miembros, incluida la cuenta de administración. Las cuentas de los miembros individuales no se pueden suspender ni deshabilitar GuardDuty por sí mismas.
4. Terraform crea el GuardDuty detector en la cuenta de seguridad para el administrador GuardDuty delegado.
5. Si aún no está activado, Terraform habilita la protección de S3. GuardDuty Para obtener más información, consulte la protección de Amazon S3 en Amazon GuardDuty (GuardDuty documentación).
6. Terraform inscribe como miembros a todas las cuentas actuales y activas de la organización. GuardDuty
7. Terraform configura al administrador GuardDuty delegado para que publique los resultados agregados de todas las cuentas de los miembros en el segmento S3 de la cuenta de registro.
8. Terraform repite los pasos 3 a 7 para cada región de AWS que elija.

Automatizar y escalar

El código de muestra proporcionado está modularizado para que pueda integrarlo en su CI/CD proceso de implementación automática.

Tools (Herramientas)

Servicios de AWS

- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- Amazon GuardDuty es un servicio de supervisión continua de la seguridad que analiza y procesa los registros para identificar actividades inesperadas y potencialmente no autorizadas en su entorno de AWS.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.
- AWS Organizations es un servicio de administración de cuentas que le permite agrupar varias cuentas de AWS en una organización que usted crea y administra de manera centralizada.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS SDK para Python (Boto3) es un kit de desarrollo de software que permite integrar su aplicación, biblioteca o script de Python con los servicios de AWS.

Otras herramientas y servicios

- HashiCorp Terraform es una aplicación de interfaz de línea de comandos que le ayuda a usar código para aprovisionar y administrar la infraestructura y los recursos de la nube.
- Python es un lenguaje de programación informático de uso general.
- jq es un procesador de línea de comandos que le ayuda a trabajar con archivos JSON.

Repositorio de código

El código de este patrón está disponible en el GitHub repositorio -. amazon-guardduty-for-aws organizations-with-terraform

Epics

Habilitar GuardDuty en la organización

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	En un intérprete de comandos de Bash, ejecute el siguiente comando. En Clonar el repositorio, en la sección de información adicional, puedes copiar el comando completo que contiene la URL del GitHub repositorio. De este modo, se clona el organizations-with-terraform repositorio amazon-guardduty-for-aws- desde GitHub. `git clone <github-repository-url>`	DevOps ingeniero
Edite el archivo de configuración de Terraform.	1. En la carpeta `root` del repositorio clonado, replique el archivo configuration.json.sample ejecutando el siguiente comando. `cp configuration.json.sample configuration.json` 2. Edite el nuevo archivo configuration.json y defina los valores de cada una de las siguientes variables:	DevOps ingeniero, AWS general, Terraform, Python

Tarea	Descripción	Habilidades requeridas
	• `management_acc_id` – ID de cuenta de la cuenta de administración. • `delegated_admin_acc_id` – ID de cuenta de la cuenta de seguridad. • `logging_acc_id` – ID de cuenta de la cuenta de registro. • `target_regions` — Lista separada por comas de las regiones de AWS en las que desea activarlas. GuardDuty • `organization_id` — ID de AWS Organizations de la organización en la que está realizando la activación GuardDuty. • `default_region` – Región en la que se almacena su estado de Terraform en la cuenta de administración. Es la misma región en la que implementó el bucket de S3 y la tabla de DynamoDB para el backend de Terraform. • `role_to_assume_for_role_creation` – Nombre que desea asignar a un nuevo rol	

Tarea	Descripción	Habilidades requeridas
	de IAM en las cuentas de seguridad y registro. Creará este nuevo rol en la siguiente historia. Terraform asume este rol para crear el rol de IAM `GuardDutyTerraformOrgRole` en las cuentas de seguridad y registro. • `finding_publishing_frequency` — Frecuencia con la que se GuardDuty publican los resultados en el segmento S3. • `guardduty_findings_bucket_region` – Región preferida en la que desea crear el bucket de S3 para los resultados publicados. • `logging_acc_s3_bucket_name` – Nombre preferido del bucket de S3 para los resultados publicados. • `security_acc_kms_key_alias` — Alias de AWS KMS para la clave utilizada para cifrar GuardDuty los hallazgos. • `s3_access_log_bucket_name` — Nombre	

Tarea	Descripción	Habilidades requeridas
	de un depósito de S3 preexistente en el que desea recopilar los registros de acceso del depósito de S3 utilizado para GuardDuty las búsquedas. Este depósito debe estar en la misma región de AWS que el depósito de GuardDuty hallazgos. • `tfm_state_backend_s3_bucket` – Nombre del bucket de S3 preexistente para almacenar el estado del backend remoto de Terraform. • `tfm_state_backend_dynamodb_table` – Nombre de la tabla de DynamoDB preexistente para bloquear el estado de Terraform. 3. Guarde y cierre el archivo de configuración.	

Tarea	Descripción	Habilidades requeridas
Genere CloudFormation plantillas para nuevas funciones de IAM.	Este patrón incluye una solución de IaC para crear dos CloudFormation plantilla s. Estas plantillas crean dos roles de IAM que Terraform usará durante el proceso de configuración. Estas plantilla s satisfacen las prácticas recomendadas de seguridad de permisos con privilegio mínimo. 1. En un intérprete de comandos de Bash, en la carpeta `root` del repositor io, acceda a `cfn-templ ates/` . Esta carpeta contiene archivos de CloudFormation plantillas con talones. 2. Ejecute el comando siguiente. Este paso reemplaza los stubs por los valores que proporcionó en el archivo configuration.json . `bash scripts/r eplace_config_stub s.sh` 3. Confirme que se hayan creado CloudFormation las siguientes plantillas	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas
	en la `cfn-templates/` carpeta: • management-account-role.yaml: este archivo contiene la definición del rol y los permisos asociados al rol de IAM en la cuenta de administración, que tiene los permisos mínimos necesarios para completar este patrón. • role-to-assume-for-role-creation.yaml: este archivo contiene la definición del rol y los permisos asociados al rol de IAM en las cuentas de seguridad y registro. Terraform asume esta función para crear la función en estas cuentas. GuardDutyTerraform OrgRole	

Tarea	Descripción	Habilidades requeridas
Cree el rol de IAM.	Siguiendo las instrucciones de Creación de una pila (CloudFormation documentación), haga lo siguiente: 1. Implemente la pila role-to-assume-for-role-creation.yaml tanto en la cuenta de seguridad como en la de registro. 2. Implemente la pila .yaml en la cuenta de administraciónmanagement-account-role. Cuando haya creado correctamente la pila y el resultado muestre el estado `CREATE_COMPLETE` , anote el nombre de recurso de Amazon (ARN) de este nuevo rol.	DevOps ingeniero, AWS general
Asuma el rol de IAM de la cuenta de administración	Como práctica recomendada de seguridad, le recomendamos que asuma la nueva función de management-account-roleIAM antes de continuar. En la interfaz de la línea de comandos de AWS (AWS CLI), ejecute el comando de Asumir el rol de IAM de la cuenta de administración, en la sección Información adicional.	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas
Ejecute el script de configuración.	En la carpeta `root` del repositorio, ejecute el siguiente comando para iniciar el script de configuración. `bash scripts/full-setup.sh` El script full-setup.sh realiza las siguientes acciones: • Exporta todos los valores de configuración como variables de entorno • Genera los archivos de código backend.tf y terraform.tfvars para cada módulo de Terraform • Permite un acceso confiable a GuardDuty la organización a través de la AWS CLI. • Importa el estado de la organización al estado de Terraform • Crea el bucket de S3 para publicar los resultados en la cuenta de registro • Crea la clave de AWS KMS para cifrar los resultados en la cuenta de seguridad • Se habilita GuardDuty en toda la organización y en todas las regiones seleccionadas, tal y como se describe	DevOps ingeniero, Python

Tarea	Descripción	Habilidades requeridas
	en la sección de arquitectura	

(Opcional) Desactivar GuardDuty en la organización

Tarea	Descripción	Habilidades requeridas
Ejecute el script de limpieza.	Si utilizó este patrón GuardDuty para activarlo en la organización y desea deshabilitarlo GuardDuty, ejecute el siguiente comando en la `root` carpeta del repositorio para iniciar el script cleanup-gd.sh. `bash scripts/cleanup-gd.sh` Este script se desactiva GuardDuty en la organización de destino, elimina todos los recursos desplegados y restaura la organización a su estado anterior antes de utilizar Terraform para activarlo. GuardDuty **Note** Este script no elimina los archivos de estado de Terraform ni bloquea los archivos de los backends locales y remotos. Si	DevOps ingeniero, AWS general, Terraform, Python

Tarea	Descripción	Habilidades requeridas
	necesita hacerlo, debe llevar a cabo estas acciones manualmente. Este script tampoco elimina la organización importada ni las cuentas que gestiona. El acceso seguro para GuardDuty no está desactivado como parte del script de limpieza.	
Elimine los roles de IAM.	Elimine las pilas que se crearon con las plantillas role-to-assume-for-role-creation.yaml y .yaml. management-account-role CloudFormation Para obtener más información, consulta Eliminar una pila (documentación). CloudFormation	DevOps ingeniero, AWS general

Recursos relacionados

Documentación de AWS

- Administrar varias cuentas (GuardDuty documentación)
- Otorgar privilegio mínimo (documentación de IAM)

Marketing de AWS

- Amazon GuardDuty
- AWS Organizations

Otros recursos

- Terraform
- Documentación de Terraform CLI

Información adicional

Clone el repositorio

Ejecute el siguiente comando para clonar el GitHub repositorio.

```
git clone https://github.com/aws-samples/amazon-guardduty-for-aws-organizations-with-terraform
```

Asuma el rol de IAM de la cuenta de administración

Para asumir el rol de IAM en la cuenta de administración, ejecute el siguiente comando. Sustituya `<IAM role ARN>` con el ARN del rol de IAM.

```
export ROLE_CREDENTIALS=$(aws sts assume-role --role-arn <IAM role ARN> --role-session-name AWSCLI-Session --output json)
export AWS_ACCESS_KEY_ID=$(echo $ROLE_CREDENTIALS | jq .Credentials.AccessKeyId | sed 's/"//g')
export AWS_SECRET_ACCESS_KEY=$(echo $ROLE_CREDENTIALS | jq .Credentials.SecretAccessKey | sed 's/"//g')
export AWS_SESSION_TOKEN=$(echo $ROLE_CREDENTIALS | jq .Credentials.SessionToken | sed 's/"//g')
```

Verifique las mejores prácticas operativas para PCI DSS 4.0 mediante AWS Config

Tala Qraitem y Alex Goff, Amazon Web Services

Resumen

El Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS) describe los protocolos técnicos y operativos esenciales para proteger los datos de pago. El PCI DSS se desarrolló para fomentar y mejorar la seguridad de los datos de las cuentas de tarjetas de pago. También facilita la adopción global de medidas de seguridad coherentes. Si bien está diseñado específicamente para entornos con datos de cuentas de tarjetas de pago, puede utilizar el PCI DSS para protegerse contra las amenazas y proteger otros elementos del ecosistema de pagos.

La versión 4.0 del PCI DSS se publicó para abordar los requisitos cambiantes, proporcionar aclaraciones u orientación adicional y mejorar la estructura y el formato del estándar. Para más información sobre los cambios, consulte Summary of changes from PCI DSS version 3.2.1 to 4.0.

Un paquete de AWS Config conformidad es un conjunto de AWS Config reglas y acciones correctivas que le ayudan a crear controles de seguridad, operativos o de optimización de costos. Puede implementar un paquete de conformidad como una sola entidad en un Cuenta de AWS solo lugar Región de AWS, o puede implementarlo en toda la organización en uno. AWS Organizations

Los paquetes de conformidad de la versión 4.0 de PCI DSS complementan y se basan en el paquete de conformidad de la versión 3.2.1. Las reglas del paquete de conformidad se corresponden con las reglas del estándar. Para más información, consulte la asignación que se proporciona en la sección Adjuntos. Puede elegir entre dos versiones de este paquete de conformidad: una que incluye los tipos de recursos globales y otra que los excluye.

> **Important**
>
> Los paquetes de conformidad no están diseñados para garantizar plenamente el cumplimiento de un estándar de gobernanza o cumplimiento específicos. Debe evaluar si su uso cumple con los requisitos legales y normativos aplicables.

Requisitos previos y limitaciones

Requisitos previos

- Tenga una Cuenta de AWS activa.
- Configurar. AWS Config
- Cumpla los requisitos previos de los paquetes de conformidad.
- Implemente el paquete de conformidad de la versión 3.2.1 de PCI DSS.
- Tenga permisos para acceder a los paquetes de conformidad AWS Config y gestionarlos. Para ver una política de ejemplo, consulte la sección Información adicional de este patrón.

Limitaciones

- Cuenta de AWS Tiene cuotas predeterminadas, antes denominadas límites, para cada uno Servicio de AWS de ellos. A menos que se indique lo contrario, cada cuota es específica de la región. Puede solicitar los aumentos de algunas cuotas, pero no todas se pueden aumentar. Asegúrese de familiarizarse con los límites de servicio de AWS Config, tales como los límites de los paquetes de conformidad de una sola cuenta y los paquetes de conformidad de la organización.
- La versión de este paquete de conformidad que incluye los tipos de recursos globales está destinada a implementarse solo en la región de `us-east-1`.
- La versión de este paquete de conformidad que excluye los tipos de recursos globales está destinada a implementarse solo en las regiones siguientes.
  - `ap-east-1`
  - `ap-south-1`
  - `ap-northeast-2`
  - `ap-southeast-1`
  - `ap-southeast-2`
  - `ap-northeast-1`
  - `ca-central-1`
  - `eu-central-1`
  - `eu-west-1`
  - `eu-west-2`
  - `eu-west-3`
  - `eu-north-1`
  - `sa-east-1`

- us-east-2
- us-west-1
- us-west-2

Tools (Herramientas)

Servicios de AWS

- AWS Configproporciona una vista detallada de sus recursos Cuenta de AWS y de cómo están configurados. Le ayuda a identificar cómo se relacionan los recursos entre sí y cómo han cambiado sus configuraciones a lo largo del tiempo.
- AWS Systems Manager lo ayuda a administrar las aplicaciones y la infraestructura que se ejecutan en la Nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo necesario para detectar y resolver problemas operativos y le ayuda a administrar sus AWS recursos de forma segura y a escala.

Repositorio de código

Los paquetes de conformidad se encuentran en el repositorio de paquetes de AWS Config conformidad. GitHub Este repositorio contiene las siguientes plantillas relacionadas con la versión 4.0 de PCI DSS:

- Mejores prácticas operativas para PCI-DSS-v4.0- .yaml including-global-resourcetypes
- Prácticas recomendadas operativas para PCI-DSS-v4.0- .yaml excluding-global-resourcetypes

Epics

Implementación y administración del paquete de conformidad

Tarea	Descripción	Habilidades requeridas
Descargue el paquete de conformidad.	Si va a implementar el paquete de conformidad en la región, descargue la plantilla Operational-Best-Practices-for-PCI-DSS-v4.0- .yaml. us-	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`east-1` including-global-resourcetypes Si vas a implementar el paquete de conformidad en otra región, descarga la plantilla Operational-Best-Practices-for-PCI-DSS-v4.0- .yaml. excluding-global-resourcetypes	
(Opcional) Modifique el paquete de conformidad.	Puede modificar la plantilla del paquete de conformidad para adaptarla a las necesidades únicas de su organización. Por ejemplo, puede crear acciones de corrección personalizadas. Para obtener más información sobre cómo crear y modificar plantillas, consulte Creación de plantillas para paquetes de conformidad personalizados en la AWS Config documentación.	AWS general

Tarea	Descripción	Habilidades requeridas
Implemente el paquete de conformidad.	Si va a realizar la implementación en un destino Cuenta de AWS o Región de AWS, siga las instrucciones que se indican en la documentación sobre la AWS Config implementación de paquetes de conformidad. Puede usar el Consola de administración de AWS o el AWS Command Line Interface (AWS CLI). Si va a implementar el paquete de conformidad en una organización AWS Organizations, siga las instrucciones de la documentación sobre cómo implementar el paquete de AWS Config conformidad mediante la AWS Systems Manager configuración rápida.	AWS general
(Opcional) Edite el paquete de conformidad.	Si desea editar el paquete de conformidad, siga las instrucciones de Edición de los paquetes de conformidad de la documentación. AWS Config Puede utilizar el Consola de administración de AWS o el. AWS CLI	AWS general

Tarea	Descripción	Habilidades requeridas
(Opcional) Elimine el paquete de conformidad.	Si desea eliminar el paquete de conformidad, siga las instrucciones de la documentación sobre cómo eliminar los AWS Config paquetes de conformidad. Puede utilizar el Consola de administración de AWS o el. AWS CLI	AWS general

Recursos relacionados

AWS resources

- Paquetes de conformidad para AWS Config (AWS Config documentación)
- Implemente AWS Config el paquete de conformidad mediante Quick Setup (documentación de Systems Manager)
- Cumple con las normas PCI DSS en AWS (sitio web)AWS
- PCI DSS version 4.0 on AWS (guía de cumplimiento)

Recursos de PCI DSS

- PCI DSS version 4.0 Resource Hub
- Biblioteca de documentos del Consejo de Normas de Seguridad PCI
- Summary of changes from PCI DSS version 3.2.1 to 4.0

Información adicional

El siguiente es un ejemplo de política AWS Identity and Access Management (IAM) que permite al usuario acceder a los paquetes de conformidad AWS Config y gestionarlos:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "config:PutConfigRule",
                "config:PutConformancePack",
                "config:DeleteConfigRule",
                "config:DeleteRemediationConfiguration",
                "config:DeleteConformancePack",
                "config:PutRemediationConfigurations",
                "config:BatchGetAggregateResourceConfig",
                "config:BatchGetResourceConfig",
                "config:Get*",
                "config:Describe*",
                "config:Deliver*",
                "config:List*",
                "config:Select*"
            ],
            "Resource": "*"
        }
    ]
}
```

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Más patrones

- Acceda a un host bastión mediante Session Manager y Amazon EC2 Instance Connect
- Acceda a las aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS Fargate PrivateLink, AWS y un Network Load Balancer
- Acceda a las aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS PrivateLink y un Network Load Balancer
- Acceda a aplicaciones de contenedores de forma privada en Amazon EKS mediante AWS PrivateLink y un Network Load Balancer
- Permitir a EC2 las instancias el acceso de escritura a los buckets de S3 en las cuentas de AMS
- Asociar un AWS CodeCommit repositorio de una cuenta Cuenta de AWS a Amazon SageMaker AI Studio Classic de otra cuenta
- Autentique a los usuarios de la aplicación React mediante las interfaces de usuario de Amazon Cognito y AWS Amplify
- Automatice la adición o actualización de entradas de registro de Windows con AWS Systems Manager
- Automatice la aplicación del cifrado en AWS Glue mediante una CloudFormation plantilla de AWS
- Adjunte automáticamente una política gestionada por AWS para Systems Manager a los perfiles de EC2 instancia mediante Cloud Custodian y AWS CDK
- Cifrar automáticamente los volúmenes de Amazon EBS nuevos y existentes
- Bloquee el acceso público a Amazon RDS mediante Cloud Custodian
- Centralice la resolución de DNS mediante AWS Managed Microsoft AD Microsoft Active Directory local
- Implemente un escaneo Checkov personalizado y centralizado para aplicar la política antes de implementar AWS la infraestructura
- Comprueba EC2 las instancias para ver si hay etiquetas obligatorias en el lanzamiento
- Configurar el acceso entre cuentas a Amazon DynamoDB
- Configure el cifrado HTTPS para Oracle JD Edwards EnterpriseOne en Oracle WebLogic mediante un Application Load Balancer
- Configure autenticación TLS mutua para aplicaciones ejecutadas en Amazon EKS
- Configure la autenticación de Windows para Amazon RDS for Microsoft SQL Server mediante AWS Managed Microsoft AD
- Conectar mediante un túnel SSH en pgAdmin

- Crear una aplicación React con AWS Amplify y añadir autenticación con Amazon Cognito
- Cree un informe con los hallazgos de Network Access Analyzer sobre el acceso entrante a Internet en múltiples Cuentas de AWS
- Personaliza las CloudWatch alertas de Amazon para AWS Network Firewall
- Implemente una ChatOps solución para gestionar los resultados de los escaneos SAST mediante Amazon Q Developer en aplicaciones de chat, acciones personalizadas y CloudFormation
- Implemente la validación de seguridad de la codificación en tiempo real mediante un servidor MCP con Kiro y otros asistentes de codificación
- Documentación del diseño de su AWS Landing Zone
- Habilite conexiones cifradas para instancias de base de datos de PostgreSQL en Amazon RDS
- Cifrar una instancia de base de datos de Amazon RDS para PostgreSQL existente
- Imponga el etiquetado automático de las bases de datos de Amazon RDS en el lanzamiento
- Imponga el etiquetado de los clústeres de Amazon EMR en el lanzamiento
- Asegúrese de que el registro de Amazon EMR en Amazon S3 esté habilitado en el lanzamiento
- Genere una CloudFormation plantilla de AWS que contenga las reglas administradas por AWS Config mediante Troposphere
- Reciba notificaciones de Amazon SNS cuando cambie el estado de clave de una clave de AWS KMS
- Ayudar a reforzar el etiquetado en DynamoDB
- Identifique y avise cuando los recursos de Amazon Data Firehose no estén cifrados con una clave AWS KMS
- Implemente la autenticación basada en Microsoft Entra ID en una aplicación de mainframe modernizada de AWS Blu Age
- Implemente la autenticación SAML 2.0 para Amazon WorkSpaces mediante Auth0 y AWS Managed Microsoft AD
- Implemente SHA1 el hash para los datos de PII al migrar de SQL Server a PostgreSQL
- Mejore el rendimiento operativo habilitando Amazon DevOps Guru en varias regiones y cuentas de AWS y OUs con la CDK de AWS
- Incorpore y migre instancias de EC2 Windows a una cuenta de AWS Managed Services
- Migración de Amazon RDS para Oracle a Amazon RDS para PostgreSQL en modo SSL mediante AWS DMS
- Migración de ELK Stack a Elastic Cloud en AWS

- Migre una carga de trabajo de F5 BIG-IP a F5 BIG-IP VE en Nube de AWS
- Aprovisionamiento de roles de IAM con privilegio mínimo mediante la implementación de una solución de máquina expendedora de roles
- Proteja y optimice el acceso de los usuarios a una base de datos de federación DB2 en AWS mediante contextos de confianza
- Envíe AWS WAF registros a Splunk mediante AWS Firewall Manager Amazon Data Firehose
- Sirva contenido estático en un bucket de Amazon S3 a través de una VPC mediante Amazon CloudFront
- Configure el end-to-end cifrado para aplicaciones en Amazon EKS mediante cert-manager y Let's Encrypt
- Utilice el usuario IDs en las políticas de IAM para el control de acceso y la automatización
- Verifique que los equilibradores de carga ELB requieran la terminación de TLS
- Visualización de los registros y las métricas de AWS Network Firewall mediante Splunk
- Visualice los informes de credenciales de IAM para todas las cuentas de AWS mediante Amazon Quick Sight

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.