Conceptos y procedimientos de AMS Accelerate

# Guía del usuario de AMS Accelerate

Version May 26, 2026

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

# Guía del usuario de AMS Accelerate: Conceptos y procedimientos de AMS Accelerate

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

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

# Table of Contents

¿Qué es AMS Accelerate? ..... 1
Planes de operaciones ..... 1
Acelere el plan de operaciones ..... 2
Plan de operaciones avanzado ..... 2
Funcionamiento ..... 3
Términos clave ..... 3
Descripción del servicio ..... 10
Características del plan de operaciones de AWS Managed Services (AMS) AMS Accelerate ..... 10
Configuraciones admitidas ..... 14
Servicios admitidos ..... 16
Funciones y responsabilidades ..... 20
Alcance de los cambios realizados por AMS Accelerate ..... 35
Sistemas operativos no compatibles ..... 37
Contacto y escalación ..... 38
Horarios de contacto ..... 38
Horario comercial ..... 39
Ruta de escalación ..... 39
Inventario de recursos ..... 40
Controles de infraestructura ..... 40
Introducción ..... 48
Incorporación ..... 48
Requisitos previos de incorporación ..... 48
Paso 1. Descubrimiento de cuentas ..... 51
Paso 2. Recursos de gestión de la incorporación ..... 53
Paso 3. Funciones de incorporación con políticas predeterminadas ..... 63
Paso 4. Personalice las funciones ..... 73
Uso de las consolas AMS ..... 76
Patrones AMS ..... 77
Cómo funcionan los patrones AMS ..... 78
Patrones AMS ..... 78
Configuración de instancias automatizada ..... 82
Funcionamiento ..... 83
Instalación automática de SSM Agent ..... 84

Cambios automatizados en la configuración de las instancias ..... 86
Fuera de AMS Accelerate ..... 90
Efectos de desconexión ..... 91
Desembarque con dependencias ..... 93
Obtener asistencia para dejar de embarcar ..... 94
Ajustes de notificación ..... 94
Etiquetado ..... 96
Etiquetas ..... 97
¿Qué son las etiquetas? ..... 98
Cómo funciona el etiquetado ..... 98
Etiquetas administradas por el cliente ..... 98
Acelere las etiquetas gestionadas ..... 102
Etiquetas proporcionadas por el cliente ..... 103
Herramientas de administración de etiquetas ..... 104
Etiquetador de recursos ..... 104
CloudFormation ..... 125
Terraform ..... 129
Informes de incidentes, solicitudes de servicio y preguntas sobre facturación ..... 131
Administración de incidentes ..... 131
¿Qué es la gestión de incidentes? ..... 132
Cómo funcionan la respuesta y la resolución de incidentes ..... 133
Trabajando con incidentes ..... 134
Gestión de solicitudes de servicio ..... 137
Cuándo usar una solicitud de servicio ..... 138
Cómo funciona la administración de solicitudes de servicio ..... 139
Crear una solicitud de servicio ..... 140
Supervisión y actualización de una solicitud de servicio ..... 141
Gestionar las solicitudes de servicio con la API de soporte ..... 142
Respuesta a una solicitud de servicio generada por AMS Accelerate ..... 143
Pruebas de informes de incidentes y solicitudes de servicio ..... 144
¿Preguntas sobre facturación ..... 144
Gestión de eventos planificados ..... 145
Criterios AMS PEM ..... 145
Tipos de PEM ..... 145
El proceso AMS PEM ..... 146
PEM FAQs ..... 146

Operaciones bajo demanda ... 148
Solicitar AMS Operations On Demand ... 156
Realizar cambios en las ofertas de Operations on Demand ... 157
Informes y opciones ... 158
Informes a petición ... 158
Informes de gestión de hosts de AMS ... 159
Informes de AMS Backup ... 159
AWS Config Informe de cumplimiento de controles ... 162
Informe de configuración de respuesta de AMS Config Rules ... 164
Informes de Top Talkers prevenidos y seguimiento ... 166
Informe de detalles de cargos de facturación ... 168
Informes de Trusted Remediator ... 169
Informes de autoservicio ... 173
Operaciones de API internas ... 174
Informe de parches (diario) ... 177
Informe de Backup (diario) ... 188
Informe de incidentes (semanal) ... 193
Informe de facturación (mensual) ... 197
Informes agregados ... 200
Paneles de informes de autoservicio de AMS ... 202
Política de conservación de los datos ... 210
Fuera de SSR ... 210
Administración de accesos ... 212
Cómo acceder a la consola ... 212
Permisos para usar funciones ... 212
¿Por qué y cuándo accedemos a su cuenta ... 227
Activadores de acceso ... 227
Acceda a las funciones de IAM ... 228
¿Cómo accedemos a su cuenta ... 230
¿Cómo y cuándo usar root ... 231
Administración de la seguridad ... 232
Uso del documento SSM de Log4j para detectar incidencias ... 233
Supervisión de la seguridad de la infraestructura ... 234
Cómo utilizar roles vinculados a servicios ... 236
AWS políticas gestionadas ... 250
Protección de datos ... 259

Monitoriza con Amazon Macie ... 260
Supervise con GuardDuty ... 260
Supervise con el firewall DNS Amazon Route 53 Resolver ... 262
Cifrado de datos ... 263
AWS Identity and Access Management ... 264
Autenticación con identidades en AMS Accelerate ... 264
Administración de acceso mediante políticas ... 272
Respuesta a un incidente de seguridad ... 273
Funcionamiento ... 274
Preparación ... 274
Detect ... 275
Análisis ... 276
Contención ... 277
Erradicación ... 279
Recuperar ... 280
Informe posterior al incidente ... 280
Guías de respuesta a incidentes de seguridad ... 281
Registro y supervisión de eventos de seguridad ... 287
Conformidad de la configuración ... 288
Biblioteca de reglas AMS Config ... 289
Respuestas a las infracciones ... 315
Crear excepciones a las reglas ... 317
Reduzca AWS Config los costos ... 318
Respuestas a los hallazgos personalizadas ... 318
Respuesta a incidentes ... 320
Respuesta a incidentes e incorporación ... 321
Resiliencia ... 321
Control de seguridad para sistemas end-of-support operativos ... 322
Prácticas recomendadas de seguridad ... 322
Revisiones de seguridad de la solicitud de cambios ... 322
Proceso de gestión de riesgos de seguridad del cliente ... 323
Estándares técnicos de AMS Accelerate ... 324
Controles estándar en AMS Accelerate ... 324
Cambios que introduzcan riesgos de seguridad altos o muy altos en su entorno ... 340
Preguntas frecuentes sobre seguridad ... 342
¿Cuándo acceden los ingenieros de operaciones de AMS a mis entornos? ... 342

¿Qué funciones asumen los ingenieros de operaciones de AMS cuando acceden a mis cuentas? ..... 342
¿Cómo accede un ingeniero de operaciones de AMS a mi cuenta? ..... 343
¿Cómo hago un seguimiento de los cambios realizados por AMS en mis AWS cuentas gestionadas por AMS? ..... 343
¿Cuáles son los controles de proceso para que el ingeniero de operaciones de AMS acceda a mi cuenta? ..... 344
¿Cómo se gestiona el acceso privilegiado? ..... 345
¿Los ingenieros de operaciones de AMS utilizan MFA? ..... 345
¿Qué ocurre con su acceso cuando un empleado de AMS deja la organización o cambia de puesto? ..... 345
¿Qué controles de acceso regulan el acceso de los ingenieros de operaciones de AMS a mis cuentas? ..... 345
¿Cómo monitorea AMS el acceso de los usuarios root? ..... 346
¿Cómo responde AMS a los incidentes de seguridad? ..... 346
¿A qué marcos y certificaciones estándares del sector se adhiere AMS? ..... 346
¿Cómo puedo acceder a los informes más recientes sobre la certificación, los marcos y el cumplimiento de la seguridad? AWS ..... 347
¿Comparte AMS diagramas de arquitectura de referencia sobre los distintos aspectos de las funciones de AMS? ..... 348
¿Cómo controla AMS quién accede a mis cuentas y qué necesita la empresa para acceder a ellas? ..... 348
¿Los ingenieros de AMS tienen acceso a mis datos almacenados en un servicio de almacenamiento de AWS datos, como Amazon S3, Amazon RDS, DynamoDB y Amazon Redshift? ..... 348
¿Los ingenieros de AMS tienen acceso a los datos de los clientes almacenados en Amazon EBS, Amazon EFS y Amazon FSx? ..... 349
¿Cómo se restringe o controla el acceso a los puestos de automatización que tienen altos privilegios en mis entornos? ..... 349
¿Cómo implementa AMS el principio del mínimo privilegio tal como se propugna en el AWS Well-Architected Framework para las funciones de automatización? ..... 349
¿Qué sistemas de registro y supervisión se utilizan para detectar intentos de acceso no autorizados o actividades sospechosas relacionadas con funciones de automatización? ..... 350
¿Cómo se gestionan los incidentes o brechas de seguridad relacionados con la infraestructura de automatización y qué protocolos ayudan a responder y mitigar con rapidez? ..... 350

¿Se realizan periódicamente evaluaciones de seguridad, análisis de vulnerabilidades y pruebas de penetración en la infraestructura de automatización? ..... 350
¿Cómo se restringe el acceso a la infraestructura de automatización únicamente al personal autorizado? ..... 351
¿Qué medidas se implementan para mantener los estándares de seguridad y evitar el acceso no autorizado o las filtraciones de datos en el proceso de automatización? ..... 351
¿Están activadas la detección o el monitoreo de anomalías para el acceso o el registro de auditoría para detectar el aumento de privilegios o el uso indebido del acceso a fin de alertar proactivamente al equipo de AMS? ..... 352
¿Qué tipos de datos de clientes se extraen de las cuentas gestionadas por AMS y cómo se utilizan y almacenan? ..... 352
Supervisión y gestión de eventos ..... 353
¿Qué es la supervisión? ..... 353
Cómo funciona la supervisión ..... 354
Notificaciones agrupadas de instancias EC2 ..... 356
Notificación de alertas basada en etiquetas ..... 357
Alertas del monitoreo de referencia en AMS ..... 358
Notificaciones de incidentes compatibles con las aplicaciones en AMS ..... 384
AppRegistry Incorpore y cree aplicaciones ..... 385
Cree etiquetas para permitir el enriquecimiento de mayúsculas y minúsculas ..... 386
Personalice la gravedad de los casos de soporte de AMS para sus aplicaciones ..... 386
Revisa los permisos necesarios ..... 387
Administrador de alarmas ..... 388
Cómo funciona Alarm Manager ..... 388
Cómo empezar con Alarm Manager ..... 390
Etiquetas de Alarm Manager ..... 391
Perfiles de configuración de Alarm Manager ..... 395
Creación de CloudWatch alarmas adicionales ..... 414
Remediación automática de alertas por parte de AMS ..... 414
Fallo en la comprobación del estado de EC2: notas sobre la automatización de la remediación ..... 421
Automatización de la corrección del uso de volúmenes de EC2 ..... 421
Automatización de la corrección de eventos de bajo almacenamiento en Amazon RDS ..... 422
Automatización de la remediación de volúmenes y capacidad de ONTAP ..... 423
Router de eventos AMS ..... 424
Amazon EventBridge Managed Rules implementadas por AMS ..... 424

Creación de reglas administradas para AMS ... 427
Edición de reglas gestionadas para AMS ... 427
Eliminar reglas administradas para AMS ... 427
Remediador de confianza ... 427
Ventajas principales ... 427
Cómo funciona Trusted Remediator ... 428
Términos clave ... 429
Comience con Trusted Remediator ... 430
Recomendaciones de Compute Optimizer compatibles ... 433
Comprobaciones compatibles Trusted Advisor ... 438
Recomendaciones de Security Hub (CSPM) compatibles ... 499
Configure la corrección de comprobaciones ... 502
Flujo de trabajo de decisiones en modo ejecución ... 506
Configure los tutoriales de corrección ... 506
Trabaje con las soluciones ... 510
Registros de remediación ... 514
Integración con Quick ... 520
Prácticas recomendadas ... 522
FAQs ... 523
Supervisión y gestión de incidentes para EKS ... 527
¿Qué es la supervisión y la gestión de incidentes para Amazon EKS? ... 527
Cómo funcionan la supervisión y la gestión de incidentes para Amazon EKS ... 528
Matriz de responsabilidad de AMS (RACI) ... 529
Alertas de referencia ... 532
Alertas y acciones ... 532
Requisitos ... 540
Incorporación ... 542
Fuera de bordo ... 543
Gestión de la continuidad ... 545
Cómo funciona la gestión de la continuidad ... 545
Seleccione un plan de respaldo de AMS ... 546
Plan de respaldo de AMS predeterminado ... 547
Plan de respaldo mejorado ... 547
Plan de respaldo para datos sensibles ... 548
Plan de respaldo para la incorporación de AMS Accelerate ... 548
Etiquete sus recursos para respaldarlos ... 549

Vea las copias de seguridad en las bóvedas de AMS ... 551
Supervisión e informes de las copias de seguridad ... 552
Administración de parches ... 554
Recomendaciones de aplicación de parches ... 555
Recomendaciones sobre la responsabilidad del parche ... 556
Guía para los equipos de aplicaciones ... 557
Guía para los equipos de operaciones de seguridad ... 557
Guía para los equipos de gobierno y cumplimiento ... 558
Ejemplo de diseño para una aplicación Windows de alta disponibilidad ... 558
Preguntas frecuentes sobre recomendaciones de parches ... 559
Cree una ventana de parches ... 559
Límites del período de mantenimiento de los parches ... 560
Crea una ventana de parches de Patch Tuesday: consola AMS ... 561
Crear ventana de parches: CloudFormation ... 562
Crear ventana de parches: consola de Systems Manager ... 563
Crear ventana de parches: Systems Manager CLI ... 565
Parche con ganchos ... 567
Los enganches de conexión AMS RACI ... 567
Cree documentos SSM para los patch hooks ... 568
Configure la ventana de mantenimiento de parches de AMS para utilizar sus documentos de comandos de SSM como enlaces de parches de AMS ... 569
Línea base del parche AMS Accelerate ... 570
Línea base predeterminada del parche ... 571
Línea base de parches personalizada ... 571
Permisos de aplicación de parches bajo demanda ... 572
Comprenda las notificaciones y los fallos de los parches ... 573
Solicitudes de servicios de parches y notificaciones por correo electrónico ... 573
Notificaciones de parches a través de eventos CloudWatch ... 574
Investigación de errores de parches ... 578
Optimización de costes con AMS Resource Scheduler ... 580
Uso de recursos con Resource Scheduler ... 581
Programador de recursos de incorporación ... 583
Personalización del programador de recursos ... 583
Uso del programador de recursos ... 584
Trabajando con períodos y cronogramas ... 587
Etiquetado de recursos ... 593

Estimador de costos ..... 594
Supresor de alarmas ..... 595
Administración de registros: ..... 596
Administración de registros: AWS CloudTrail ..... 596
Acceder a los CloudTrail registros y auditarlos ..... 598
Protección y conservación de los registros CloudTrail ..... 598
Acceso a los registros de Amazon EC2 ..... 598
Conservación de los registros de Amazon EC2 ..... 599
Administración de registros — Amazon EC2 ..... 599
Administración de registros: Amazon VPC Flow Logs ..... 600
Seguimiento de los cambios ..... 602
Ver tus registros de cambios ..... 603
Consultas predeterminadas ..... 604
Modificación del filtro de fecha y hora en las consultas ..... 614
Ejemplos de consultas por defecto ..... 616
Cambiar los permisos de registro ..... 627
AWS Systems Manager en Accelerate ..... 629
Documentos disponibles sobre AMS Accelerate SSM ..... 629
Versiones de documentos AMS Accelerate SSM ..... 629
Precios de Systems Manager ..... 630
Historial de revisión ..... 631
Actualizaciones anteriores ..... 657
..... dclxxxvi

# ¿Qué es AMS Accelerate?

Bienvenido a AMS Accelerate para Amazon Web Services (AWS). AMS Accelerate ofrece una gama de servicios operativos para ayudarlo a alcanzar la excelencia operativa en AWS. Ya sea que acabe de empezar a trabajar en la nube, desee ampliar su equipo actual o necesite una solución operativa a largo plazo, Accelerate puede ayudarle a cumplir sus objetivos operativos en la nube. Al aprovechar Servicios de AWS una biblioteca de automatizaciones, configuraciones y manuales, ofrecemos una solución end-to-end operativa para entornos nuevos y existentes. AWS

El servicio Accelerate aprovecha un conjunto de funciones Servicios de AWS y funciones nativas para proporcionar un conjunto integral de capacidades de administración de infraestructura. Dentro de ellas Servicios de AWS, Accelerate crea y mantiene conjuntos selectos de controles de monitoreo, barreras de detección, automatizaciones y manuales para operar la infraestructura de manera segura y compatible.

Temas


- Planes de operaciones de AMS
- Uso del plan de operaciones AMS Accelerate
- Términos clave de AMS
- Descripción del servicio
- Capacidades para sistemas operativos no compatibles en Accelerate
- Contacto y escalación
- Inventario de recursos para Accelerate


## Planes de operaciones de AMS

AWS Managed Services (AMS) está disponible con dos planes de operaciones: AMS Accelerate y AMS Advanced. Un plan de operaciones ofrece un conjunto específico de características y tiene diferentes niveles de servicio, capacidades técnicas, requisitos, precios y restricciones. Nuestros planes de operaciones le ofrecen la flexibilidad de seleccionar las capacidades operativas del tamaño adecuado para cada una de sus cargas de AWS trabajo. En esta sección, se describen las capacidades y las diferencias, así como las responsabilidades, características y beneficios asociados a cada plan, para que pueda entender qué plan de operaciones es el mejor para sus cuentas.

Para ver una comparación detallada de las características de los dos planes de operaciones, consulte Características de AWS Managed Services.

## Plan de operaciones de AMS Accelerate

AMS Accelerate es el plan de operaciones de AMS que le ayuda a gestionar la day-to-day infraestructura de su AWS entorno nuevo o existente. AMS Accelerate ofrece servicios operativos, como supervisión, gestión de incidentes y seguridad. AMS Accelerate también ofrece un complemento de parche opcional para las cargas de trabajo EC2 basadas en Amazon que requieren parches periódicos.

Con AMS Accelerate, usted decide cuáles Cuentas de AWS quiere que opere AMS Accelerate, las regiones de AWS en las que quiere que opere AMS Accelerate, los complementos que necesita y los acuerdos de nivel de servicio (SLAs) que necesita. Para obtener más información, consulte Uso del plan de operaciones y la descripción del servicio de AMS Accelerate.

## Plan de operaciones de AMS Advanced

AMS Advanced proporciona servicios de ciclo de vida completo para aprovisionar, ejecutar y dar soporte a su infraestructura. Además de los servicios operativos proporcionados por AMS Accelerate, AMS Advanced también incluye servicios adicionales, como la gestión de las zonas de aterrizaje, los cambios y el aprovisionamiento de la infraestructura, la gestión del acceso y la seguridad de los terminales.

AMS Advanced despliega una landing zone a la que migras tus AWS cargas de trabajo y recibes los servicios operativos de AMS. Nuestras zonas de destino gestionadas con múltiples cuentas vienen preconfiguradas con la infraestructura necesaria para facilitar la autenticación, la seguridad, la creación de redes y el registro.

AMS Advanced también incluye un sistema de gestión de cambios y accesos que protege sus cargas de trabajo al impedir el acceso no autorizado o la implementación de cambios riesgosos en su infraestructura. AWS Los clientes deben crear una solicitud de cambio (RFC) mediante nuestro sistema de gestión de cambios para implementar la mayoría de los cambios en sus cuentas de AMS Advanced. Puede crear cambios RFCs a partir de una biblioteca de cambios automatizados previamente examinados por nuestros equipos de seguridad y operaciones, o bien solicitar cambios manuales que son revisados e implementados por nuestro equipo de operaciones si los considera seguros y compatibles con AMS Advanced.

# Uso del plan de operaciones AMS Accelerate

AMS Accelerate es el plan de operaciones de AMS que permite operar la infraestructura de AWS que soporta cargas de trabajo. Tanto si sus cargas de trabajo ya están en una cuenta de AWS como si planea migrar otras nuevas, puede beneficiarse de los servicios operativos de AMS Accelerate, como la supervisión y las alertas, la gestión de incidentes, la gestión de la seguridad y la gestión de copias de seguridad, sin tener que pasar por una nueva migración, sufrir tiempos de inactividad ni cambiar la forma en que utiliza AWS. AMS Accelerate también ofrece un complemento de parches opcional para cargas de trabajo EC2 basadas que requieren la aplicación de parches con regularidad.

Con AMS Accelerate, tiene la libertad de usar, configurar e implementar todos los servicios de AWS de forma nativa o con las herramientas que prefiera. Puede seguir utilizando sus mecanismos de acceso y cambio actuales, mientras que AMS aplica constantemente prácticas comprobadas que ayudan a ampliar su equipo, optimizar los costes, aumentar la seguridad y la eficiencia y mejorar la resiliencia.

Si bien AMS Accelerate puede simplificar sus operaciones, usted sigue siendo responsable del desarrollo, la implementación, las pruebas, el ajuste y la administración de las aplicaciones. AMS Accelerate solo realiza cambios en su cuenta como resultado de incidentes, alarmas, correcciones y algunas solicitudes de servicio. AMS Accelerate no aprovisiona recursos en la cuenta en su nombre. AMS Accelerate proporciona asistencia para la resolución de problemas de infraestructura que afectan a las aplicaciones, pero AMS Accelerate no accede a las configuraciones de sus aplicaciones ni las valida sin su conocimiento y aprobación. Los servicios y cambios de AMS Accelerate se proporcionan directamente en la AWS consola APIs, por lo que puede seguir aprovechando sus cuentas actuales con AWS las soluciones de AWS Marketplace disponibles. AMS Accelerate no modifica el código de sus infrastructure-as-code plantillas (por ejemplo, CloudFormation las plantillas), pero puede orientar a sus equipos sobre los cambios necesarios para seguir las mejores prácticas operativas y de seguridad.

# Términos clave de AMS

- AMS Advanced: los servicios descritos en la sección «Descripción del servicio» de la documentación avanzada de AMS. Consulte la descripción del servicio.
- Cuentas avanzadas de AMS: AWS cuentas que cumplen en todo momento todos los requisitos de incorporación avanzada de AMS. Para obtener información sobre las ventajas de AMS Advanced, los casos prácticos y ponerse en contacto con un representante de ventas, consulte AWS Managed Services.

- Cuentas AMS Accelerate: AWS cuentas que cumplen en todo momento todos los requisitos de incorporación de AMS Accelerate. Consulte Cómo empezar a utilizar AMS Accelerate.
- AWS Managed Services: AMS o AMS Accelerate.
- Cuentas de AWS Managed Services: las cuentas AMS o las cuentas AMS Accelerate.
- Recomendación fundamental: recomendación emitida AWS mediante una solicitud de servicio en la que se le informa de que es necesario tomar medidas para protegerse de posibles riesgos o interrupciones en sus recursos o en los Servicios de AWS mismos. Si decide no seguir una recomendación crítica antes de la fecha especificada, usted es el único responsable de cualquier daño que se derive de su decisión.
- Configuración solicitada por el cliente: cualquier software, servicio u otra configuración que no esté identificada en:
  - Accelerate: configuraciones compatibles o AMS Accelerate; descripción del servicio.
  - AMS Advanced: configuraciones compatibles o AMS Advanced; descripción del servicio.
- Comunicación de incidentes: AMS le comunica un incidente o usted solicita un incidente a AMS a través de un incidente creado en el Support Center de AMS Accelerate y en la consola de AMS para AMS. La consola AMS Accelerate proporciona un resumen de los incidentes y las solicitudes de servicio en el panel de control y enlaces al Support Center para obtener más información.
- Entorno gestionado: las cuentas AMS Advanced o las cuentas AMS Accelerate gestionadas por AMS.

  En el caso de AMS Advanced, se incluyen las cuentas de zona de aterrizaje multicuenta (MALZ) y de zona de aterrizaje de cuenta única (SALZ).
- Fecha de inicio de la facturación: al día hábil siguiente, AWS recibirá la información solicitada en el correo electrónico de incorporación de AWS Managed Services. El correo electrónico de incorporación de AWS Managed Services hace referencia al correo electrónico que usted envía para recopilar la información necesaria para activar los servicios gestionados de AWS en sus cuentas. AWS

  En el caso de las cuentas que usted inscriba posteriormente, la fecha de inicio de la facturación es el día siguiente al envío por parte de AWS Managed Services de una notificación de activación de AWS Managed Services para la cuenta inscrita. Se produce una notificación de activación de AWS Managed Services cuando:

  1. Concede acceso a una AWS cuenta compatible y se la entrega a AWS Managed Services.
  2. AWS Managed Services diseña y crea la cuenta de AWS Managed Services.

- Finalización del servicio: puede cancelar los servicios gestionados de AWS para todas las cuentas de AWS Managed Services o para una cuenta específica de AWS Managed Services por cualquier motivo avisando con al AWS menos 30 días de antelación mediante una solicitud de servicio. En la fecha de finalización del servicio, puede:
  1. AWS le entrega el control de todas las cuentas de AWS Managed Services o de las cuentas de AWS Managed Services especificadas, según corresponda, o
  2. Las partes eliminan las AWS Identity and Access Management funciones que dan AWS acceso a todas las cuentas de AWS Managed Services o a las cuentas de AWS Managed Services especificadas, según proceda.
- Fecha de finalización del servicio: la fecha de finalización del servicio es el último día del mes natural siguiente al final del período de preaviso de rescisión obligatorio de 30 días. Si el final del período de notificación de rescisión requerido cae después del día 20 del mes calendario, la fecha de finalización del servicio es el último día del mes calendario siguiente. Los siguientes son ejemplos de escenarios para las fechas de terminación.
  - Si el aviso de rescisión se proporciona el 12 de abril, el aviso de 30 días finaliza el 12 de mayo. La fecha de finalización del servicio es el 31 de mayo.
  - Si se proporciona un aviso de rescisión el 29 de abril, el aviso de 30 días finaliza el 29 de mayo. La fecha de finalización del servicio es el 30 de junio.
- Prestación de AWS Managed Services: AWS pone a su disposición los servicios gestionados de AWS Managed Services y los puede utilizar para cada cuenta de AWS Managed Services a partir de la fecha de inicio del servicio.
- Cancelación de cuentas de AWS Managed Services específicas: puede cancelar los servicios de AWS Managed Services de una cuenta específica de AWS Managed Services por cualquier motivo mediante AWS notificación mediante una solicitud de servicio («Solicitud de cancelación de la cuenta AMS»).

Condiciones de gestión de incidentes:

- Evento: un cambio en su entorno de AMS.
- Alerta: cada vez que un evento de un Servicio de AWS dispositivo compatible supera un umbral y activa una alarma, se crea una alerta y se envía un aviso a tu lista de contactos. Además, se crea un incidente en tu lista de incidentes.
- Incidente: una interrupción no planificada o una degradación del rendimiento de su entorno de AMS o AWS Managed Services que se traduce en un impacto según lo informado por AWS Managed Services o por usted.

- Problema: una causa raíz subyacente compartida de uno o más incidentes.
- Resolución de incidentes o resolución de un incidente:
  - AMS ha restablecido todos los servicios o recursos de AMS no disponibles relacionados con ese incidente a un estado disponible, o
  - AMS ha determinado que las pilas o los recursos no disponibles no se pueden restaurar a un estado disponible, o
  - AMS ha iniciado una restauración de la infraestructura autorizada por usted.
- Tiempo de respuesta ante un incidente: diferencia de tiempo entre el momento en que se crea un incidente y el momento en que AMS proporciona una respuesta inicial a través de la consola, el correo electrónico, el centro de servicio o el teléfono.
- Tiempo de resolución de incidentes: la diferencia de tiempo entre el momento en que AMS o usted crean un incidente y el momento en que se resuelve el incidente.
- Prioridad de incidentes: cómo AMS o usted priorizan los incidentes, ya sea baja, media o alta.
  - Baja: un problema no crítico con su servicio AMS.
  - Medio: hay un servicio de AWS disponible en su entorno gestionado, pero no funciona según lo previsto (según la descripción del servicio correspondiente).
  - Alto: (1) la consola AMS o uno o más AMS de su APIs entorno gestionado no están disponibles; o (2) una o más pilas o recursos de AMS de su entorno gestionado no están disponibles y la falta de disponibilidad impide que la aplicación desempeñe su función.

  AMS puede reclasificar los incidentes de acuerdo con las directrices anteriores.
- Restauración de la infraestructura: volver a implementar las pilas existentes, en función de las plantillas de las pilas afectadas, e iniciar una restauración de datos en función del último punto de restauración conocido, a menos que se especifique lo contrario, cuando no sea posible resolver los incidentes.

Términos de infraestructura:

- Entorno de producción gestionado: una cuenta de cliente en la que residen las aplicaciones de producción del cliente.
- Entorno no productivo gestionado: cuenta de cliente que solo contiene aplicaciones que no son de producción, como aplicaciones de desarrollo y pruebas.
- Pila de AMS: grupo de uno o más AWS recursos que AMS administra como una sola unidad.

- Infraestructura inmutable: modelo de mantenimiento de infraestructura típico de los grupos de Amazon EC2 Auto Scaling (ASGs) en el que los componentes de infraestructura actualizados (en AWS la AMI) se sustituyen en cada implementación, en lugar de actualizarse in situ. La ventaja de una infraestructura inmutable es que todos los componentes permanecen en un estado sincrónico, ya que siempre se generan a partir de la misma base. La inmutabilidad es independiente de cualquier herramienta o flujo de trabajo para crear la AMI.
- Infraestructura mutable: modelo de mantenimiento de infraestructura típico de las pilas que no son grupos de Amazon EC2 Auto Scaling y que contienen una sola instancia o solo unas pocas instancias. Este modelo es el que más se parece a la implementación de sistemas tradicional, basada en hardware, en la que un sistema se implementa al principio de su ciclo de vida y, posteriormente, las actualizaciones se van añadiendo capas a ese sistema a lo largo del tiempo. Todas las actualizaciones del sistema se aplican a las instancias de forma individual y pueden provocar un tiempo de inactividad del sistema (según la configuración de la pila) debido al reinicio de la aplicación o del sistema.
- Grupos de seguridad: firewalls virtuales para que la instancia controle el tráfico entrante y saliente. Los grupos de seguridad actúan en el ámbito de la instancia, no en el de la subred. Por lo tanto, cada instancia de una subred de la VPC podría tener asignado un conjunto diferente de grupos de seguridad.
- Acuerdos de nivel de servicio (SLAs): parte de los contratos de AMS con usted que definen el nivel de servicio esperado.
- El SLA no está disponible y no está disponible:
  - Una solicitud de API enviada por usted que produce un error.
  - Una solicitud de consola enviada por ti que da como resultado una respuesta HTTP de cinco veces mayor (el servidor no puede ejecutar la solicitud).
  - Cualquiera de las Servicio de AWS ofertas que constituyen pilas o recursos en su infraestructura gestionada por AMS se encuentra en un estado de «interrupción del servicio», como se muestra en el Service Health Dashboard.
  - La falta de disponibilidad que resulte directa o indirectamente de una exclusión de AMS no se tiene en cuenta al determinar la elegibilidad para los créditos de servicio. Los servicios se consideran disponibles a menos que cumplan con los criterios para no estar disponibles.
- Objetivos de nivel de servicio (SLOs): parte de los contratos de AMS con usted que definen objetivos de servicio específicos para los servicios de AMS.

Términos de aplicación de parches:

- Parches obligatorios: actualizaciones de seguridad críticas para abordar problemas que podrían comprometer el estado de seguridad de su entorno o cuenta. Una «actualización de seguridad crítica» es una actualización de seguridad calificada como «crítica» por el proveedor de un sistema operativo compatible con AMS.
- Parches anunciados frente a parches publicados: los parches se anuncian y publican por lo general según un calendario. Los parches emergentes se anuncian cuando se descubre la necesidad de aplicarlos y, por lo general, poco después de su publicación.
- Complemento de parche: parche basado en etiquetas para instancias de AMS que aprovecha la funcionalidad AWS Systems Manager (SSM) para que pueda etiquetar instancias y parchearlas utilizando una línea base y una ventana que usted configure.
- Métodos de parches:
  - Parcheo in situ: parcheo que se realiza cambiando las instancias existentes.
  - Parcheo de reemplazo de la AMI: aplicación de parches que se realiza cambiando el parámetro de referencia de la AMI de una configuración de lanzamiento de grupo de EC2 Auto Scaling existente.
- Proveedor de parches (proveedores de sistemas operativos, terceros): los parches los proporciona el proveedor o el órgano rector de la aplicación.
- Tipos de parches:
  - Actualización de seguridad crítica (CSU): actualización de seguridad calificada como «crítica» por el proveedor de un sistema operativo compatible.
  - Actualización importante (IU): una actualización de seguridad calificada como «importante» o una actualización no relacionada con la seguridad calificada como «crítica» por el proveedor de un sistema operativo compatible.
  - Otra actualización (OU): actualización realizada por el proveedor de un sistema operativo compatible que no es una CSU ni una IU.
- Parches compatibles: AMS admite parches a nivel de sistema operativo. El proveedor publica actualizaciones para corregir vulnerabilidades de seguridad u otros errores o para mejorar el rendimiento. Para obtener una lista de las configuraciones compatibles actualmente OSs, consulte Support Configurations.

Términos de seguridad:

- Controles de Detective: una biblioteca de monitores creados o habilitados por AMS que proporcionan una supervisión continua de los entornos y las cargas de trabajo gestionados por los

clientes para detectar configuraciones que no se ajustan a los controles de seguridad, operativos o del cliente, y toman medidas al notificar a los propietarios, modificar de forma proactiva o cancelar los recursos.

Condiciones de la solicitud de servicio:

- Solicitud de servicio: una solicitud suya para que AMS tome una medida en su nombre.
- Notificación de alerta: aviso que AMS publica en su página de lista de solicitudes de servicio cuando se activa una alerta de AMS. El contacto configurado para su cuenta también recibe una notificación mediante el método configurado (por ejemplo, el correo electrónico). Si tiene etiquetas de contacto en sus instancias o recursos y ha dado su consentimiento a su administrador de prestación de servicios en la nube (CSDM) para las notificaciones basadas en etiquetas, la información de contacto (valor clave) de la etiqueta también se notificará para recibir alertas de AMS automatizadas.
- Notificación de servicio: una notificación de AMS que se publica en la página de la lista de solicitudes de servicios.

Términos varios:

- Interfaz de AWS Managed Services: para AMS: la consola avanzada de AWS Managed Services, la API CM de AMS y la Soporte API. Para AMS Accelerate: la Soporte consola y la Soporte API.
- Satisfacción del cliente (CSAT): El CSAT de AMS se basa en análisis exhaustivos, que incluyen valoraciones de casos por correspondencia en cada caso o correspondencia, cuando se presentan, encuestas trimestrales, etc.
- DevOps: DevOps es una metodología de desarrollo que aboga firmemente por la automatización y la supervisión en todos los pasos. DevOps tiene como objetivo acortar los ciclos de desarrollo, aumentar la frecuencia de despliegue y ofrecer versiones más fiables, ya que reúne las funciones de desarrollo y operaciones, que tradicionalmente estaban separadas, sobre la base de la automatización. Cuando los desarrolladores pueden gestionar las operaciones y las operaciones sirven de base para el desarrollo, los problemas se descubren y resuelven más rápidamente y los objetivos empresariales se alcanzan más fácilmente.
- ITIL: La biblioteca de infraestructura de tecnología de la información (denominada ITIL) es un marco de ITSM diseñado para estandarizar el ciclo de vida de los servicios de TI. ITIL se organiza en cinco etapas que cubren el ciclo de vida de los servicios de TI: estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora del servicio.

- Administración de servicios de TI (ITSM): conjunto de prácticas que alinean los servicios de TI con las necesidades de su empresa.
- Servicios de monitorización gestionados (MMS): AMS opera su propio sistema de monitorización, Managed Monitoring Service (MMS), que consume eventos de AWS salud y agrega datos de CloudWatch Amazon y datos de Servicios de AWS otros, y notifica a los operadores de AMS (en línea las 24 horas del día, los 7 días de la semana) cualquier alarma creada a través de un tema del Amazon Simple Notification Service (Amazon SNS).
- Espacio de nombres: cuando crea políticas de IAM o trabaja con Amazon Resource Names (ARNs), identifica y utiliza un espacio Servicio de AWS de nombres. Los espacios de nombres se utilizan para identificar acciones y recursos.

# Descripción del servicio

AMS Accelerate es un plan operativo del servicio AWS Managed Services para gestionar las operaciones de su AWS infraestructura.

## Características del plan de operaciones de AWS Managed Services (AMS) AMS Accelerate

AMS Accelerate ofrece las siguientes funciones:

- Gestión de incidentes:

  La gestión de incidentes es el proceso que utiliza el servicio AMS para responder a los incidentes denunciados.

  AMS Accelerate detecta y responde de forma proactiva a los incidentes y ayuda a su equipo a resolverlos. Puede ponerse en contacto con los ingenieros de operaciones de AMS Accelerate las 24 horas del día, los 7 días de la semana a AWS través del Support Center, con acuerdos de nivel de servicio (SLA) de tiempo de respuesta en función del nivel de respuesta que haya seleccionado para su cuenta.
- Supervisión:

  La supervisión es el proceso que utiliza el servicio AMS para rastrear sus recursos.

  Las cuentas inscritas en AMS Accelerate se configuran con un despliegue básico de CloudWatch eventos y alarmas de Amazon que se ha optimizado para reducir el ruido e identificar un posible

incidente próximo. Tras recibir las alertas, el equipo de AMS recurre a recursos, personal y procesos automatizados para recuperar el buen estado de los recursos y, cuando es necesario, se pone en contacto con sus equipos para proporcionarles información sobre lo que se aprende sobre este comportamiento y cómo prevenirlo. Si la solución no funciona, AMS inicia el proceso de gestión de incidentes. Puede cambiar las líneas base actualizando el archivo de configuración predeterminado.

- Seguridad:

  La gestión de la seguridad es el proceso que utiliza el servicio AMS para proteger sus recursos. AWS Managed Services protege sus activos de información y ayuda a mantener segura su infraestructura de AWS mediante el uso de varios controles, incluidos AWS Config Rules y Amazon GuardDuty.

  AMS Accelerate mantiene una biblioteca de medidas correctivas Reglas de AWS Config y de medidas correctivas para garantizar que todas sus cuentas cumplan con los estándares del sector en materia de seguridad e integridad operativa. Reglas de AWS Config realiza un seguimiento continuo del cambio de configuración entre sus recursos registrados. Si un cambio infringe alguna de las condiciones de la regla, AMS informa de sus conclusiones y permite subsanar las infracciones de forma automática o previa solicitud, en función de la gravedad de la infracción. Reglas de AWS Config facilitar el cumplimiento de los estándares establecidos por: el Centro de Seguridad de Internet (CIS), el Marco de Seguridad en la Nube (CSF) del Instituto Nacional de Estándares y Tecnología (NIST), la Ley de Portabilidad y Responsabilidad de los Seguros de Salud (HIPAA) y el Estándar de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI).

  Además, AMS Accelerate utiliza Amazon GuardDuty para identificar actividades potencialmente no autorizadas o maliciosas en su entorno de AWS. GuardDuty AMS supervisa los hallazgos las 24 horas del día, los 7 días de la semana. AMS colabora con usted para comprender el impacto de las conclusiones y las medidas correctivas basándose en las recomendaciones de las mejores prácticas. AMS también apoya a Amazon Macie para proteger sus datos confidenciales, como la información de salud personal (PHI), la información de identificación personal (PII) y los datos financieros. Por último, AMS supervisa y clasifica todos los eventos ALERT y BLOCK de Amazon Route 53 Resolver generados en las cuentas gestionadas para inspeccionar más a fondo el tráfico de la red y aumentar sus capacidades de detección.

- Administración de parches:

  La administración de parches es el proceso que utiliza el servicio AMS para actualizar los recursos.

En el caso de una AWS cuenta con el complemento de parche, AWS Managed Services aplica e instala las actualizaciones de los proveedores en las instancias de Amazon EC2 para los sistemas operativos compatibles durante los períodos de mantenimiento que elija. AMS crea una instantánea de la instancia antes de aplicar el parche, supervisa la instalación del parche y le notifica el resultado. Si el parche no funciona, AMS investigará el error y recomendará una línea de acción para solucionar el problema. O bien, AMS restaura la instancia para revertirla, si se solicita. AMS proporciona informes sobre la cobertura de cumplimiento de los parches y le informa sobre las medidas recomendadas para su empresa.

- Administración de Backup:

  AMS utiliza la administración de copias de seguridad para tomar instantáneas de sus recursos.

  AWS Managed Services crea, supervisa y almacena instantáneas de los AWS servicios compatibles AWS Backup con. Para definir los cronogramas, la frecuencia y el período de retención de las copias de seguridad, debe crear AWS Backup planes al incorporar cuentas y aplicaciones. Los planes se asocian a los recursos. AMS rastrea todos los trabajos de respaldo y, cuando un trabajo de respaldo falla, alerta a nuestro equipo para que ejecute una reparación. AMS aprovecha sus instantáneas para realizar acciones de restauración durante los incidentes, si es necesario. AMS le proporciona un informe de cobertura de respaldo y un informe de estado de respaldo.

- Gestión de problemas:

  AMS realiza un análisis de tendencias para identificar e investigar los problemas e identificar la causa raíz. Los problemas se solucionan con una solución alternativa o permanente que evite que se repita un impacto similar en el servicio en el futuro. Se puede solicitar un informe posterior al incidente (PIR) para cualquier incidente «grave», una vez resuelto el problema. El PIR recoge la causa raíz y las medidas preventivas adoptadas, incluida la implementación de medidas preventivas.

- Expertos designados:

  AMS Accelerate también designa a un administrador de prestación de servicios en la nube (CSDM) y a un arquitecto de nube (CA) para que se asocien con su organización e impulsen la excelencia operativa y de seguridad. Su CSDM y su CA le brindan orientación durante y después de la configuración y la incorporación de AMS Accelerate, le entregan un informe mensual con sus métricas operativas y trabajan con usted para identificar posibles ahorros de costos mediante herramientas como AWS Cost Explorer, Cost and Usage Reports y. Trusted Advisor

- Herramientas de operaciones:

  AMS Accelerate puede proporcionar operaciones continuas para la infraestructura de su carga de trabajo en AWS. Nuestros servicios de parches, copias de seguridad, supervisión y administración de incidentes dependen de que los recursos estén etiquetados y que el AWS Systems Manager (SSM) y los CloudWatch agentes estén instalados y configurados en las instancias de Amazon EC2 con un perfil de instancia de IAM que los autorice a interactuar con los servicios de SSM y Amazon. CloudWatch AMS Accelerate proporciona herramientas como Resource Tagger, que le ayuda a etiquetar sus recursos en función de reglas, y una configuración de instancias automatizada para instalar los agentes necesarios en sus instancias de Amazon EC2. Si sigue prácticas de infraestructura inmutable, puede completar los requisitos previos directamente en la consola o en las plantillas de infraestructura como código.

- Optimización de costes:

  AMS Resource Scheduler automatiza el inicio y la parada de las instancias de Amazon Elastic Compute Cloud (Amazon EC2), las instancias de Amazon Relational Database Service (Amazon RDS) y los grupos de Amazon EC2 Auto Scaling. El programador de recursos de AMS le ayuda a reducir los costes operativos al detener los recursos que no se utilizan y volver a ponerlos en marcha cuando se necesita su capacidad.

- Registro e informes:

  AWS Managed Services agrega y almacena los registros generados como resultado de las operaciones en CloudWatch los registros de flujo de Amazon VPC y Amazon VPC. CloudTrail El registro desde AMS ayuda a acelerar la resolución de incidentes y las auditorías del sistema. AMS Accelerate también le proporciona un informe de servicio mensual en el que se resumen las principales métricas de rendimiento de AMS, incluidos un resumen ejecutivo y una visión, las métricas operativas, los recursos gestionados, el cumplimiento del acuerdo de nivel de servicio (SLA) de AMS y las métricas financieras relacionadas con los gastos, el ahorro y la optimización de costes. Los informes los entrega el gerente de prestación de servicios en la nube (CSDM) de AMS que usted designe.

- Gestión de solicitudes de servicio:

  Para solicitar información sobre su entorno gestionado, su AMS o sus ofertas de AWS servicios, envíe las solicitudes de servicio mediante la consola AMS Accelerate. Puede enviar una solicitud de servicio si tiene preguntas prácticas sobre AWS los servicios y las funciones o para solicitar servicios AMS adicionales.

Todos los clientes de AMS Accelerate comienzan con la gestión de incidentes, el monitoreo, el monitoreo de la seguridad, el registro de registros, las herramientas necesarias, la administración de copias de seguridad y las capacidades de generación de informes. Puede añadir el complemento de gestión de parches AMS por un precio adicional.

> **Note**
>
> Para ver una lista de funciones no compatibles AWS GovCloud (US), consulte En qué se diferencia AMS Accelerate de AWS GovCloud (US)

## Configuraciones admitidas

AMS Accelerate admite las siguientes configuraciones:

- Idioma: inglés.
- Regiones: consulte las AWS regiones compatibles con AWS Managed Services en la página web de servicios AWS regionales.

  > **Note**
  >
  > Las regiones de AWS introducidas antes del 20 de marzo de 2019 se consideran regiones «originales» y están habilitadas de forma predeterminada. Las regiones que se introduzcan después de esta fecha son Opt-in «» Regiones y están deshabilitadas de forma predeterminada. Si su cuenta utiliza varias regiones y ha incorporado AMS Accelerate a una cuenta con una «Opt-in» región habilitada como región predeterminada, la función de informes de AMS solo estará disponible en esa región. Si no estableces una región predeterminada, la última región que visitaste será tu región predeterminada. Para habilitar una región, consulte Habilitar una región. Para establecer una región predeterminada, consulte Elegir una región. Para obtener una lista del Opt-in estado de cada región, consulte Regiones disponibles en la Guía del usuario de Amazon Elastic Compute Cloud.

- Arquitectura de sistema operativo (x86-64 o ARM64): cualquiera compatible con Systems Manager y. CloudWatch
- Sistemas operativos compatibles:
  - AlmaLinux 8.3-8.9, 9.x (solo AlmaLinux es compatible con la arquitectura x86)

- Amazon Linux 2023
- Amazon Linux 2 (fecha prevista de finalización del soporte para AMS el 30 de junio de 2026)
- Oracle Linux 9.x, 8.x
- Red Hat Enterprise Linux (RHEL) 9.x, 8.x
- SUSE Linux Enterprise Server 15 SP6
- SUSE Linux Enterprise Server para SAP 15 SP3 y versiones posteriores
- Microsoft Windows Server 2025, 2022, 2019, 2016
- Ubuntu 20.04, 22.04, 24.04

- Sistemas operativos End of Support (EOS) compatibles:

> **Note**
>
> Los sistemas operativos End of Support (EOS) están fuera del período de soporte general del fabricante del sistema operativo y presentan un mayor riesgo de seguridad. Los sistemas operativos EOS se consideran configuraciones compatibles solo si AMS-required los agentes son compatibles con el sistema operativo y se cumplen las siguientes condiciones:
>
> 1. dispone de un amplio soporte con el proveedor del sistema operativo que le permite recibir actualizaciones, o
> 2. cualquier instancia que utilice un sistema operativo EOS sigue los controles de seguridad especificados por AMS en la guía del usuario de Accelerate, o
> 3. usted cumple con cualquier otro control de seguridad compensatorio exigido por AMS.
>
> En caso de que AMS deje de ser compatible con un sistema operativo EOS, AMS emitirá una recomendación fundamental para actualizar el sistema operativo.
> AMS-required los agentes pueden incluir, entre otros: Amazon AWS Systems Manager CloudWatch, el agente Endpoint Security (EPS) y Active Directory (AD) Bridge (solo Linux).

- Ubuntu Linux 18.04
- SUSE Linux Enterprise Server 15 SP3, SP4 y SP5
- Servidor SUSE Linux Enterprise para SAP 15 SP2
- SUSE Linux Enterprise Server 12 SP5
- Servicio SUSE Linux Enterprise para SAP 12 SP5

  - Microsoft Windows Server 2012/2012 R2
  - Red Hat Enterprise Linux (RHEL) :7.x
  - Oracle Linux 7,5-7,9
- Si lo utiliza AWS Control Tower para administrar su entorno de múltiples cuentas, asegúrese de que está ejecutando la última versión de AWS Control Tower para garantizar la compatibilidad con Accelerate. No se admiten los entornos que utilizan AWS Control Tower versiones anteriores a la 2.7 (publicada en abril de 2021). Para obtener información sobre cómo realizar la actualización AWS Control Tower, consulta Cómo actualizar tu zona de aterrizaje.

## Servicios admitidos

AWS Managed Services proporciona servicios de soporte de administración operativa para los siguientes AWS servicios. Cada AWS servicio es distinto y, en consecuencia, el nivel de soporte de gestión operativa de AMS varía en función de la naturaleza y las características del AWS servicio subyacente. Si solicita que los AWS Managed Services presten servicios para cualquier software o servicio que no esté identificado expresamente como compatible en la siguiente lista, todos los servicios gestionados de AWS proporcionados para dichas configuraciones solicitadas por el cliente se tratarán como un «servicio beta» en virtud de las condiciones del servicio.

- Incidentes: todos los servicios AWS
- Solicitud de servicio: Todos los AWS servicios
- Aplicación de parches: Amazon EC2
- Copias de seguridad y restauración: todas ellas Servicios de AWS compatibles con. AWS Backup Para obtener una lista de los servicios compatibles AWS Backup, consulte los recursos AWS Backup compatibles.
- Programador de recursos: instancias de Amazon Elastic Compute Cloud (Amazon EC2), grupos de Amazon Relational Database Service (Amazon RDS) y Amazon EC2 Auto Scaling
- Servicios supervisados para detectar eventos operativos: comprobaciones compatibles y Trusted Advisor, Application Load Balancer, Aurora, Amazon EC2, Elastic Load Balancing, Amazon FSx NetApp para ONTAP, Amazon FSx para Windows File Server, NAT gateway (un servicio de traducción de direcciones de red (NAT)), Amazon Redshift OpenSearch Panel de estado, Amazon Relational Database Service Amazon (Amazon RDS), VPN. Site-to-Site Para obtener más información sobre lo que AMS Accelerate monitorea como parte de un servicio, consulte Alertas del monitoreo de referencia en AMS.

- Servicios supervisados mediante reglas de configuración de seguridad: AWS Account GuardDuty, Macie, Amazon API Gateway, AWS Certificate Manager, AWS Config,, CloudTrail, CloudWatch AWS CodeBuild, Amazon DynamoDB AWS Database Migration Service, Amazon EC2, Amazon, Amazon ElastiCache Elastic Block Store (Amazon EBS), Amazon Elastic File System (Amazon EFS), Amazon Elastic Kubernetes Service (Amazon (EKS), Elastic Load Balancing OpenSearch , Amazon Service, Amazon EMR, ( AWS Key Management Service IAM),, Amazon Redshift AWS Identity and Access Management , Amazon Relational Database Service AWS Lambda, Amazon S3, Amazon AI, Amazon SageMaker AWS Secrets Manager Simple Notification Service AWS Systems Manager, Amazon VPC (grupo de seguridad, volumen, dirección IP elástica, conexión VPN, pasarelas de Internet), Amazon VPC Flow Logs. Para obtener más información, consultaCumplimiento de la configuración en Accelerate y Protección de datos en Accelerate. Puede encontrar información adicional sobre la seguridad de AMS en nuestra Guía de seguridad privada AWS Artifact, a la que puede acceder en la pestaña Informes de AWS Managed Services.

> **Note**
>
> AMS Accelerate para la región de Asia Pacífico (Malasia) no admite la supervisión con Amazon Macie, la supervisión y la gestión de incidentes para Amazon EKS ni la supervisión de los recursos de Amazon FileSystem EFS, Amazon EC2 y NatGateway Amazon EKS Cluster. Tampoco admite la instalación automática del agente SSM.

> **Note**
>
> AMS Accelerate para la región de Oriente Medio (Emiratos Árabes Unidos) admite un conjunto de funciones específicas, tal como se describe en la siguiente tabla. El acceso a la consola de cuentas y a las instancias de AMS en esta región depende exclusivamente de los activadores de las solicitudes de servicio entrantes. Para obtener más información sobre la disponibilidad de Accelerate en la región de Oriente Medio (Emiratos Árabes Unidos), consulte a su administrador de cuentas o al gerente de prestación de servicios AWS en la nube (CSDM).

| Funciones incluidas en el ámbito de AMS Accelerate para la región de Oriente Medio (EAU) | Descripción de la característica |
| --- | --- |
| Administración de incidentes | AMS proporciona asistencia y respuesta a incidentes para ayudar a su equipo a resolver los problemas. Para que AMS lo ayude con la gestión de incidentes, debe enviar una solicitud de servicio. AMS no detecta ni responde de forma proactiva a los incidentes en esta región. |
| Supervisión | Tras recibir tu solicitud de servicio, AMS puede ayudarte a solucionar los problemas relaciona dos con los recursos. AMS utiliza soluciones, personal y procesos automatizados para que sus recursos recuperen un estado saludable . AMS no configura los CloudWatch eventos ni las alarmas de referencia en esta región. Si ya dispone de herramientas de supervisi ón, es posible que disponga de un seguimien to proactivo de sus recursos en función de la evaluación de Cloud Architect (CA) y del CSDM. |
| Seguridad | Tras recibir tu solicitud de servicio, AMS puede ayudarte a solucionar los problemas de seguridad. AMS no implementa controles de seguridad GuardDuty ni supervisa los Reglas de AWS Config hallazgos de seguridad en esta región. Si ya dispone de herramientas de seguridad, es posible que disponga de una supervisión proactiva de la seguridad en función de la evaluación de la CA y el CSDM. |
| Administración de parches | AMS puede aplicar actualizaciones de proveedores a las instancias de Amazon EC2 para los sistemas operativos compatibl |

| Funciones incluidas en el ámbito de AMS Accelerate para la región de Oriente Medio (EAU) | Descripción de la característica |
| --- | --- |
| | es durante los períodos de mantenimiento elegidos y crear instantáneas previas a la aplicación de parches. Para que AMS le ayude con la administración de los parches, debe enviar una solicitud de servicio. Las notificac iones y los informes de los parches de AMS no están disponibles en esta región. |
| Administración de Backup | AMS puede crear y almacenar instantán eas con el Servicios de AWS apoyo de las copias de AWS Backup seguridad y ayudar a remediarlas. Para que AMS le ayude con la gestión de las copias de seguridad, debe enviar una solicitud de servicio. AMS no realiza un seguimiento de los trabajos de copia de seguridad en esta región. |
| Expertos designados | AMS designa a un arquitecto de nube (CA) y a un administrador de prestación de servicios en la nube (CSDM) para que se asocien con las organizaciones de los clientes e impulsen la excelencia operativa y de seguridad. |
| Gestión de solicitudes de servicio | Para solicitar información sobre su entorno gestionado, su AMS o sus Servicio de AWS ofertas, envíe las solicitudes de servicio a través de la consola AMS Accelerate. Puede enviar una solicitud de servicio si tiene preguntas sobre cómo hacerlo Servicios de AWS y sus funciones, o si desea solicitar los servicios de AMS que están disponibles en esta región, tal y como se describe en esta tabla. |

# Funciones y responsabilidades

La matriz responsable, responsable, consultada e informada de AMS Accelerate (RACI) asigna la responsabilidad principal al cliente o a AMS en relación con una variedad de actividades. En la tabla se describen sus responsabilidades (el «Cliente») en comparación con las nuestras («AMS Accelerate»).

Alcance de los cambios realizados por AMS AccelerateEn esta sección se enumeran las circunstancias específicas en las que AMS está autorizada a realizar cambios en su cuenta y algunos tipos de cambios que AMS nunca realiza.

## Matriz RACI de AMS Accelerate

AMS Accelerate administra su infraestructura de AWS. La siguiente tabla proporciona una descripción general de las funciones y responsabilidades que tienen usted y AMS Accelerate en relación con las actividades del ciclo de vida de una aplicación que se ejecuta en el entorno gestionado.

- R significa Parte responsable que hace el trabajo para lograr la tarea.
- C son las siglas de Consultado, una parte cuya opinión se solicita, normalmente como expertos en la materia, y con la que existe comunicación bilateral.
- I son las siglas de Informado, una parte que recibe información sobre el progreso, a menudo solo una vez finalizada la tarea.

> **Note**
>
> Algunas secciones contienen una «R» tanto para AMS como para Clientes. Esto se debe a que, en el modelo de responsabilidad AWS compartida, tanto AMS como los clientes asumen una propiedad conjunta para responder a los problemas de infraestructura y aplicaciones.

| Actividad | Cliente | AWS Managed Services (AMS) |
| --- | --- | --- |
| Patrones de AMS | | |

| Actividad | Cliente | AWS Managed Services (AMS) |
|---|---|---|
| Crea nuevos patrones | I | R |
| Implemente y personalice patrones | R | C, I |
| Pruebe y elimine patrones | R | I |
| Ciclo de vida de la aplicación | | |
| Desarrollo de aplicaciones | R | I |
| Requisitos, análisis y diseño de la infraestructura de aplicaciones | R | I |
| Implementación de aplicaciones | R | I |
| Implementación de recursos de AWS | R | I |
| Supervisión de aplicaciones | R | I |
| Aplicación testing/optimization | R | I |
| Solucionar problemas y resolver problemas de aplicaciones | R | I |
| Solucionar problemas y resolverlos | R | I |
| Monitorización compatible con la infraestructura de AWS | C | R |
| Respuesta a incidentes relacionados con problemas de red de AWS | C | R |
| Respuesta a incidentes por problemas de recursos de AWS | C | R |
| Incorporación de cuentas gestionadas | | |
| Conceda acceso a la cuenta gestionada de AWS al equipo y las herramientas de AMS | R | C |

| Actividad | Cliente | AWS Managed Services (AMS) |
|---|---|---|
| Implemente cambios en la cuenta o el entorno para permitir el despliegue de herramientas en la cuenta. Por ejemplo, cambios en las políticas de control de servicios (SCP) | R | C |
| Instale agentes SSM en instancias EC2 | R | C |
| Instale y configure las herramientas necesarias para proporcionar los servicios de AMS. Por ejemplo, CloudWatch agentes, scripts para aplicar parches, alarmas, registros y otros | I | R |
| Gestione el ciclo de vida del acceso y la identidad para los ingenieros de AMS | I | R |
| Recopile todos los datos necesarios para configurar los servicios de AMS. Por ejemplo, los plazos de mantenimiento de los parches, la duración, el cronograma y los objetivos | R | I |
| Solicite la configuración de los servicios de AMS y proporcione todos los datos necesarios | R | I |
| Configure los servicios AMS según lo solicite el cliente. Por ejemplo, ventanas de mantenimiento de parches, etiquetador de recursos y administrador de alarmas | C | R |
| Gestione el ciclo de vida de los usuarios y sus permisos, para los servicios de directorio local, que se utilizan para acceder a las cuentas e instancias de AWS | R | I |
| Recomiende la optimización de instancias reservadas | I | R |
| Incorpore las cuentas a Trusted Remediator | C, I | R |
| Administración de parches | | |

| Actividad | Cliente | AWS Managed Services (AMS) |
|---|---|---|
| Recopile todos los datos necesarios para configurar las ventanas de mantenimiento de los parches, las bases de referencia y el objetivo | R | I |
| Solicite la configuración de las ventanas y líneas base de mantenimiento de los parches y proporcione todos los datos necesarios | R | I |
| Configure los períodos de mantenimiento de los parches, las bases de referencia y los objetivos de los parches según lo solicite el cliente | C | R |
| Supervise las actualizaciones aplicables al sistema operativo compatibl e y al software preinstalado con el sistema operativo compatible para las instancias EC2 | I | R |
| Informe sobre las actualizaciones faltantes del sistema operativo compatible y la cobertura del período de mantenimiento | I | R |
| Tome instantáneas de las instancias antes de aplicar las actualizaciones | I | R |
| Aplique actualizaciones a las instancias EC2 según la configuración del cliente | I | R |
| Investigue las actualizaciones fallidas de las instancias de EC2 | C | R |
| Actualice las AMI y las pilas para Auto-Scaling grupos (ASG) | R | C |
| Parchee el sistema operativo Windows y los paquetes de Microsoft instalados en el sistema operativo que se rigen por Windows Update | I | R |
| Parchee las aplicaciones instaladas, el software o las dependencias de aplicaciones no administradas por Windows Update | R | I |
| Aplica parches al sistema operativo Linux y a cualquier paquete cuya administración esté habilitada por el administrador de paquetes nativo del sistema operativo (por ejemplo, Yum, Apt o Zypper) | I | R |

| Actividad | Cliente | AWS Managed Services (AMS) |
|---|---|---|
| Parchee las aplicaciones instaladas, el software o las dependencias de aplicaciones que no administre el administrador de paquetes nativo del sistema operativo Linux | R | I |
| Copia de seguridad | | |
| Recopile todos los datos necesarios para configurar los planes de respaldo y los recursos de destino | R | I |
| Solicite la configuración de los planes de Backup y proporcione todos los datos necesarios | R | I |
| Configure los planes y objetivos de respaldo según lo solicite el cliente | C | R |
| Especifique los programas de respaldo y los recursos objetivo | R | I |
| Realice copias de seguridad según el plan | I | R |
| Investigue los trabajos de respaldo fallidos | I | R |
| Informe sobre el estado y la cobertura de los trabajos de respaldo | I | R |
| Valide los respaldos | R | I |
| Solicite la restauración de copias de seguridad de los recursos de los servicios de AWS compatibles como parte de la gestión de incidentes | R | I |
| Realice actividades de restauración de copias de seguridad para los recursos de los servicios de AWS compatibles | I | R |
| Restaure las aplicaciones personalizadas o de terceros afectadas | R | I |
| Redes | | |

| Actividad | Cliente | AWS Managed Services (AMS) |
|---|---|---|
| Aprovisionamiento y configuración de VPC de cuentas administradas, IGW, Direct Connect y otros servicios de red de AWS | R | I |
| Configurar y utilizar la seguridad de AWS Groups/NAT/NACL dentro de la cuenta gestionada | R | I |
| Configuración e implementación de redes dentro de la red del cliente (por ejemplo DirectConnect) | R | I |
| Configuración e implementación de redes dentro de la red de AWS | R | I |
| Supervise la seguridad de la red definida por AMS, incluidos los grupos de seguridad | I | R |
| Network-level configuración y administración de registros (registros de flujo de VPC y otros) | I | R |
| Registro | | |
| Registre todos los registros de cambios de la aplicación | R | I |
| Registre los registros de cambios en la infraestructura de AWS | I | R |
| Habilitar y agregar el registro de auditoría de AWS | I | R |
| Agregue registros de los recursos de AWS | I | R |
| Supervisión y remediación | | |
| Recopile todos los datos necesarios para configurar el administrador de alarmas, el etiquetador de recursos y los umbrales de alarma | R | I |
| Solicite la configuración del administrador de alarmas y proporcione todas las entradas necesarias | R | I |

| Actividad | Cliente | AWS Managed Services (AMS) |
|---|---|---|
| Configure el administrador de alarmas, el etiquetador de recursos y los umbrales de alarma según lo solicite el cliente. | C | R |
| Implemente las métricas y alarmas CloudWatch de referencia de AMS según la configuración del cliente | I | R |
| Supervise los recursos de AWS compatibles mediante CloudWatch métricas y alarmas de referencia | I | R |
| Investigue las alertas de los recursos de AWS | C | R |
| Corrija las alertas en función de la configuración definida o cree un incidente | I | R |
| Defina, supervise e investigue los monitores específicos del cliente | R | I |
| Investigue las alertas del monitoreo de aplicaciones | R | C |
| Configure Trusted Advisor las comprobaciones para su corrección | R | C |
| Corrija automáticamente las comprobaciones compatibles Trusted Advisor | I | R |
| Corrija manualmente las comprobaciones compatibles Trusted Advisor | R | C |
| Informe el estado de la corrección | I | R |
| Solucione los errores de corrección | R | C |
| Arquitectura de seguridad | | |
| Revise los recursos y el código de AMS para detectar problemas de seguridad y posibles amenazas | I | R |

| Actividad | Cliente | AWS Managed Services (AMS) |
|---|---|---|
| Implemente controles de seguridad en los recursos y el código de AMS para mitigar los riesgos de seguridad | I | R |
| Habilite los servicios de AWS compatibles para la administración de la seguridad de la cuenta y sus recursos de AWS | I | R |
| Administre las credenciales privilegiadas para el acceso a la cuenta y al sistema operativo de los ingenieros de AMS | I | R |
| Gestión de riesgos de seguridad | | |
| Supervise los servicios de AWS compatibles para la gestión de la seguridad, como GuardDuty Macie | I | R |
| Defina y cree reglas de AMS-defined configuración para detectar si los recursos de AWS cumplen con las prácticas recomendadas de seguridad del Center for Internet Security (CIS) y el NIST. | I | R |
| Reglas de AMS-defined Config de Monitor | I | R |
| Informar sobre el estado de conformidad de las reglas de Config | I | R |
| Defina una lista de las Config Rules requeridas y corríjalas | I | R |
| Evalúe el impacto de corregir las reglas de AMS-defined Config | R | I |
| Solicitar la corrección de las reglas de AMS-defined Config en la cuenta de AWS | R | I |
| Realice un seguimiento de los recursos exentos de las reglas de AMS-defined Config | R | I |
| Corrija las reglas de AMS-defined configuración compatibles en la cuenta de AWS | C | R |

| Actividad | Cliente | AWS Managed Services (AMS) |
|---|---|---|
| Corrija las reglas de AMS-defined configuración no compatibles en la cuenta de AWS | R | I |
| Defina, supervise e investigue las reglas de configuración específicas del cliente | R | I |
| Gestión de incidentes | | |
| Notificar sobre los incidentes detectados por AMS en los recursos de AWS | I | R |
| Notifique sobre incidentes en AWS los recursos | R | I |
| Notifique los incidentes a los AWS recursos en función de la supervisión | I | R |
| Gestione los problemas y las interrupciones del rendimiento de las aplicaciones | R | I |
| Clasifique la prioridad de los incidentes | I | R |
| Proporcione una respuesta a los incidentes | I | R |
| Proporcione la resolución de incidentes o la restauración de la infraestructura de los recursos con las copias de seguridad disponibles | C | R |
| Respuesta a un incidente de seguridad: prepárese | | |
| Comunicaciones | | |
| Proporcione y actualice los datos de contacto de seguridad del cliente para que AMS los utilice durante los eventos de seguridad, las notificaciones y las escaladas de seguridad | R | I |

| Actividad | Cliente | AWS Managed Services (AMS) |
|---|---|---|
| Guarde y administre los datos de contacto de seguridad del cliente proporcionados para utilizarlos durante los eventos y las escaladas de seguridad | C | R |
| Entrenamiento | | |
| Proporcione al cliente la documentación necesaria para respaldar a AMS durante el proceso de respuesta a incidentes | I | R |
| Practique la responsabilidad compartida durante los procesos de respuesta a incidentes mediante jornadas de juego sobre seguridad | R | R |
| Administración de recursos | | |
| Configure la gestión de seguridad compatible Servicios de AWS para las alertas, la correlación de alertas, la reducción del ruido y otras reglas | I | R |
| Mantenga un inventario completo de AWS los recursos (Amazon EC2, Amazon S3, etc.), que incluya detalles sobre el valor y la importancia de cada activo para la empresa. Esta información será fundamental para determinar una estrategia de contención eficaz | R | C |
| Emplee AWS etiquetas para identificar los recursos y las cargas de trabajo | R | C |
| Defina y configure la retención y el archivado de registros | I | R |
| Establezca una base segura definiendo y aplicando las políticas y configuraciones de seguridad de la organización para la administración de AWS cuentas, servicios y acceso | R | I |
| Respuesta a incidentes de seguridad: detectar | | |
| Registro, indicadores y monitoreo | | |

| Actividad | Cliente | AWS Managed Services (AMS) |
|---|---|---|
| Configure el registro y la supervisión para permitir la administración de eventos, por ejemplo, y las cuentas | I | R |
| El monitor admite Servicios de AWS alertas de seguridad | I | R |
| Implemente y gestione herramientas de seguridad para terminales | R | I |
| Supervise el malware en las instancias mediante la seguridad de los puntos finales | R | I |
| Notifique al cliente los eventos detectados mediante mensajes salientes | I | R |
| Coordine las comunicaciones internas con las partes interesadas y las actualizaciones del liderazgo para mejorar el tiempo de respuesta | R | I |
| Defina, implemente y mantenga los servicios de detección estándar de AMS (por ejemplo, Amazon GuardDuty y AWS Config) | C | R |
| Registre los registros AWS de cambios en la infraestructura | R | I |
| Habilite y configure el registro y la supervisión para permitir la administr ación de eventos para la aplicación | R | C |
| Implemente y mantenga una lista de permitidos, una lista de denegacio nes y detecciones personalizadas en los servicios de AWS seguridad compatibles (por ejemplo, Amazon) GuardDuty | R | R |
| Informes de eventos de seguridad | | |
| Notifique a AMS de una actividad sospechosa o de una investigación de seguridad activa | R | I |
| Notifique al cliente los incidentes y eventos de seguridad detectados | I | R |

| Actividad | Cliente | AWS Managed Services (AMS) |
|---|---|---|
| Notifique el evento planificado que pueda desencadenar el proceso de respuesta a incidentes de seguridad | R | I |
| Respuesta a incidentes de seguridad: analice | | |
| Investigación y análisis | | |
| Realice una respuesta inicial a una alerta de seguridad compatible generada por una fuente de detección compatible | I | R |
| Evalúe false/true los aspectos positivos con los datos disponibles | R | R |
| Genere una instantánea de las instancias afectadas para compartirla con el cliente si es necesario | I | R |
| Realice tareas forenses, como la cadena de custodia, el análisis del sistema de archivos, el análisis forense de la memoria y el análisis binario | R | C |
| Recopile los registros de las aplicaciones para facilitar la investigación | R | I |
| Recopile datos y registros para ayudar a investigar las alertas de seguridad | R | R |
| Involucre a las pymes Servicios de AWS en las investigaciones de seguridad | C | R |
| Comparta los registros de investigación del equipo Servicios de AWS de soporte con los clientes durante una investigación | I | R |
| ¿Comunicación | | |
| Envíe alertas y notificaciones desde las fuentes de detección de AMS para los recursos gestionados | I | R |

| Actividad | Cliente | AWS Managed Services (AMS) |
|---|---|---|
| Gestione las alertas y las notificaciones de los eventos de seguridad de las aplicaciones | R | I |
| Comuníquese con el punto de contacto de seguridad del cliente durante la investigación de un incidente de seguridad | R | I |
| Respuesta a un incidente de seguridad: contiene | | |
| Estrategia y ejecución de la contención | | |
| Evalúe los riesgos y decida la estrategia de contención, reconociendo los posibles impactos en el servicio | R | C |
| Haga una copia de seguridad de los sistemas afectados para analizarlos más a fondo | I | R |
| Contenga las aplicaciones y las cargas de trabajo (mediante la configuración específica de la aplicación o la actividad de respuesta) | R | C |
| Defina la estrategia de contención en función del incidente de seguridad y del recurso afectado | I | R |
| Habilite el cifrado y el almacenamiento seguro de las copias de seguridad puntuales de los sistemas afectados | C | R |
| Ejecute las acciones de contención compatibles para AWS los recursos, incluidas las instancias EC2, la red y la IAM | I | R |
| Respuesta a incidentes de seguridad: erradicar | | |
| Estrategia y ejecución de la erradicación | | |
| Defina las opciones de erradicación en función del incidente de seguridad y del recurso afectado en función de las cargas de trabajo de las aplicaciones de los clientes | C | R |

| Actividad | Cliente | AWS Managed Services (AMS) |
|---|---|---|
| Decida la estrategia de erradicación acordada, el calendario de ejecución de la erradicación y las consecuencias | R | I |
| Defina las medidas de erradicación en función del incidente de seguridad y del recurso afectado en las cargas de trabajo gestionadas por AMS | C | R |
| Erradique las amenazas y refuerce AWS los recursos, incluidas las instancias de EC2, la red y la erradicación de la IAM | R | C |
| Erradique las amenazas y refuerce las aplicaciones y las cargas de trabajo (mediante una configuración específica de la aplicación o una actividad de respuesta) | R | I |
| Respuesta a incidentes de seguridad: recuperación | | |
| Preparación y ejecución de la recuperación | | |
| Configure los planes y objetivos de respaldo según lo solicite el cliente | I | R |
| Revise los planes de respaldo para restaurar las cargas de trabajo gestionadas por AMS | R | I |
| Realice actividades de restauración de copias de seguridad para obtener los recursos compatibles Servicios de AWS | I | R |
| Respalde las aplicaciones del cliente, la configuración de las aplicacio nes y los ajustes de implementación, y revise los planes de respaldo para restaurar las aplicaciones y cargas de trabajo del cliente después de un incidente | R | I |
| Restaure las aplicaciones y las cargas de trabajo de los clientes (mediante pasos de restauración específicos de la aplicación) | R | I |
| Respuesta a un incidente de seguridad: informe posterior al incidente | | |

| Actividad | Cliente | AWS Managed Services (AMS) |
|---|---|---|
| Informes posteriores al incidente | | |
| Comparta las lecciones aprendidas y las medidas de acción apropiadas con el cliente después del incidente, según sea necesario | I | R |
| Gestión de problemas | | |
| Correlaciona los incidentes para identificar los problemas | I | R |
| Realice un análisis de la causa raíz (RCA) de los problemas | I | R |
| Solucione los problemas | I | R |
| Identifique y solucione los problemas de las aplicaciones | R | I |
| Administración de servicios | | |
| Solicite información mediante solicitudes de servicio | R | I |
| Responder a las solicitudes de servicio | I | R |
| Proporcione recomendaciones de optimización de costos | I | R |
| Prepare y entregue un informe de servicio mensual | I | R |
| Gestión de cambios | | |
| Procesos y herramientas de gestión de cambios para el aprovisio namiento y la actualización de los recursos en el entorno gestionado | R | I |
| Mantenimiento del calendario de cambios de aplicaciones | R | I |
| Aviso de próxima ventana de mantenimiento | R | I |
| Registre los cambios realizados por AMS Operations | I | R |

| Actividad | Cliente | AWS Managed Services (AMS) |
|---|---|---|
| Optimización de costos | | |
| Recopile todas las entradas necesarias para configurar el Programador de recursos | R | I |
| Solicite la incorporación y la configuración del Programador de recursos y proporcione todos los datos necesarios | R | I |
| Implemente el programador de recursos según la configuración del cliente | C, I | R |
| Desactive y active el programador de recursos en la cuenta del cliente | R | C |
| Cree, elimine, describa y actualice los horarios | C | R |
| Cree, elimine, describa y actualice períodos | C | R |
| Investigue y solucione problemas con Resource Scheduler | I | R |
| Solicitud de desconexión del programador de recursos | R | I |
| Desconecte el programador de recursos de la cuenta | C, I | R |

## Alcance de los cambios realizados por AMS Accelerate

AMS Accelerate solo realiza cambios para los fines y situaciones específicos que se describen a continuación. AMS solo realiza cambios a nivel de infraestructura, mediante la consola o las API. AMS nunca cambia las capas de aplicaciones, control o dominio. Puede ver cualquier cambio realizado por AMS (u otros usuarios) mediante nuestro conjunto de consultas prediseñadas; para ello, consulteSeguimiento de los cambios en sus cuentas de AMS Accelerate.

AWS resources

AMS Accelerate despliega o actualiza AWS los recursos solo en las siguientes situaciones:

- Para implementar y actualizar las herramientas y los recursos que necesita AMS.
- Como parte de la supervisión de AMS, en respuesta a eventos y alarmas.
- Para solucionar los problemas de seguridad como parte de ello Respuestas a las infracciones en Accelerate (hacer que los recursos que no cumplan con las normas se ajusten a las mejores prácticas de seguridad).
- Durante la reparación y la restauración como parte de una respuesta a un incidente.
- Al responder a las solicitudes de los clientes para configurar las funciones de AMS, como las siguientes:
  - Gestor de alarmas
  - Etiquetador de recursos
  - Parchee las líneas base y las ventanas de mantenimiento
  - Programador de recursos
  - Planes de copia de seguridad

AMS Accelerate no despliega ni actualiza los recursos fuera de estas situaciones. Si necesita la ayuda de AMS para realizar cambios en otras situaciones, considere la posibilidad de utilizar Operations on Demand.

Software del sistema operativo

AMS Accelerate puede realizar cambios en el software de su sistema operativo en caso de no disponibilidad mediante la resolución de incidentes, tal como se define en nuestro acuerdo de nivel de servicio. AMS también puede realizar cambios en sus sistemas operativos como parte deConfiguración automatizada de instancias en AMS Accelerate.

Código y configuración de la aplicación

AMS Accelerate nunca modifica el código (por ejemplo, las CloudFormation plantillas de AWS, otras plantillas de infraestructura como código o funciones de Lambda), pero puede guiar a sus equipos sobre los cambios necesarios para seguir las mejores prácticas operativas y de seguridad. AMS Accelerate proporciona asistencia para la resolución de problemas de infraestructura que afectan a las aplicaciones, pero AMS Accelerate no accede a las configuraciones de las aplicaciones ni las valida.

# Capacidades para sistemas operativos no compatibles en Accelerate

Un sistema operativo no compatible es cualquier sistema operativo que no figure en la lista. Configuraciones admitidas AMS considera que las instancias con sistemas operativos no compatibles son «configuraciones solicitadas por el cliente» y están sujetas a las condiciones del servicio Betas y AWS Previews.

El siguiente conjunto limitado de capacidades de AMS está disponible para instancias con sistemas operativos no compatibles:

| Capability | Notas |
| --- | --- |
| Administración de incidentes | AMS proporciona respuesta a incidentes. |
| Gestión de solicitudes de servicio | AMS responde a las solicitudes de servicio. |
| Monitoreo | AMS supervisa y responde a las comprobaciones de estado EC2 del sistema Amazon y a las comprobaciones de estado de las instancias. Las comprobaciones de estado del sistema incluyen: pérdida de conectividad de red, pérdida de alimentación del sistema, problemas de software en el host físico y problemas de hardware en el host físico que afectan a la accesibilidad de la red.<br><br>Las comprobaciones del estado de las instancias incluyen: una configuración de red o inicio incorrecta, memoria agotada, sistema de archivos dañado y núcleo incompatible. |
| Administración de la seguridad | AMS supervisa y responde a las EC2 GuardDuty conclusiones y AWS Config normas de Amazon. |
| Administración de copias de seguridad | AMS proporciona una gestión de la continuidad en Accelerate para EC2 utilizar AWS Backup planes y bóvedas personalizados por AMS. |

# Contacto y escalación

Cuenta con un administrador de prestación de servicios en la nube (CSDM) designado que proporciona asesoramiento en todo AMS Accelerate y tiene un conocimiento detallado de su caso de uso y de la arquitectura tecnológica para el entorno gestionado. CSDMs colabore con los administradores de cuentas, los administradores técnicos de cuentas, los arquitectos de nube de AWS Managed Services (CAs) y los arquitectos de soluciones de AWS (SAs), según proceda, para ayudar a lanzar nuevos proyectos y ofrecer recomendaciones de mejores prácticas a lo largo de los procesos de desarrollo y operaciones del software. El CSDM es el principal punto de contacto de AMS. Las principales responsabilidades de su CSDM son:

- Organice y dirija reuniones mensuales de revisión del servicio con los clientes.
- Proporcione detalles sobre la seguridad, las actualizaciones de software para el entorno y las oportunidades de optimización.
- Defienda sus requisitos, incluidas las solicitudes de funciones para AMS Accelerate.
- Responda y resuelva las solicitudes de informes de facturación y servicio.
- Proporcione información para recomendaciones de optimización financiera y de capacidad.

## Horarios de contacto

Puede ponerse en contacto con AMS Accelerate por diferentes motivos y en diferentes momentos.

| Característica | AMS Accelerate |
|---|---|
| | Nivel premium |
| Solicitud de servicio | 24/7 |
| Gestión de incidentes (P2-P3) | 24/7 |
| Copia de seguridad y recuperación | 24/7 |
| Administración de parches | 24/7 |
| Monitorización y alertas | 24/7 |

| Característica | AMS Accelerate |
| --- | --- |
| | Nivel premium |
| Gestor de prestación de servicios en la nube (CSDM) | De lunes a viernes: de 08:00 a 17:00, horario comercial local |

## Horario comercial

| Característica | AMS Accelerate |
| --- | --- |
| | Nivel premium |
| Solicitud de servicio | 24/7 |
| Gestión de incidentes (P1) | 24/7 |
| Gestión de incidentes (P2-P3) | 24/7 |
| Copia de seguridad y recuperación | 24/7 |
| Administración de parches | 24/7 |
| Monitorización y alertas | 24/7 |
| Gestor de prestación de servicios en la nube (CSDM) | De lunes a viernes: de 09:00 a 17:00, horario comercial local |

## Ruta de escalación

AMS apoya a los clientes con la gestión de incidentes y solicitudes de servicio, las 24 horas del día, los 7 días de la semana y los 365 días del año, de conformidad con el acuerdo de nivel de servicio de AMS que se aplica a la cuenta.

Para informar de un problema de rendimiento de los servicios de AWS o AMS que afecte a su entorno gestionado, utilice la consola de AMS y envíe un caso de incidente. Para obtener más información, consulte Enviar un incidente a Accelerate. Para obtener información general sobre la gestión de incidentes de AMS, consulteGestión de incidentes en AMS Accelerate.

Para solicitar información o consejos, o para solicitar servicios adicionales a AMS, utilice la consola AMS y envíe una solicitud de servicio. Para obtener más información, consulte Crear una solicitud de servicio en Accelerate. Para obtener información general sobre las solicitudes de servicio de AMS, consulteGestión de solicitudes de servicio en Accelerate.

## Inventario de recursos para Accelerate

Todos los recursos que AMS Accelerate despliega en sus Cuenta de AWS cuentas se enumeran en el `resource_inventory.zip`archivo (hoja de cálculo de Excel).

> **Note**
>
> En la columna Nombre del recurso, el prefijo CFN: indica un identificador CloudFormation lógico en lugar de un nombre de recurso. Se muestran para los recursos sin nombre, por ejemplo, para las políticas de bucket de S3.

AMS implementa un conjunto de servicios tal y como se describe en la. Descripción del servicio El costo de implementarlos es bajo cuando se implementan en una cuenta vacía, pero el costo aumenta a medida que aumenta la utilización. Por ejemplo, se crean registros y se invocan las reglas de configuración a medida que cambian los recursos.

Cuando se realizan varios cambios en las reglas de configuración, se pueden activar varias invocaciones de conformidad con la configuración, lo que se traduce en costes más altos. La misma posibilidad se aplica a Amazon que CloudWatch se usa para monitorear instancias: cuanto más granular sea su monitoreo, mayor será el costo del servicio. AWS Backup es otro ejemplo. Si tiene varias copias de seguridad almacenadas o si tiene períodos de retención más largos, está utilizando más espacio de almacenamiento y el costo es mayor.

Estas cifras son difíciles de predecir. Durante su revisión empresarial mensual con su gerente de prestación de servicios en la nube (CSDM), lleve un registro de los cambios y trabaje para identificar las áreas de oportunidad para reducir los costos.

### Controles de infraestructura

AMS Accelerate despliega recursos que pueden estar marcados como errores de configuración en algunos controles. Sin embargo, estas configuraciones son compensaciones intencionadas por la optimización de costos o están cubiertas por controles compensatorios. AMS recomienda utilizar la

información de esta documentación para activar el control o marcar una excepción. AWS Security Hub

Temas


- Controles de autorremediación del Security Hub en Accelerate
- Otros controles de Security Hub en Accelerate


## Controles de autorremediación del Security Hub en Accelerate

Los siguientes controles de autorremediación están disponibles en Accelerate.

Temas


- S3.7 - Los depósitos de uso general de S3 deben utilizar la replicación entre regiones
- S3.11: los buckets de uso general de S3 deben tener habilitadas las notificaciones de eventos
- S3.13 - Los depósitos S3 de uso general deben tener configuraciones de ciclo de vida
- S3.15 - Los cubos S3 de uso general deberían tener activado Object Lock
- Config.1: AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos


S3.7 - Los depósitos de uso general de S3 deben utilizar la replicación entre regiones

Recursos:

- <account_id>arn:aws:s3: ::ams-a -alarm manager- <region>
- <account_id>arn:aws:s3: ::ams-a - - patch-data-reporting <region>
- <region>arn:aws:s3: ::ams-a <account_id>- - patch-data-reporting -audit
- arn:aws:s3::: - ams-config-recorder-bucket <account_id>
- <account_id>arn:aws:s3::: - -auditoría ams-config-recorder-bucket

Los buckets S3 que utilizan los componentes de la infraestructura de AMS no permiten la replicación entre regiones para optimizar los costes. Al habilitar la replicación entre regiones, se incurre en gastos de transferencia de datos para la replicación de datos entre regiones, además de costos de almacenamiento adicionales en la región de destino. En el caso de los segmentos que admiten las operaciones internas de AMS y no requieren redundancia geográfica de forma predeterminada, la

replicación entre regiones añadiría costos continuos significativos sin proporcionar los beneficios necesarios.

Dado que estos depósitos almacenan datos operativos, como la gestión de alarmas, los informes de parches y el registro de la configuración, en una sola región, no es necesaria la replicación entre regiones para las operaciones normales de AMS. Sin embargo, AMS ofrece la capacidad de permitir la replicación entre regiones en estos depósitos en función de sus requisitos específicos de recuperación ante desastres o de conformidad. Póngase en contacto con AMS si necesita ayuda para configurar la replicación entre regiones para su caso de uso.

S3.11: los buckets de uso general de S3 deben tener habilitadas las notificaciones de eventos

Recursos:

- <account_id>arn:aws:s3: ::ams-a -alarm manager- <region>
- <account_id>arn:aws:s3: ::ams-a - - patch-data-reporting <region>
- <region>arn:aws:s3: ::ams-a <account_id>- - patch-data-reporting -audit
- arn:aws:s3::: - ams-config-recorder-bucket <account_id>
- <account_id>arn:aws:s3::: - -auditoría ams-config-recorder-bucket

Los buckets S3 que utilizan los componentes de la infraestructura de AMS no tienen habilitadas las notificaciones de eventos para optimizar los costes. La activación de las notificaciones de eventos de S3 conlleva cargos por el mecanismo de entrega de notificaciones (como Amazon Simple Notification Service, SQS o AWS Lambda las invocaciones), que pueden acumularse en función del volumen de operaciones de S3. Consulte los precios de Amazon SNS para obtener más información.

Dado que estos paquetes son compatibles con las operaciones internas de AMS y, de forma predeterminada, no requieren flujos de trabajo basados en eventos, no habilitamos las notificaciones de eventos para evitar costes innecesarios. Sin embargo, AMS ofrece la posibilidad de activar las notificaciones de eventos en estos grupos en función de sus requisitos específicos de supervisión o automatización. Póngase en contacto con AMS si necesita ayuda para configurar las notificaciones de eventos para su caso de uso.

S3.13 - Los depósitos S3 de uso general deben tener configuraciones de ciclo de vida

Recursos:

- arn:aws:s3::: - ams-config-recorder-bucket <account_id>
- <account_id>arn:aws:s3::: - -auditoría ams-config-recorder-bucket

Históricamente, el componente al que pertenecen estos recursos de S3 no incluía estas configuraciones por motivos de rentabilidad. Sin embargo, AMS ofrece la posibilidad de corregir este control mediante su configuración. Póngase en contacto con AMS si necesita ayuda para hacerlo.

S3.15 - Los cubos S3 de uso general deberían tener activado Object Lock

Recursos:

- <account_id>arn:aws:s3: ::ams-a -administrador de alarmas- <region>

Los cubos S3 que utiliza el sistema AMS Alarm Manager no tienen activado Object Lock por motivos de rentabilidad. La activación de Object Lock puede aumentar los costes (se requieren llamadas adicionales a la API, lo que se traduce en un aumento de CloudTrail los datos) y la complejidad operativa, especialmente en el caso de los buckets que requieren actualizaciones o eliminaciones frecuentes de objetos como parte de su funcionamiento normal. Sin embargo, puede activar Object Lock manualmente en estos depósitos si sus requisitos de cumplimiento o retención de datos requieren esta función. Póngase en contacto con AMS si necesita ayuda con esta configuración.

Recursos:

- <account_id>arn:aws:s3: ::ams-a - - patch-data-reporting <region>
- <region>arn:aws:s3: ::ams-a <account_id>- - patch-data-reporting -audit

El bloqueo de objetos no se puede activar en los buckets y debido a limitaciones del servicio. `ams-a<AccountID>-patch-data-reporting-<Region>` `ams-a<AccountID>-patch-data-reporting-<Region>-audit` AWS El patch-data-reporting depósito recibe datos del inventario de Systems Manager a través de SSM Resource Data Sync, que no es compatible con S3 Object Lock. El depósito de auditoría sirve como destino de los registros de acceso al servidor S3, que no puede tener activado Object Lock. Para obtener más información, consulte Crear una sincronización de datos de recursos para el inventario en la Guía del AWS Systems Manager usuario. Estas restricciones AWS de servicio hacen que Object Lock sea técnicamente imposible y, al mismo tiempo, mantenga la funcionalidad requerida.

Config.1: AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos

Recursos:

- Config Recorder

Durante la incorporación, AMS se despliega AWS Config con la función vinculada al servicio de forma predeterminada. `AWSServiceRoleForConfig` Sin embargo, este control puede fallar si ha proporcionado AWS Identity and Access Management funciones personalizadas AWS Config en lugar de utilizar la función vinculada al servicio para reducir los costes. Si bien las funciones personalizadas pueden funcionar, requieren una gestión manual de las políticas y es posible que no reciban actualizaciones automáticamente cuando se AWS Config añada compatibilidad con nuevos tipos de recursos o funciones.

Puede corregir este problema por sí mismo actualizando la AWS Config grabadora para que utilice la función vinculada al servicio. `AWSServiceRoleForConfig` Esta es la configuración recomendada y se ajusta a las prácticas recomendadas. AWS Para obtener instrucciones detalladas sobre la AWS Config infraestructura implementada por AMS, consulte Supervisión de la seguridad de la infraestructura.

## Otros controles de Security Hub en Accelerate

Los siguientes controles de compensación están disponibles en Accelerate.

Temas

- Lambda.3 - Las funciones de Lambda deben estar en una VPC
- S3.17 - Los depósitos de uso general de S3 deberían cifrarse en reposo con AWS KMS keys
- KMS.2: Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS
- S3.9 - Los depósitos de uso general de S3 deberían tener habilitado el registro de acceso al servidor
- EC2.6: el registro de flujo de VPC debe estar habilitado en todos VPCs

### Lambda.3 - Las funciones de Lambda deben estar en una VPC

Recursos:

- AMSAlarmManagerDeploymentHandler
- AMSAlarmManagerOrphanedAlarmCleanup
- AMSAlarmManagerRemediation
- AMSAlarmManagerReporting
- AMSAlarmManagerTriggerEvaluation

- AMSAlarmManagerValidation
- AMSConfigExtensionDeploymentHandler
- AMSConfigFSXExtension
- AMSConfigOutpostExtension
- AMSConfigSyntheticCanaryExtension

Las AWS Lambda funciones implementadas por AMS no se comunican con los recursos de sus cuentas. Por lo tanto, no requieren la colocación de interfaces de red elásticas (ENIs) dedicadas ni de VPC. La implementación de estas funciones fuera de una VPC reduce los costos y mejora la velocidad de implementación. Este enfoque no plantea ningún problema de seguridad en la comunicación dentro de los recursos. Dado que estas funciones de Lambda funcionan de forma independiente y no acceden a los recursos basados en la VPC, la implementación de la VPC añade complejidad y gastos innecesarios sin proporcionar beneficios de seguridad adicionales.

S3.17 - Los depósitos de uso general de S3 deberían cifrarse en reposo con AWS KMS keys

Recursos:

- <account_id>arn:aws:s3: ::ams-a -administrador de alarmas- <region>

Los depósitos de Amazon Simple Storage Service que utiliza el sistema AMS Alarm Manager utilizan claves de cifrado gestionadas por Amazon (SSE-S3) en lugar de claves KMS gestionadas por el cliente (SSE-KMS). La implementación de claves administradas por el cliente requiere que concedas a AMS permisos explícitos para usar tus claves de KMS mediante políticas clave. Esto introduce una complejidad y un riesgo operativos adicionales. El uso de este control proporciona un cifrado sólido en reposo y, al mismo tiempo, evita costes adicionales y complejidad operativa para usted.

Si modifica las políticas de claves, rota las claves de forma incorrecta o las elimina o desactiva accidentalmente, la supervisión de AMS fallará inmediatamente. Esta dependencia de la disponibilidad de las claves gestionada por el cliente pone en peligro la infraestructura crítica de monitoreo y alerta de AMS. Podría interrumpir las capacidades de monitoreo en tiempo real, la emisión de alertas, la respuesta a incidentes y la visibilidad del estado de los servicios. Las claves de cifrado gestionadas por Amazon cifran automáticamente los datos en reposo sin necesidad de gestionar las políticas de claves, los programas de rotación o los permisos de acceso. Esta implementación cumple con los requisitos de cifrado y, al mismo tiempo, mantiene la rentabilidad y la simplicidad operativa de la infraestructura gestionada AMS.

Recursos:

- <account_id><region>arn:aws:s3: ::ams-a -cloudtrail-log- -audit

El depósito de registro de AWS CloudTrail auditoría no puede utilizar el cifrado debido a las limitaciones del servicio AWS KMS . AWS Los buckets S3 que sirven como destinos de registro de acceso al servidor no deben tener activado el cifrado de claves KMS. Para obtener más información, consulte Configuración del cifrado predeterminado y Solución de problemas del registro de acceso al servidor en la Guía del usuario de Amazon Simple Storage Service. Si se habilita el AWS KMS cifrado en los depósitos de destino de registro, se pueden producir errores de registro y problemas operativos. En su lugar, este bucket utiliza el cifrado gestionado por Amazon S3 (SSE-S3). Esto proporciona el cifrado en reposo y, al mismo tiempo, mantiene la compatibilidad con la funcionalidad de registro de acceso al servidor S3.

KMS.2: Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS

Recursos:

- Clave KMS: alias/ams/patchreporting

La política en línea contiene la palabra «Recurso»: ["*"] en una política de claves de KMS, que es una política basada en recursos adjunta a una clave de KMS específica (ams_ssm_inventory_bucket_kms_key). El ámbito de las políticas clave se basa intrínsecamente en la clave individual, y el uso de un asterisco (*) en el elemento Recurso es una práctica habitual, ya que el ámbito de aplicación de la política ya está limitado por la propia clave. AWS Para obtener más información, consulte Creación de una política clave y una política clave predeterminada en la AWS KMS keys Guía para desarrolladores. Esta configuración no supone ningún riesgo para la seguridad, ya que el acceso está limitado a una única clave de KMS, no a todas las claves de la cuenta.

S3.9 - Los depósitos de uso general de S3 deberían tener habilitado el registro de acceso al servidor

Recursos:

- ams-config-recorder-bucket<account_id>- -auditoría

Estos depósitos S3 son depósitos de destino de registro de acceso para AWS Config los depósitos de Recorder. S3 recomienda no configurar el registro de acceso en estos depósitos, ya que

generaría bucles de registro infinitos, lo que aumentaría los costes de forma innecesaria. AWS Security Hub recomienda, en cambio, que en este escenario se supriman las conclusiones de los recursos.

Corrección:

Deberías suprimir este hallazgo para los grupos afectados, ya que los resultados no son útiles. Si no quieres suprimir los hallazgos, puedes configurar de forma opcional el registro automático en el depósito. El registro automático conlleva el riesgo de que el registro se elimine si AMS actualiza el depósito.

EC2.6: el registro de flujo de VPC debe estar habilitado en todos VPCs

Recursos:

- VPC predeterminada al crear la cuenta

De forma predeterminada, AMS no habilita los registros de flujo de VPC para la VPC predeterminada.

Corrección:

Puedes corregir el control automáticamente añadiendo la clave/valor de la `ams:managed=true` etiqueta, borrando el estado de la regla de configuración y volviendo a ejecutar la evaluación de la regla. El componente de corrección automática de AMS habilita los registros de flujo de la VPC en la VPC.

# Cómo empezar con AMS Accelerate

Si todavía no tiene una cuenta de AWS Managed Services (AMS), comience por ponerse en contacto con un representante de ventas de Amazon Web Services (AWS) a través de nuestra página AWS Managed Services: póngase en contacto con ventas.

Tras suscribirse a un AMS, el equipo de AMS Accelerate le guiará a través del siguiente proceso de incorporación para cada uno de sus Cuentas de AWS miembros.

Consulte el conjunto de funciones aquí: Características de AWS Managed Services

> **Note**
>
> AMS Accelerate es compatible con GovCloud las regiones. Si su servicio residirá en un AWS GovCloud (US) Region, consulte también Cómo empezar con AWS GovCloud (US).

## Proceso de incorporación de cuentas para Accelerate

La incorporación de una cuenta a AMS Accelerate consta de cuatro etapas.

1. Paso 1. Descubrimiento de cuentas en Accelerateevalúa el estado actual de su cuenta e identifica los obstáculos técnicos a la hora de incorporarla.
2. Paso 2. Incorporación de recursos de gestión en Acceleratele pide que acepte los términos y condiciones y que cree un puesto de incorporación para los arquitectos de nube de AMS Accelerate (CAs), quienes lo ayudarán a establecer una base de seguridad y a resolver los problemas según sea necesario.
3. Paso 3. Incorporación de funciones de AMS con políticas predeterminadaspara las funciones de Accelerate, como la supervisión, la aplicación de parches y las copias de seguridad.
4. Paso 4. Personalice las funciones de Acceleregarantiza que los recursos, incluidas EC2 las instancias, estén configurados correctamente para su aplicación.

### Acelere los requisitos previos de incorporación

Antes de iniciar el proceso de incorporación, es importante comprender las dependencias técnicas en las que se basan los componentes de Accelerate.

> **Note**
>
> Para utilizar AMS Accelerate, debe tener uno de los dos Soporte planes compatibles: Enterprise On-Ramp o Enterprise. Los planes Developer y Business no cumplen los requisitos para optar a AMS Accelerate. Para obtener más información sobre los diferentes planes, consulte Comparar Soporte planes.

## AMS Accelerate VPC: puntos finales

Un punto de enlace de VPC permite conexiones privadas entre su VPC y los servicios compatibles AWS y los servicios de punto final de VPC con tecnología. AWS Si necesita filtrar la conectividad a Internet saliente, configure los siguientes puntos de enlace del servicio de VPC para garantizar que AMS Accelerate tenga conectividad con sus dependencias de servicio.

> **Note**
>
> En la siguiente lista, *region* representa el identificador de una AWS región, por `us-east-2` ejemplo, de la región EE.UU. Este (Ohio).

```
com.amazonaws.region.logs
com.amazonaws.region.monitoring
com.amazonaws.region.ec2
com.amazonaws.region.ec2messages
com.amazonaws.region.ssm
com.amazonaws.region.ssmmessages
com.amazonaws.region.s3
com.amazonaws.region.events
```

Para obtener información sobre cómo configurar los puntos de enlace de VPC de AWS, consulte Puntos de enlace de VPC.

> **Note**
>
> Si va a crear puntos de enlace de VPC en su cuenta para todos los servicios mencionados anteriormente, consulte esta plantilla de ejemplo. CloudFormation Puede actualizar esta plantilla y eliminar o añadir la definición de puntos finales de VPC según su caso de uso.

## Conectividad a Internet saliente en Accelerate

1. Descargue egressMgmt.zip.
2. Abra el archivo **ams-egress.json**.
3. Busque lo siguiente URLs en las propiedades de JSON:
   - `WindowsPatching`
   - `RedHatPatching`
   - `AmazonLinuxPatching`
   - `EPELRepository`
4. Permita el acceso a estas URLs.

## Probando la conectividad saliente en Accelerate

Pruebe la conectividad saliente mediante uno de los siguientes métodos.

> **Note**
>
> Antes de ejecutar el script o el comando, sustituya el rojo *`region`* por el identificador de su región, por ejemplo. `us-east-1`

### Guión de Windows PowerShell

```
$region = 'region'
@('logs', 'monitoring', 'ec2', 'ec2messages', 'ssm', 'ssmmessages', 's3', 'events') |
    ForEach-Object {
        Test-NetConnection ("$_.$region.amazonaws.com") -Port 443
    } |
    Format-Table ComputerName, RemotePort, RemoteAddress, PingSucceeded,
 TcpTestSucceeded -AutoSize
```

### Comando de Linux

```
region='region'
for endpoint in logs monitoring ec2 ec2messages ssm ssmmessages s3 events; do
    nc -zv "$endpoint.$region.amazonaws.com" 443
done
```

### Amazon EC2 Systems Manager en Accelerate

Debe instalar el AWS Systems Manager agente (agente SSM) en todas las instancias de EC2 que desee que administre AMS. También debe añadir los permisos de bucket que requiere el agente SSM. Para obtener una descripción general que incluye Amazon EC2, consulte. Paso 3. Incorporación de funciones de AMS con políticas predeterminadas

### IAM en Accelerate

Para que los usuarios puedan leer y configurar las funciones de AMS Accelerate, como acceder a la consola AMS o configurar las copias de seguridad, debe conceder permisos explícitos en AWS Identity and Access Management (IAM) para realizar esas acciones. Para ver, por ejemplo, las políticas de IAM, consulte Permisos para usar las funciones de AMS.

## Paso 1. Descubrimiento de cuentas en Accelerate

AMS trabaja con usted durante el proceso de detección de la cuenta para evaluar su estado actual e identificar los obstáculos técnicos que impiden la incorporación de la cuenta. AMS no proporciona servicios operativos durante la fase de descubrimiento de la cuenta. AMS utiliza la función `AWSServiceRoleForSupport` vinculada al servicio para identificar los obstáculos técnicos y, después, trabaja con usted para solucionarlos antes de pasar a la fase de incorporación a nivel de cuenta.

### Proceso de descubrimiento de cuentas en Accelerate

Para ayudarlo a analizar y descubrir su cuenta, AMS realiza comprobaciones operativas para identificar los bloqueadores técnicos mediante llamadas a la API de solo lectura. Una vez que su cuenta se ha incorporado a AMS, estas comprobaciones se realizan bajo demanda para mantener el estado de la cuenta. AMS trabaja con usted para corregir cualquier hallazgo relacionado con estas comprobaciones cuando sea necesario. AMS utiliza las siguientes comprobaciones operativas y acciones de API de solo lectura como parte del descubrimiento de cuentas:

| Verificación operativa | Finalidad | AWS Llamadas a la API utilizadas |
| --- | --- | --- |
| AWS Control Tower Evaluación de versiones | Identifica la AWS Control Tower versión para asegurarse de que es la versión mínima | • `ControlTower:GetLandingZone` |

| Verificación operativa | Finalidad | AWS Llamadas a la API utilizadas |
| --- | --- | --- |
| | compatible para incorporarla. Cuenta de AWS | • `ControlTower:ListEnabledControls`<br>• `ControlTower:ListLandingZones` |
| AWS CloudTrail Evaluación | Identifica AWS CloudTrail los senderos y sus configuraciones para incorporarlos Cuenta de AWS a fin de minimizar los costos de los CloudTrail senderos. | • `CloudTrail:GetTrail`<br>• `CloudTrail:ListTrails`<br>• `S3:GetBucketOwnershipControls`<br>• `S3:GetBucketPolicy`<br>• `KMS:GetKeyPolicy`<br>• `CloudTrail:GetEventSelectors`<br>• `S3:GetBucketLogging`<br>• `S3: GetBucketLifecycleConfiguration`<br>• `S3: GetBucketEncryption` |
| CloudFormation Evaluación de ganchos | Identifica los CloudFormation ganchos en su incorporación Cuenta de AWS que bloquean el despliegue del servicio AMS en su Cuenta de AWS. | • `CloudFormation:ListTypes` |

| Verificación operativa | Finalidad | AWS Llamadas a la API utilizadas |
| --- | --- | --- |
| Evaluación de instancias de Amazon EC2 | Identifica las instancias de EC2 Cuenta de AWS que no ejecutan el AWS Systems Manager agente (agente SSM) y que no son compatibles con AMS. | • `EC2:DescribeInstances`<br>• `EC2:DescribeImages`<br>• `SSM:DescribeInstanceInformation` |

AMS Accelerate sigue las mejores prácticas del sector para cumplir y mantener los requisitos de conformidad. El acceso de AMS Accelerate Discovery a su cuenta se registra AWS CloudTrail a través de la función AWSServiceRoleForSupport vinculada al servicio. Esto ayuda a cumplir con los requisitos de supervisión y auditoría. Para obtener información al respecto AWS CloudTrail, consulte la Guía AWS CloudTrail del usuario.

## Paso 2. Incorporación de recursos de gestión en Accelerate

Esta es una descripción general del proceso de incorporación de los recursos de gestión.

Aceptas los términos

Su administrador de prestación de servicios en la nube (CSDM) lo guiará durante el proceso de aceptación. Debe aceptar los términos y condiciones Regiones de AWS, seleccionar los complementos y un acuerdo de nivel de servicio (SLA).

Concedes permisos a las funciones de AMS

Debe conceder acceso a los procesos de AMS y a su Cloud Architect. Para ello, debe crear una CloudFormation pila para cada función. Véase La plantilla para crear funciones de AMS y despuésCree `aws_managedservices_onboarding_role` con CloudFormation para Accelerate. Para obtener más información, consulte Gestión de acceso en AMS Accelerate.

AMS revisa su configuración

Su arquitecto de nube (CA) también busca posibles problemas de configuración en su cuenta, como las políticas de control de servicios (SCPs), y los problemas de seguridad que puedan impedir que AMS implemente las herramientas y los recursos que AMS necesita. Su CA trabaja con usted para

ayudarlo a corregir los hallazgos y eliminar cualquier obstáculo que impida el despliegue de las herramientas y los recursos de AMS.

AMS revisa las configuraciones de sus AWS CloudTrail rutas

Su arquitecto de nube (CA) revisará las configuraciones de sus CloudTrail rutas y confirmará si desea que AMS implemente una CloudTrail ruta global o integre Accelerate con los recursos de rutas de su CloudTrail cuenta o de la organización. Si decide que Accelerate se integre con su CloudTrail ruta, su CA le guiará para realizar las actualizaciones necesarias en las configuraciones de sus recursos de CloudTrail rutas.

AMS despliega recursos de administración

El equipo de AMS despliega herramientas y AWS recursos para proporcionar los diferentes servicios de AMS Accelerate. Una vez finalizada, AMS ha creado la cuenta AWS Managed Services y AMS le notifica que la cuenta está activa.

Con esto concluye la fase de incorporación de los recursos de administración. Puede pasar directamente al siguiente paso del proceso de incorporación:. Paso 3. Incorporación de funciones de AMS con políticas predeterminadas

> **Note**
>
> Ahora que su cuenta está activa, tiene la opción de realizar cualquiera de estas tareas:
>
> - Cree incidentes y solicitudes de servicio para la AWS infraestructura mediante la consola Support Center. Consulte Informes de incidentes, solicitudes de servicio y preguntas sobre facturación en AMS Accelerate.
> - Consulte el estado de conformidad en su cuenta de las AWS Config reglas implementadas por AMS,Cumplimiento de la configuración en Accelerate.
> - Localice y analice los GuardDuty hallazgos y Macie (opcional). Consulte Supervise con GuardDuty.
> - Registros de acceso y auditoría CloudTrail
> - Realice un seguimiento de los cambios en su cuenta de AMS Accelerate. Consulte Seguimiento de los cambios en sus cuentas de AMS Accelerate.
> - Utilice Resource Tagger para crear etiquetas. Consulte Acelere el etiquetador de recursos.
> - Solicite parches, Backup e AWS Config informes. Consulte Informes y opciones.

## Revise y actualice sus configuraciones para permitir que AMS Accelerate utilice su CloudTrail sendero

AMS Accelerate se basa en el AWS CloudTrail registro para gestionar las auditorías y el cumplimiento de todos los recursos de su cuenta. Durante la incorporación, usted decide si Accelerate despliega un CloudTrail registro en su AWS región principal o utiliza los eventos generados por su CloudTrail cuenta o registro organizacional existente. Si su cuenta no tiene una ruta configurada, Accelerate implementará una CloudTrail ruta gestionada durante la incorporación.

> **Important**
>
> CloudTrail La configuración de administración de registros solo es necesaria si decide integrar AMS Accelerate con su CloudTrail cuenta o el registro de su organización.

Revise las configuraciones CloudTrail de las rutas, la política de bucket de Amazon S3 y la política AWS KMS clave del destino de entrega de sus CloudTrail eventos con su Cloud Architect (CA)

Antes de que Accelerate pueda CloudTrail usar su registro, debe trabajar con su arquitecto de nube (CA) para revisar y actualizar sus configuraciones a fin de cumplir con los requisitos de Accelerate. Si decide integrar Accelerate con el registro de su CloudTrail organización, su CA trabajará con usted para actualizar su destino de entrega de CloudTrail eventos, el bucket de Amazon S3 y las políticas AWS KMS clave para permitir las consultas entre cuentas desde su cuenta de Accelerate. Su bucket de Amazon S3 puede estar en una cuenta gestionada por Accelerate o en una cuenta que usted administre. Durante la incorporación, Accelerate valida si las consultas se pueden realizar en el destino de entrega de los eventos de seguimiento de su CloudTrail organización y detiene la incorporación si las consultas fallan. Usted trabaja con su CA para corregir estas configuraciones de modo que se pueda reanudar la incorporación.

Revise y actualice las configuraciones de su CloudTrail cuenta o registro organizacional

Se requieren las siguientes configuraciones para integrar Accelerate CloudTrail Log Management en su CloudTrail cuenta o los recursos de registro de su organización:

- Su CloudTrail registro está configurado para registrar todos los eventos Regiones de AWS.
- Su CloudTrail ruta tiene habilitados los eventos de servicio global.
- El registro de su CloudTrail cuenta u organización registra todos los eventos de administración, incluidos los de lectura y escritura, AWS KMS y el registro de eventos de la API de datos de Amazon RDS está activado.

- Su registro tiene CloudTrail habilitada la validación de la integridad de los archivos de registro.
- El bucket de Amazon S3 que traza CloudTrail entrega eventos para cifrar los eventos mediante el cifrado SSE-S3 o SSE-KMS.
- El bucket de Amazon S3 al que envía el evento su CloudTrail ruta tiene habilitado el registro de acceso al servidor.
- El bucket CloudTrail de Amazon S3 al que entrega el evento tiene una configuración de ciclo de vida que conserva los datos de la CloudTrail ruta durante al menos 18 meses.
- El depósito de Amazon S3 al que se envía CloudTrail el evento en el que se envía el evento tiene la propiedad del objeto establecida como propietario del depósito.
- Accelerate puede acceder al bucket de Amazon S3 al que se envía el evento a través de tu CloudTrail ruta.

Revise y actualice la política de buckets de Amazon S3 para el destino de entrega de sus CloudTrail eventos

Durante la incorporación, trabajas con tu arquitecto de nube (CA) para añadir las declaraciones de política de bucket de Amazon S3 al destino de entrega de tus CloudTrail eventos. Para permitir que sus usuarios consulten los cambios en el bucket de Amazon S3 de destino de entrega de CloudTrail eventos desde su cuenta de Accelerate, puede implementar una función de IAM con un nombre uniforme en cada cuenta de su organización que Accelerate administre y añadirla a la `aws:PrincipalArn` lista de todas las declaraciones de política de bucket de Amazon S3. Con esta configuración, sus usuarios pueden consultar y analizar los eventos del registro de la CloudTrail organización de su cuenta en Accelerate mediante Athena. Para obtener más información sobre cómo actualizar una política de bucket de Amazon S3, consulte Añadir una política de bucket mediante la consola de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

> **Important**
>
> La actualización de la política de buckets de Amazon S3 solo es necesaria cuando Accelerate se integra con una CloudTrail ruta que envía eventos a un bucket de S3 centralizado. Accelerate no admite la integración con una CloudTrail ruta que realice entregas a un bucket centralizado, pero que no tenga las cuentas de una AWS organización.

> **Note**
>
> Antes de actualizar su política de buckets de Amazon S3, sustituya *red* los campos por los valores aplicables:
>
> - *amzn-s3-demo-bucket*con el nombre del bucket de Amazon S3 que contiene los eventos de seguimiento de sus cuentas.
> - *your-organization-id*con el ID de la AWS organización a la que pertenecen sus cuentas.
> - *your-optional-s3-log-delievery-prefix*con el prefijo de entrega de cubos Amazon S3 de tu CloudTrail ruta. Por ejemplomy-bucket-prefix, el que puede haber establecido al crear el CloudTrail sendero.
>
>   Si no ha configurado un prefijo de entrega de buckets de Amazon S3 para su ruta, elimine «*your-optional-s3-log-delievery-prefix*» y la barra diagonal correspondiente (/) de las siguientes declaraciones de política de buckets de Amazon S3.

Las siguientes tres declaraciones de política de bucket de Amazon S3 otorgan a Accelerate acceso para recuperar las configuraciones y ejecutar consultas de AWS Athena para analizar los CloudTrail eventos en el bucket de Amazon S3 de destino de entrega de eventos desde su cuenta de Accelerate.

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWBUCKETCONFIGAUDIT",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetEncryptionConfiguration"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
```

```
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
},
{
    "Sid": "DONOTDELETE-AMS-ALLOWLISTBUCKET",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringLike": {
            "s3:prefix": "your-optional-s3-log-delievery-prefix/AWSLogs/*"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
},
{
    "Sid": "DONOTDELETE-AMS-ALLOWGETOBJECT",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/your-optional-s3-log-delievery-
prefix/AWSLogs/*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
```

```
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
}
```

Revise y actualice la política AWS KMS clave del destino de entrega de sus CloudTrail eventos

Durante la incorporación, trabajas con tu arquitecto de nube (CA) para actualizar la política de AWS KMS claves utilizada para cifrar los eventos de CloudTrail seguimiento que se envían a tu bucket de Amazon S3. Asegúrese de adjuntar las declaraciones de política AWS KMS clave de referencia a su clave actual. AWS KMS Esto configura Accelerate para que se integre con el bucket de Amazon S3 de destino de entrega de eventos de CloudTrail seguimiento existente y descifre los eventos. Para permitir que sus usuarios consulten los cambios en el bucket de Amazon S3 de destino de entrega de CloudTrail eventos desde su cuenta de Accelerate, puede implementar un rol de IAM con un nombre uniforme en cada cuenta de su organización que Accelerate administre y añadirlo a la lista «aws:PrincipalArn». Con esta configuración, sus usuarios pueden consultar eventos.

Hay diferentes escenarios AWS KMS clave de actualización de políticas que hay que tener en cuenta. Es posible que solo tenga una AWS KMS clave configurada en su CloudTrail ruta para cifrar todos los eventos y no tenga una AWS KMS clave que cifre los objetos de su bucket de Amazon S3. O bien, puede tener una AWS KMS clave que cifra los eventos enviados por CloudTrail y otra AWS KMS clave que cifra todos los objetos almacenados en su bucket de Amazon S3. Cuando tiene dos AWS KMS claves, actualiza la política de claves de cada AWS KMS clave para que Accelerate pueda acceder a sus CloudTrail eventos. Asegúrese de modificar la declaración de política AWS KMS clave de referencia por la política AWS KMS clave existente antes de actualizar la política. Para obtener más información sobre cómo actualizar una política AWS KMS clave, consulte Cambiar una política clave en la Guía del AWS Key Management Service usuario.

> **Important**
>
> Solo debe actualizar su política de AWS KMS claves cuando Accelerate se integre en un CloudTrail registro con el cifrado SSE-KMS de los archivos de registro activado.

> **Note**
>
> Antes de aplicar esta declaración de política AWS KMS clave a la AWS KMS clave utilizada para cifrar los AWS CloudTrail eventos que se envían a su bucket de Amazon S3, sustituya los siguientes *red* campos por los valores aplicables:
>
> - *YOUR-ORGANIZATION-ID*con el ID de la AWS organización a la que pertenecen tus cuentas.

Esta declaración de política AWS KMS clave otorga a Accelerate el acceso para descifrar y consultar los eventos de seguimiento enviados al bucket de Amazon S3 desde cada cuenta de su organización, con acceso restringido a Athena, que Accelerate utiliza para consultar y CloudTrail analizar eventos. .

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWTRAILOBJECTDECRYPTION",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "YOUR-ORGANIZATION-ID"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
}
```

## La plantilla para crear funciones de AMS

El siguiente rol de AMS otorga permisos a su arquitecto de nube (CA) de AMS. El siguiente archivo zip contiene el código y la CloudFormation plantilla de Terraform que simplifican la creación del rol de IAM, la política de permisos y la política de confianza. Para obtener más información, consulte con su CA.

| Nombre de función | Requerido por | Plantillas de ejemplo |
| --- | --- | --- |
| `aws_managedservices_onboarding_role` | El personal de AMS solo durante la incorporación | onboarding_role_minimal.zip |

> **Note**
>
> Tras seleccionar y descargar una plantilla de muestra (una por función), la cargará como definiciones de CloudFormation pilas. Cree `aws_managedservices_onboarding_role` con CloudFormation para Accelerate

## Cree **`aws_managedservices_onboarding_role`** con CloudFormation para Accelerate

Puede crear el AWS Identity and Access Management rol,`aws_managedservices_onboarding_role`, CloudFormation desde. Consola de administración de AWS O bien, puede usar los comandos de AWS CloudShell para implementar el rol.

Use la Consola de administración de AWS

> **Note**
>
> Antes de empezar, ten listo para cargar un archivo JSON o YAML para cada rol. Para obtener más información, consulte La plantilla para crear funciones de AMS.

Para crear el rol a partir de Consola de administración de AWS, complete los siguientes pasos:

1. Inicie sesión en Consola de administración de AWS y abra la CloudFormation consola en https://console.aws.amazon.com/cloudformation.

2. Selecciona Crear pila > Con nuevos recursos (estándar). Verás la página siguiente.

3. Selecciona Cargar un archivo de plantilla, carga el archivo JSON o YAML del rol de IAM y, a continuación, selecciona Siguiente. Verás la página siguiente.

4. Introduzca el nombre de la pila «**ams-onboarding-role**» en el campo Nombre de la pila. Introduzca una DateOfExpirycon el formato "YYYY-MM-DDT00:00:00Z" (se recomiendan 30 días a partir de la fecha actual). Continúa desplazándote hacia abajo y seleccionando Siguiente hasta llegar a esta página:

5. Asegúrese de que la casilla de verificación esté seleccionada y, a continuación, seleccione Crear pila.
6. Asegúrese de que la pila se haya creado correctamente.

Usa los comandos de AWS CloudShell

Para implementar la función de `aws_managedservices_onboarding_role` IAM, ejecute el siguiente comando en AWS CloudShell:

AWS CLI

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/onboarding_role_minimal.zip" -o "onboarding_role_minimal.zip"
unzip -q -o onboarding_role_minimal.zip
aws cloudformation create-stack \
    --stack-name "aws-managedservices-onboarding-role" \
    --capabilities CAPABILITY_NAMED_IAM \
    --template-body file://onboarding_role_minimal.json \
    --parameters ParameterKey=DateOfExpiry,ParameterValue="`date -d '+30 days' -u '+
%Y-%m-%dT%H:%M:%SZ'`"
```

AWS Tools for PowerShell

```
Invoke-WebRequest -Uri 'https://docs.aws.amazon.com/en_us/managedservices/
latest/accelerate-guide/samples/onboarding_role_minimal.zip' -OutFile
 'onboarding_role_minimal.zip'
Expand-Archive -Path 'onboarding_role_minimal.zip' -DestinationPath . -Force
New-CFNStack `
    -StackName 'aws-managedservices-onboarding-role' `
    -Capability CAPABILITY_NAMED_IAM `
    -TemplateBody (Get-Content 'onboarding_role_minimal.json' -Raw) `
    -Parameter @{ParameterKey = "DateOfExpiry"; ParameterValue = (Get-
Date).AddDays(30).ToString('yyyy-MM-ddTHH:mm:ssZ')}
```

Después de crear el rol, trabaje con su arquitecto de nube (CA) para completar el Paso 2. Incorporación de recursos de gestión en Accelerate proceso. Cuando AMS le informe de que su cuenta está activa, estará listo para incorporar sus instancias.

## Paso 3. Incorporación de funciones de AMS con políticas predeterminadas

En esta fase, incorporará las funciones de AMS con las políticas predeterminadas. Estas incluyen añadir EC2 instancias de Amazon y configurar la supervisión, las copias de seguridad, AWS Config las correcciones y los parches (si corresponde, AMS Patch Orchestrator es un complemento que debe solicitar específicamente) de acuerdo con sus preferencias. Puede hacerlo usted mismo o solicitar que AMS incorpore funciones en función de sus datos. Para solicitar la ayuda de AMS, cree una solicitud de servicio y proporcione todos los datos necesarios para completar la tarea. Recuerde que las solicitudes de servicio no se resuelven de forma inmediata.

> **Note**
>
> Si bien una cuenta puede usar políticas predeterminadas para realizar copias de seguridad, aplicar parches o monitorear, los recursos deben estar etiquetados para que la política adecuada sea efectiva.

Temas

- Plantilla de inicio rápido (opcional) en Accelerate
- Incorporación: acelere la supervisión
- Incorporación de EC2 instancias para acelerar

- Incorporación en AWS Backup Accelerate
- Integración de parches en Accelerate
- Revise los informes de no conformidad en Accelerate

## Plantilla de inicio rápido (opcional) en Accelerate

La plantilla Quick Start automatiza el despliegue y la configuración de AMS Resource Tagger en las cuentas habilitadas para AWS Accelerate. Esta plantilla ahorra tiempo y esfuerzo en comparación con la configuración manual. Utilice esta plantilla tal cual para definir los conceptos básicos de supervisión, aplicación de parches y copias de seguridad en una sola cuenta. O bien, úselo StackSet para aplicar la configuración en todas las unidades de Organizations para estandarizar la configuración de varias cuentas.

También puedes usarlo como punto de partida para crear tu propio perfil personalizado de AMS Resource Tagger y usar fragmentos de la documentación para crear definiciones más complejas de etiquetado.

Funcionalidad de plantilla de inicio rápido

La plantilla de inicio rápido realiza las siguientes tareas:

- Crea e implementa una versión de configuración para AMS Resource Tagger.
- Aplica etiquetas a las EC2 instancias de Amazon que permiten la administración de AMS y la creación de recursos de monitoreo.
- (Opcional) Aplica etiquetas a EC2 las instancias administradas para que puedan ser parcheadas según el cronograma deseado y crea un período de mantenimiento de parches para facilitar la aplicación de parches.

> **Warning**
>
> De forma predeterminada, las instancias se reinician y las detenidas se inician automáticamente para instalar los parches.

- (Opcional) Aplica etiquetas a EC2 las instancias administradas que permiten realizar copias de seguridad de las mismas según se define en el plan de backup de AMS predeterminado.
- (Opcional) Aplica etiquetas a los recursos gestionados de Amazon Relational Database Service (Amazon RDS) que permiten realizar copias de seguridad de ellos de acuerdo con el plan de copia

de seguridad mejorado. Un plan de respaldo también permite la recuperación puntual (PITR) para Amazon RDS. Si la copia de seguridad automática de Amazon RDS no está habilitada, la base de datos se reiniciará cerca de la hora de la siguiente ventana de copia de seguridad.

Anulaciones y exclusiones de la plantilla de inicio rápido

Después de usar esta plantilla para crear una pila de inicio rápido, siga los siguientes pasos para excluir instancias específicas de Management/Monitoring, Parcheo o Backup:

- Administración y supervisión: para impedir que AMS gestione y supervise una EC2 instancia, añada esta etiqueta a la instancia:. `ExcludeFromAMSQuickStartMonitoring=true`
- Aplicación de parches: esta EC2 plantilla de inicio rápido excluye de la aplicación de parches a las instancias que son miembros de un grupo de Auto Scaling, Amazon Elastic Container Service o un clúster de Amazon Elastic Kubernetes Service.

  Para deshabilitar la creación de una ventana de aplicación de parches y el etiquetado de instancias relacionado con los parches, defina el parámetro de pila en. EC2 CloudFormation `EnablePatching=false`

  Para excluir una EC2 instancia del objetivo de la ventana de creación de parches de inicio rápido`EnablePatching=true`, añada esta etiqueta a la instancia:. `ExcludeFromAMSQuickStartPatching=true`
- Backup: EC2 las instancias que son miembros de grupos de Auto Scaling, ECS o clúster EKS se excluyen del Backup mediante esta plantilla de inicio rápido.

  Para excluir una EC2 instancia de la segmentación del Plan de Backup AMS predeterminado, cuando`EnableBackup=true`, añada esta etiqueta a esa instancia:`ExcludeFromAMSQuickStartBackup=true`.

> **Tip**
>
> Puede etiquetar EC2 instancias de forma masiva. Utilice el editor de etiquetas para seleccionar y etiquetar recursos de forma masiva en un solo paso en el. Consola de administración de AWS

Parámetros de la plantilla de inicio rápido

Esta plantilla de inicio rápido configura Resource Tagger para agregar la etiqueta `ams:rt:ams-managed=true` a todas las EC2 instancias de la cuenta, excluidas las instancias a las que se agrega la `ExcludeFromAMSQuickStartMonitoring=true` etiqueta. Utilice los siguientes parámetros para controlar las partes opcionales de esta pila según sus necesidades:

| Parámetro CFN | Valor | Efecto |
|---|---|---|
| EnableBackup | 'true' (predeterminado) | Todas las EC2 instancias administradas por AMS (`ams:rt:ams-managed=true` ) se etiquetan como copias de seguridad todos `ams:rt:backup-orchestrator=true` los días a las 4 a.m. UTC, según el plan de respaldo de AMS predeterminado.<br><br>Para todas las instancias y clústeres de RDS, la plantilla aplica el `ams:rt:backup-orchestrator-enhanced=true` «respaldo continuo» con una retención máxima (31 días) según el plan de respaldo mejorado.<br><br>Si esto cambia el período de retención del PITR, es posible que la base de datos se reinicie en algunos casos, por ejemplo, si hay otras actualizaciones de configuración pendientes. |
| | 'falso' | Esta plantilla de inicio rápido no está destinada a realizar copias de seguridad de ninguna instancia. |

| Parámetro CFN | Valor | Efecto |
| --- | --- | --- |
| EnablePatching | 'false' (predeterminado) | Esta plantilla de inicio rápido no está destinada a ser parcheada en ninguna instancia. |
| | 'cierto' | Todas las instancias administradas por AMS (`ams:rt:ams-managed=true` ) se etiquetan `ams:rt:Patch Group=AMS QuickStartPatchWindow` y se crea un recurso básico de ventana de mantenimiento de SSM para facilitar la aplicación de parches de acuerdo con el cronograma definido en. `CronExpression`<br><br>Para aplicar la `ams:rt:Patch Group` etiqueta a la EC2 instancia , debe desactivar el acceso a las etiquetas de los metadatos de la instancia. |
| CronExpression | - | El valor predeterminado de `cron(0 30 19 ? * SAT#2 *)` establece el segundo sábado del mes a las 19:30 según el `Timezone` parámetro. Usa la sintaxis cron. |
| Zona horaria | - | Las instancias de destino se parchean según. `CronExpression` Utilice el formato IANA. |

Descarga la plantilla de inicio rápido

Descargue el archivo AMSQuick Start.zip.

O bien, ejecute el siguiente comando AWS CloudShellpara implementar`AMSQuickStart.yaml`:

AWS Command Line Interface

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/AMSQuickStart.zip" -o "AMSQuickStart.zip"
unzip -q -o AMSQuickStart.zip
for region in region1 region2 ;
do
aws cloudformation create-stack \
    --region $region \
    --stack-name "AMSQuickStart" \
    --template-body file://AMSQuickStart.yaml \
    --parameters \
        ParameterKey=EnableBackup,ParameterValue="true" \
        ParameterKey=EnablePatching,ParameterValue="false" \
        ParameterKey=Timezone,ParameterValue="US/Eastern" \
        ParameterKey=CronExpression,ParameterValue="cron(0 30 19 ? * SAT#2 *)" \
;
done
```

AWS Tools for PowerShell

```
Invoke-WebRequest -Uri 'https://docs.aws.amazon.com/en_us/managedservices/latest/
accelerate-guide/samples/AMSQuickStart.zip' -OutFile 'AMSQuickStart.zip'
Expand-Archive -Path 'AMSQuickStart.zip' -DestinationPath . -Force
@('region1', 'region2') | `
ForEach-Object { `
New-CFNStack `
    -Region $_ `
    -StackName 'AMSQuickStart' `
    -TemplateBody (Get-Content 'AMSQuickStart.yaml' -Raw) `
    -Parameter @(
        @{ParameterKey = "EnableBackup"; ParameterValue = "true"},
        @{ParameterKey = "EnablePatching"; ParameterValue = "false"},
        @{ParameterKey = "Timezone"; ParameterValue = "US/Eastern"},
        @{ParameterKey = "CronExpression"; ParameterValue = "cron(0 30 19 ? * SAT#2
 *)"}
    )
}
```

Para obtener una descripción de cada parámetro, consulte la sección anterior,Parámetros de la plantilla de inicio rápido.

## Incorporación: acelere la supervisión

La supervisión está habilitada de forma predeterminada para todos los recursos nuevos, excepto para las instancias de Amazon EC2. Puede empezar a monitorizar sus instancias de Amazon EC2 etiquetándolas.

Para incorporar la supervisión, primero asegúrese de que su configuración monitorea los recursos que desea que AMS supervise e ignora los recursos que desea que ignore.

Puede utilizar los siguientes CloudWatch paneles para ver cuántos de sus recursos son objeto de la supervisión y el etiquetado de AMS y cuántos no. En su cuenta, vaya a la consola de CloudWatch paneles y seleccione una de las siguientes opciones:

- Panel de informes de AMS-Alarm-Manager
- Panel de informes de AMS-Resource-Tagger

Para obtener una descripción completa de las métricas del panel, consulte:

- Visualización del número de recursos gestionados por Resource Tagger

Recursos de incorporación que se van a monitorear en Accelerate

Para anular el comportamiento predeterminado, por ejemplo, para deshabilitar la supervisión predeterminada de los recursos que no son de EC2, debe eliminar la etiqueta de esos recursos mediante un perfil de configuración personalizado. Para obtener más información sobre el etiquetado para la supervisión, consulte. Supervisión en Accelerate

La supervisión está deshabilitada para las instancias EC2 hasta que las incorpore, lo que incluye el etiquetado de las instancias mediante un perfil de configuración personalizado. En la siguiente sección, se describe la incorporación de instancias de EC2.

Creación de un perfil de configuración de monitoreo en Accelerate

- Para obtener información sobre el uso de la configuración predeterminada, consulteAcelere el administrador de alarmas.
- Para obtener información sobre el uso de una configuración personalizada, consulteModificación de la configuración predeterminada de la alarma Accelerate.

## Incorporación de EC2 instancias para acelerar

EC2 las instancias se incorporan a AMS Accelerate mediante un proceso denominado configuración automatizada de instancias, que garantiza que cada instancia escriba los registros correctos y emita las métricas correctas para que AMS la administre correctamente. Deberías incorporar todas tus EC2 instancias, a menos que desees específicamente que AMS ignore algunas. La configuración automatizada de instancias requiere que se cumplan condiciones específicas que permitan a AMS configurar la instancia (para obtener más información, consulteRequisitos previos para la configuración automatizada de instancias en Accelerate). La condición más importante es que el AWS Systems Manager agente (agente SSM) debe estar instalado en cada EC2 instancia de Amazon que desee que AMS gestione por usted. Para obtener más información sobre el agente SSM, consulte Trabajar con el agente SSM.

SSM viene preinstalado de serie para Accelerate AMIs

El agente SSM ya está instalado en los siguientes AWS sistemas operativos AMIs .

- Amazon Linux y Amazon Linux 2
- SUSE Linux Enterprise Server (SLES) 12 y 15
- Microsoft Windows Server 2019, 2016, 2012 R2, 2012
- Ubuntu Linux 18.04 y 20.04

Si está utilizando uno de los que se AWS proporcionan, consulte AMIs. Etiquetado de instancias en Accelerate

Instalación manual de SSM por SSM en Accelerate

Para los siguientes sistemas operativos, o cuando utilice una AMI personalizada, puede instalar manualmente el agente SSM. O bien, puede usar la función de instalación automática del agente AMS SSM. Para obtener más información sobre la instalación automática de SSM, consulteInstalación automática de SSM Agent. Para obtener instrucciones sobre la instalación manual, seleccione el enlace correspondiente a su sistema operativo:

- Instalación de CentOS SSM
- Instalación de Oracle SSM
- Instalación de Red Hat SSM
- Instalación de SUSE Linux Enterprise Server SSM
- Instalación de Windows SSM

Etiquetado de instancias en Accelerate

Una vez instalado el agente SSM, debe etiquetar las instancias. Consulte Etiquetado en AMS Accelerate.

Configuración automatizada de instancias en Accelerate

Una vez etiquetada la instancia, AMS realiza una configuración de instancia automatizada, que incluye:

- Registra los registros y las métricas del sistema operativo
- Habilite el acceso remoto para los ingenieros de AMS
- Ejecute comandos remotos en la instancia

Estas tareas son esenciales para los servicios de monitoreo, parches y registro de AMS, y para que AMS responda a los incidentes. Para obtener más información sobre cómo configurar la configuración automatizada de instancias, consulteConfiguración automatizada de instancias en AMS Accelerate.

Una vez completada la configuración automatizada de la instancia, podrá:

- Cree incidentes y solicitudes de servicio para las EC2 instancias y los sistemas operativos de Amazon mediante la consola Support Center. Para obtener más información, consulte Informes de incidentes, solicitudes de servicio y preguntas sobre facturación en AMS Accelerate.
- Acceder a los EC2 registros de Amazon y auditarlos
- Obtenga informes de parches

## Incorporación en AWS Backup Accelerate

Para configurar las copias de seguridad, debe crear políticas de copia de seguridad denominadas planes de copia de seguridad. Un plan de copias de seguridad especifica de qué AWS recursos se van a realizar copias de seguridad, con qué frecuencia se deben realizar copias de seguridad y el período de retención de las copias de seguridad. Recomendamos evaluar los requisitos de continuidad, seguridad y conformidad de su organización para determinar qué planes de respaldo necesita.

Inscríbase

- Asegúrese de que AWS Backup esté habilitada para cada cuenta, región y tipo de recurso siguiendo estos pasos:

  Primeros pasos 1: suscripción al servicio.

  Opcionalmente, Primeros pasos 2: cree una copia de seguridad bajo demanda.

Elija un plan de respaldo

- Para elegir un plan de respaldo, consulteSeleccione un plan de respaldo de AMS.

Añadir recursos

Los recursos no están asociados a un plan de respaldo de forma predeterminada. Deben añadirse a un plan de respaldo.

- Para añadir recursos a un plan de respaldo, consulteEtiquete sus recursos para aplicar los planes de respaldo de AMS.
- Para habilitar la copia de seguridad en todos los recursos mediante etiquetas, consulteAdministración de etiquetas para copias de seguridad en Accelerate.

## Integración de parches en Accelerate

Debe configurar los parches para garantizar que su software cumpla con sus políticas up-to-date de conformidad.

AWS Backup requisito previo: Para permitir la creación de una instantánea del volumen raíz durante el período de mantenimiento de la aplicación de parches, asegúrese de que AWS Backup esté habilitada para cada cuenta y región para el tipo de recurso de Amazon EBS siguiendo estos pasos: Introducción 1: suscripción del servicio. (No es necesario que continúe con la sección Introducción 2: creación de una copia de seguridad bajo demanda).

Cuándo aplicar el parche: el parcheo se produce durante un período de mantenimiento. Puede programar los períodos de mantenimiento para que los parches solo se apliquen durante los tiempos preestablecidos.

Qué parchear: debes asociar las EC2 instancias de Amazon que deseas parchear a un período de mantenimiento. Para asociar las instancias a una ventana de mantenimiento, las EC2 instancias de

Amazon deben estar etiquetadas y la ventana de mantenimiento debe tener esas etiquetas como objetivo.

Qué parches instalar: mediante las líneas base de los parches, se establecen reglas para la aprobación automática de determinados tipos de parches, como los del sistema operativo o los de alta gravedad. También puede especificar excepciones a sus reglas, por ejemplo, listas de parches que siempre se aprueban o rechazan.

Consulte Recomendaciones de aplicación de parches para obtener orientación sobre las políticas de EC2 parches de Amazon.

- Para empezar a configurar la administración de parches, consulte Comprenda la administración de parches en AMS Accelerate
- Para crear una configuración de parches personalizada, consulteLínea base de parches personalizada con AMS Accelerate.

### Revise los informes de no conformidad en Accelerate

AMS implementa AWS Config reglas que ayudan a identificar las infracciones a las normas establecidas por el Centro de Seguridad de Internet (CIS) y el Marco de Seguridad en la Nube (CSF) del Instituto Nacional de Estándares y Tecnología (NIST). Te recomendamos que revises el informe de no conformidad con tu equipo de entrega para priorizar las medidas correctivas, de modo que tu cuenta se base en un estado conforme.

## Paso 4. Personalice las funciones de Accelerate

En esta etapa, ya ha incorporado la supervisión, la aplicación de parches y las copias de seguridad con las políticas predeterminadas. Ahora tiene la oportunidad de personalizar las políticas para que se adapten a sus necesidades.

Puede optar por utilizar las políticas predeterminadas para la aplicación de parches, copias de seguridad o supervisión, o bien elegir una política personalizada en función de sus necesidades. AMS usa etiquetas para asociar los recursos a las políticas operativas. AMS proporciona un etiquetador de recursos que le permite especificar reglas sobre cómo se aplican las etiquetas a AWS los recursos en función de la agrupación de aplicaciones u otra lógica de agrupación. Para obtener más información, consulte. Acelere el etiquetador de recursos

La función de etiquetas proporcionada por el cliente le permite añadir y eliminar etiquetas personalizadas en los recursos de AMS. Para obtener más información, consulte Etiquetas proporcionadas por el cliente en Accelerate.

Temas

- Personalice la supervisión en Accelerate
- Personalice el respaldo en Accelerate
- Personalice la aplicación de parches en Accelerate

## Personalice la supervisión en Accelerate

Para personalizar la supervisión de los recursos de la nube en función de las necesidades de su aplicación:

1. Cree una política de supervisión personalizada. Consulte Modificación de la configuración predeterminada de la alarma Accelerate.
2. Aplica una política personalizada a los recursos mediante etiquetas. Consulte Supervisión en Accelerate
3. Enruta las alertas al propietario del recurso. Consulte Notificación de alertas basada en etiquetas.

Puede utilizar los siguientes CloudWatch paneles para ver cuántos de sus recursos son objeto de la supervisión y el etiquetado de AMS y cuántos no. En su cuenta, vaya a la consola de CloudWatch paneles y seleccione una de las siguientes opciones:

- Panel de informes de AMS-Alarm-Manager
- Panel de informes de AMS-Resource-Tagger

Para obtener una descripción completa de las métricas del panel, consulte:

- Visualización del número de recursos gestionados por Resource Tagger

## Personalice el respaldo en Accelerate

No se pueden personalizar los planes de respaldo predeterminados de AMS. En su lugar, cree un nuevo plan de respaldo en función de las necesidades de su aplicación y, a continuación, adjunte los recursos a su plan personalizado mediante etiquetas. Depende de usted elegir qué recursos debe

respaldar AMS, con qué frecuencia y durante qué período de retención. Recomendamos evaluar los requisitos de continuidad, seguridad y cumplimiento de su organización para determinar qué planes de respaldo necesita.

- Para crear un plan de respaldo, consulte Creación de un plan de respaldo.
- Para asignar recursos a un plan de respaldo, consulte Asignación de recursos a un plan de respaldo.

## Personalice la aplicación de parches en Accelerate

La aplicación de parches garantiza que su software cumpla sus políticas de up-to-date conformidad y las cumpla.

Cuándo aplicar los parches: los parches se realizan durante un período de mantenimiento. Puede programar los períodos de mantenimiento para que los parches solo se apliquen durante los tiempos preestablecidos.

Qué parchear: debes asociar las EC2 instancias de Amazon que deseas parchear a un período de mantenimiento. Para asociar las instancias a una ventana de mantenimiento, las EC2 instancias de Amazon deben estar etiquetadas y la ventana de mantenimiento debe tener esas etiquetas como objetivo.

Qué parches instalar: mediante las líneas base de los parches, se establecen reglas para la aprobación automática de determinados tipos de parches, como los del sistema operativo o los de alta gravedad. También puede especificar excepciones a sus reglas, por ejemplo, listas de parches que siempre se aprueban o rechazan.

- Para obtener recomendaciones generales sobre la aplicación de parches, consulteRecomendaciones de aplicación de parches.
- Para crear ventanas de mantenimiento personalizadas, consulteCree una ventana de mantenimiento de parches en AMS.
- Para crear líneas base de parches personalizadas, consulte. Línea base de parches personalizada con AMS Accelerate
- Para enviar las alertas de parches al propietario del recurso, consulte. Comprenda las notificaciones de parches y los fallos de los parches en AMS Accelerate

# Uso de las consolas AMS

Las consolas AMS de la consola AWS de gestión están disponibles para que pueda interactuar con AMS y utilizar sus recursos gestionados por AMS Advanced y AMS Accelerate. Por lo general, las consolas AMS se comportan como cualquier otra AWS consola; sin embargo, dado que AMS es una organización privada, solo las cuentas habilitadas para AMS pueden acceder a la consola. Una vez que AMS esté activado en su cuenta, podrá acceder a la consola buscando «Managed Services» en la barra de búsqueda unificada.

> **Note**
>
> Según el rol de su cuenta, podrá acceder a la consola AMS Advanced o a la consola AMS Accelerate.

Cuando utilice las consolas AMS, tenga en cuenta las siguientes advertencias:

- La consola AMS es específica de cada cuenta. Por lo tanto, si tienes una cuenta «de prueba» para tu organización, no podrás ver los recursos en la cuenta «Prod» de esa organización. Del mismo modo, debe tener un rol de AMS Advanced para acceder a la consola de AMS Advanced.
- Las consolas AMS aplican una política de IAM al autenticarse que determina a qué consola puede acceder y qué puede hacer allí. El administrador puede aplicar políticas adicionales a la política de AMS predeterminada para restringir lo que puede ver y hacer en la consola.

La consola AMS Accelerate cuenta con las siguientes funciones:

- Página de apertura: la página de apertura tiene cuadros de información y enlaces para facilitar el acceso a .
- Páginas destacadas y enlaces en el panel de navegación izquierdo:
  - Panel de control: proporciona una descripción general del estado actual de su cuenta, que incluye:
    - Incidentes en sus recursos: un botón para abrir un caso de incidente en AWS Support Center, además de cuántos casos de incidentes están pendientes de aprobación y requieren su atención y cuántos están abiertos
    - Estado de conformidad: enlaces a reglas y recursos que no cumplen o cumplen con los requisitos

    - Solicitudes de servicio: un botón para abrir un caso de solicitud de servicio en AWS Support Center, además de cuántas están pendientes de aprobación y requieren su atención y cuántas están abiertas
    - Seguridad a nivel de cuenta: enlaces a información detallada sobre las conclusiones sobre la detección de amenazas en tiempo real y las GuardDuty conclusiones de Macie en materia de seguridad y privacidad de los datos
    - Acciones rápidas: abra las páginas de configuración de sus almacenes de Backup o instancias de parches
  - Informes: abre la página de informes y los informes predeterminados, Daily Backup y Daily Patch y Monthly Billing
  - Configuración: asegúrese de que sus recursos se gestionen correctamente y de acuerdo con sus especificaciones.
    - Instale el agente SSM: se requiere el agente SSM
    - Configure las reglas de etiquetado: abre el etiquetador de recursos AMS
    - Configurar alarmas: abre la configuración de alarmas AMS CloudWatch
    - Configurar el calendario de parches: abre la consola de AWS Systems Manager
    - Configurar líneas base de parches: abre la consola de AWS Patch Manager
    - Configurar planes de backup: abre la consola AWS Backup
- Característica destacada: información sobre las últimas actualizaciones de la consola
- Documentación: Página de inicio de la documentación de AWS Managed Services

# Patrones AMS

Un patrón de AWS Managed Services (AMS) es una solución generalizada que resuelve una familia de casos de uso en el entorno gestionado por AMS.

Mientras trabaja en la plataforma AMS, los arquitectos de nube de AMS (CAs) trabajan con usted para cumplir sus requisitos empresariales y operativos. Si bien los clientes de AMS operan de una manera única, observamos que tienen casos de uso similares. En esos casos, CAs cree plantillas de soluciones generales, o «patrones», que se utilicen en varios entornos de clientes con un esfuerzo mínimo de configuración e implementación.

Los patrones de AMS se crean para ayudar a ofrecer funciones a los clientes de AMS y, por lo general, los crea la CA de la cuenta del cliente que los solicita.

# Cómo funcionan los patrones AMS

Para solicitar más detalles sobre cada patrón, incluidas las plantillas de formación de nubes necesarias para poder implementar el patrón, envíe una solicitud de servicio de AMS con el asunto «Solicitud de detalles adicionales sobre el patrón*Pattern_Name*» (sustitúyalo por el patrón que desee) y añada su arquitecto de nube (CA) de AMS a la opción de contactos adicionales.

Los patrones de AMS se clasifican en dos (2) categorías:

- Uso general: los patrones se consideran estables, ya que han sido implementados y utilizados por varios clientes de AMS
- Modo de vista previa: AMS recomienda implementar los patrones del modo de vista previa en sus entornos que no son de producción para su validación, y consultar con su arquitecto de nube para analizar el caso de uso antes del despliegue.

> **Important**
>
> Los patrones de AMS no cumplen con los acuerdos de nivel de servicio (SLAs) y los objetivos de nivel de servicio () predeterminados de AMS. SLOs Support y actualizaciones del patrón se realizan haciendo todo lo posible.
> Este AWS contenido se proporciona sujeto a los términos del Acuerdo con el AWS cliente u otro acuerdo escrito entre el cliente y Amazon Web Services, Inc. o Amazon Web Services EMEA SARL («AWS Europa») o ambos.
> El material incluido en este software se proporciona «tal cual» y sin garantía de ningún tipo, ya sea expresa, implícita o de otro tipo, incluida, sin limitación, cualquier garantía de idoneidad para un propósito particular.

# Patrones AMS

Patrones AMS.

Patrones AMS

| Nombre | Información general | Ventajas | Categoría |
|---|---|---|---|
| Personalice las notificaciones | Personalice las notificaciones de | Añadir informaci ón contextual a las | Monitoreo |

| Nombre | Información general | Ventajas | Categoría |
| --- | --- | --- | --- |
| CloudWatch de alarma | CloudWatch alarma para incluir informaci ón de las etiquetas de la instancia, como el nombre de la instancia, el ID de la aplicación, etc. | notificaciones de alarma las hará más significativas y proporcionará información procesabl e. | |
| Informes de uso del disco | El patrón de informes de uso del disco recopila el espacio de consumo de los volúmenes en varias cuentas de aplicacio nes y presenta el resultado como un informe centralizado en Amazon S3 con la capacidad de consulta de tablas de Athena. | Proporcione informaci ón sobre el uso real de los volúmenes de las cuentas para determinar las oportunidades de ahorro de costes. | Optimización de costos |
| Prowler Stack | Realiza comprobac iones de Prowler en cuentas que utilizan Amazon EC2 donde no se CloudShell puede utilizar. | Ayude a desbloque ar la incorporación de Accelerate (Prowler) en los casos en que no CloudShel l pueda utilizarse debido a problemas de permisos o de tiempo de espera, sin que ello afecte a su postura de seguridad actual. | Seguridad |

| Nombre | Información general | Ventajas | Categoría |
| --- | --- | --- | --- |
| Replicación de AMS Amazon S3 con claves de objeto personalizadas | Haga copias de los objetos de Amazon S3 y conserve todos los metadatos y las claves de objetos (carpetas).<br><br>Elimina parte de las claves de los objetos de origen o crea claves de objetos de destino personalizadas durante la replicación. | Personalice las claves de objetos (carpetas) durante la replicación de Amazon S3 sin necesidad de scripts adicionales para mover los objetos a las carpetas requeridas. | Fiabilidad |
| Eliminación de instantáneas de Amazon EBS | Automatización basada en Lambda y CloudWatch Events para automatizar la eliminación de instantáneas de Amazon EBS tomadas fuera de Amazon AWS Backup, en función de la retención. | Ayude a eliminar las instantáneas individuales tomadas fuera de AWS Backup Orchestrator, ahorrando costes adicionales con el paso del tiempo. | Optimización de costos |

| Nombre | Información general | Ventajas | Categoría |
| --- | --- | --- | --- |
| Rotación de secretos de Amazon RDS de AMS | Mediante una CloudFormation plantilla, implement e automáticamente todos los recursos necesarios (función Lambda, grupos de seguridad, interface s de red elásticas o ENIs) necesarios para rotar los secretos de las bases de datos compatibl es de Amazon RDS, Redshift y DocumentDB. | Automatice la rotación de los secretos de las bases de datos y proporcione un mecanismo de notificación cuando se produzca un error de rotación. | Seguridad |
| Rotación automática de claves | Rote automátic amente las claves secretas y de acceso para los usuarios de IAM en función de CloudWatch Events y Lambda. | Rotación más sencilla de las claves secretas y de acceso para los usuarios de IAM. | Seguridad |

| Nombre | Información general | Ventajas | Categoría |
| --- | --- | --- | --- |
| Etiquetador de instantáneas de volúmenes de Amazon EBS | Etiquete todos los volúmenes e instantáneas de Amazon EBS con las etiquetas de las instancias de Amazon EC2 . | Ayude a categorizar y realizar un seguimiento de los costos con información empresarial significativa y relevante, lo que le permitirá validar con más facilidad en qué se gasta el dinero y posibilite el uso de la automatización para etiquetar volúmenes e instantáneas. La mejor práctica altamente recomendada por el pilar de optimización de AWS costes. | Etiquetado (optimización de costes, seguridad, gestión de incidentes y automatización) |

# Configuración automatizada de instancias en AMS Accelerate

AMS Accelerate proporciona un servicio de configuración de instancias automatizado. Este servicio garantiza que una instancia emita los registros y las métricas correctos para que AMS la administre correctamente. La configuración automatizada de las instancias tiene sus propios requisitos previos y pasos para la incorporación, que se describen más adelante en esta sección.

Temas

- Cómo funciona la configuración automatizada de instancias en Accelerate
- Instalación automática de SSM Agent
- Cambios automatizados en la configuración de las instancias

# Cómo funciona la configuración automatizada de instancias en Accelerate

La configuración automatizada de instancias permite a AMS Accelerate realizar determinadas configuraciones a diario en las instancias que usted indique añadiendo determinados agentes y etiquetas.

## Requisitos previos para la configuración automatizada de instancias en Accelerate

Estas condiciones deben cumplirse para que AMS Accelerate pueda realizar las acciones automatizadas descritas anteriormente en las instancias gestionadas.

El agente SSM está instalado

La configuración automática de instancias de AMS Accelerate requiere que el agente AWS Systems Manager SSM esté instalado.

Para obtener información sobre el uso de la función de instalación automática del agente AMS SSM, consulteInstalación automática de SSM Agent.

Para obtener información sobre la instalación manual del agente SSM, consulte lo siguiente:

- Linux: instale manualmente el agente SSM en las EC2 instancias de Amazon para Linux - AWS Systems Manager
- Windows: instale manualmente el agente SSM en las EC2 instancias de Amazon para Windows Server - AWS Systems Manager

El agente SSM se encuentra en estado administrado

La configuración automatizada de instancias de AMS Accelerate requiere un agente SSM operativo. El agente SSM debe estar instalado y la EC2 instancia de Amazon debe estar en estado gestionado. Para obtener más información, consulte la AWS documentación sobre cómo trabajar con el agente SSM.

## Configuración de instancias automatizada

Si se cumplen los requisitos previos, la adición de una etiqueta de EC2 instancia de Amazon específica inicia automáticamente la configuración automática de la instancia de AMS Accelerate. Usa uno de los siguientes métodos para añadir esta etiqueta:

1. (Se recomienda encarecidamente) Utilice el etiquetador de recursos AMS Accelerate

Para configurar la lógica de etiquetado de su cuenta, consulte. Cómo funciona el etiquetado
Una vez finalizado el etiquetado, las etiquetas y la configuración automática de las instancias se gestionan automáticamente.

2. Añada etiquetas manualmente

   Añade manualmente la siguiente etiqueta a las EC2 instancias de Amazon:

   Clave: ams:rt:ams-managed, valor: true.

> **Note**
>
> El servicio de configuración de instancias intenta aplicar las configuraciones de AMS requeridas una vez que se aplica la etiqueta ams:rt:ams-managed a la instancia. El servicio confirma las configuraciones requeridas por el AMS cada vez que se inicia una instancia y cuando se comprueba la configuración diaria del AMS.

## Instalación automática de SSM Agent

> **Important**
>
> La instalación automática de SSM Agent no es compatible con la región Asia Pacífico (Malasia).

Para que AMS gestione sus instancias de Amazon Elastic Compute Cloud (Amazon EC2), debe AWS Systems Manager instalar SSM Agent en cada instancia. Si tus instancias no tienen instalado el Agente SSM, puedes usar la función de instalación automática del Agente SSM de AMS.

> **Note**
>
> - Si su cuenta está incorporada a AMS Accelerate después del 6 de marzo de 2024, esta función está habilitada de forma predeterminada. Para desactivar esta función, póngase en contacto con su CA o CSDM.
> - Para activar esta función en las cuentas incorporadas antes del 6 de marzo de 2024, póngase en contacto con su CA o CSDM.

- Esta función solo está disponible para instancias EC2 que no estén en un grupo de Auto Scaling y que ejecuten sistemas operativos Linux compatibles con AMS.

## Requisitos previos para el uso del agente SSM

- Asegúrese de que el perfil de instancia asociado a las instancias de destino tenga una de las siguientes políticas (o permisos equivalentes a los permitidos que figuran en ellas):
  - Amazon SSMManaged EC2 InstanceDefaultPolicy
  - Amazon SSMManaged InstanceCore
- Asegúrese de que no haya una política de control de servicios en el AWS Organizations nivel que deniegue explícitamente los permisos enumerados en las políticas anteriores.

  Para obtener más información, consulte Configuración de permisos de instancia requeridos para Systems Manager.
- Para bloquear el tráfico saliente, asegúrese de que los siguientes puntos finales de la interfaz estén habilitados en la VPC en la que residen las instancias de destino (sustituya «región» en la URL según corresponda):
  - ssm.<region>.amazonaws.com
  - ssmmessages.<region>.amazonaws.com
  - mensajes ec2. <region>.amazonaws.com

  Para obtener más información, consulte Mejora de la seguridad de las instancias de EC2 mediante puntos de conexión de VPC para Systems Manager.

Para obtener consejos generales sobre cómo habilitar o solucionar problemas de la disponibilidad de los nodos gestionados, consulte la Solución 2: Compruebe que se haya especificado un perfil de instancia de IAM para la instancia (solo instancias de EC2).

> **Note**
>
> AMS detiene e inicia cada instancia como parte del proceso de instalación automática. Cuando se detiene una instancia, se pierden los datos almacenados en los volúmenes del almacén de instancias y los datos almacenados en la RAM. Para obtener más información, consulta Qué ocurre cuando detienes una instancia.

### Solicita la instalación automática del agente SSM en tus instancias

Si sus cuentas están integradas en AMS Accelerate Patch Add-On, configure una ventana de mantenimiento de parches (MW) para las instancias. Se necesita un agente SSM que funcione para completar el proceso de revisión. Si falta el agente SSM en una instancia, AMS intentará instalarlo automáticamente durante el período de mantenimiento del parche.

> **Note**
>
> AMS detiene e inicia cada instancia como parte del proceso de instalación automática. Cuando se detiene una instancia, se pierden los datos almacenados en los volúmenes del almacén de instancias y los datos almacenados en la RAM. Para obtener más información, consulta Qué ocurre cuando detienes una instancia.

### Cómo funciona la instalación automática de SSM Agent

AMS utiliza los datos de usuario de EC2 para ejecutar el script de instalación en las instancias. Para añadir el script de datos de usuario y ejecutarlo en las instancias, AMS debe detener e iniciar cada instancia.

Si la instancia ya tiene un script de datos de usuario existente, AMS completa los siguientes pasos durante el proceso de instalación automática:

1. Crea una copia de seguridad del script de datos de usuario existente.
2. Sustituye el script de datos de usuario existente por el script de instalación del agente SSM.
3. Reinicia la instancia para instalar el agente SSM.
4. Detiene la instancia y restaura el script original.
5. Reinicia la instancia con el script original.

## Cambios automatizados en la configuración de las instancias

La automatización de la configuración de instancias de AMS Accelerate realiza los siguientes cambios en su cuenta:

1. Permisos de IAM

Añade las políticas gestionadas por IAM necesarias para conceder a la instancia el permiso de uso de los agentes instalados por AMS Accelerate.

2. Agentes
   a. El CloudWatch agente de Amazon es responsable de emitir los registros y las métricas del sistema operativo. La automatización de la configuración de instancias garantiza que el CloudWatch agente esté instalado y ejecutando la versión mínima de AMS Accelerate.
   b. El agente AWS Systems Manager SSM es responsable de ejecutar los comandos remotos en la instancia. La automatización de la configuración de la instancia garantiza que el agente SSM ejecute la versión mínima de AMS Accelerate.
3. CloudWatch Configuración
   a. Para garantizar que se emitan las métricas y los registros necesarios, AMS Accelerate personaliza la CloudWatch configuración. Para obtener más información, consulte la siguiente sección,CloudWatch detalles del cambio de configuración.

La configuración automatizada de instancias realiza cambios o adiciones a los perfiles y la CloudWatch configuración de las instancias de IAM.

## Detalles de cambio de permisos de IAM

Cada instancia administrada debe tener una AWS Identity and Access Management función que incluya las siguientes políticas administradas:

- arn:aws:iam: :aws:policy/Amazon SSMManaged InstanceCore
- arn:aws:iam: :aws:policy/ CloudWatchAgentServerPolicy
- arn:aws:iam: :aws:policy/ AMSInstance ProfileBasePolicy

Las dos primeras son políticas administradas. AWS La política administrada por AMS es:

AMSInstanceProfileBasePolicy

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Action": [
                "secretsmanager:CreateSecret",
                "secretsmanager:UpdateSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:*:*:secret:/ams/byoa/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "kms:Encrypt"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Si su instancia ya tiene una función de IAM asociada, pero le falta alguna de estas políticas, AMS añadirá las políticas que faltan a su función de IAM. Si la instancia no tiene una función de IAM, AMS la asigna. AMSOSConfigurationCustomerInstanceProfile La función AMSOSConfigurationCustomerInstanceProfilede IAM tiene todas las políticas requeridas por AMS Accelerate.

> **Note**
>
> Si se alcanza el límite de 10 perfiles de instancia predeterminado, AMS aumenta el límite a 20 para poder adjuntar los perfiles de instancia necesarios.

## CloudWatch detalles del cambio de configuración

Detalles adicionales sobre la CloudWatch configuración.

- CloudWatch ubicación del archivo de configuración en la instancia:
  - Windows:%ProgramData%\ Amazon\AmazonCloudWatchAgent\ amazon-cloudwatch-agent .json

  - Linux:/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/ams-accelerate-config.json
- CloudWatch ubicación del archivo de configuración en Amazon S3:
  - Windows: https://ams-configuration-artifacts- *REGION_NAME* .s3. *REGION_NAME*.amazonaws.com/configurations/cloudwatch/latest/windows-cloudwatch-config.json
  - Linux: https://- .s3. ams-configuration-artifacts *REGION_NAME* *REGION_NAME*.amazonaws. com/configurations/cloudwatch/latest/linux-cloudwatch-config.json
- Métricas recopiladas:
  - Windows:
    - AWS Systems Manager Agente SSM (CPU_Usage)
    - CloudWatch Agente (CPU_Usage)
    - Utilización del espacio en disco para todos los discos (% de espacio libre)
    - Memoria (% de bytes comprometidos en uso)
  - Linux:
    - AWS Systems Manager Agente SSM (CPU_Usage)
    - CloudWatch Agente (CPU_Usage)
    - CPU (cpu_usage_idle, cpu_usage_iowait, cpu_usage_user, cpu_usage_system)
    - Disco (used_percent, inodes_used, inodes_total)
    - Diskio (io_time, write_bytes, read_bytes, escrituras, lecturas)
    - Mem (mem_used_percent)
    - Intercambio (swap_used_percent)
- Registros recopilados:
  - Windows:
    - Amazon SSMAgent Log
    - AmazonCloudWatchAgentLog
    - Amazon SSMError Log
    - AmazonCloudFormationLog
    - ApplicationEventLog
    - EC2ConfigServiceEventLog
    - MicrosoftWindowsAppLockerEXEAndDLLEventRegistro
    - MicrosoftWindowsAppLockerMSIAndScriptEventLog

- MicrosoftWindowsGroupPolicyOperationalEventLog
- SecurityEventLog
- SystemEventLog

- Linux:
  - /var/log/amazon/ssm/amazon-ssm-agent.log
  - /var/log/amazon/ssm/errors.log
  - /.log var/log/audit/audit
  - /-init-output.log var/log/cloud
  - /var/log/cloud-init.log
  - /var/log/cron
  - /var/log/dpkg.log
  - /var/log/maillog
  - /var/log/messages
  - /var/log/secure
  - /var/log/spooler
  - /var/log/syslog
  - /.log var/log/yum
  - /.log var/log/zypper

# Fuera de AMS Accelerate

AMS Accelerate proporciona una forma sencilla de operar un entorno operativo de clase empresarial. Además, AMS Accelerate proporciona el modelo de operaciones de infraestructura de apoyo para la AWS migración y el uso. Sin embargo, después de usar AMS Accelerate, puede decidir contratar a otros equipos o reasignar las responsabilidades de las operaciones de AWS infraestructura a otros equipos. Para ello, debe desvincular sus cuentas del servicio AMS.

Cuando cancelas una cuenta de AMS Accelerate, AMS te transfiere todas las responsabilidades definidas en la descripción de nuestro servicio. Por ejemplo, no podrás reducir los incidentes o las solicitudes de servicio a AMS. Del mismo modo, nuestros ingenieros de operaciones y de automatización dejarán de tener acceso a sus cuentas de Accelerate, lo que nos impedirá corregir los problemas de estado, disponibilidad y seguridad y conformidad. Sus AWS cargas de trabajo pueden seguir ejecutándose en las mismas cuentas en las que operaba AMS.

El equipo que se encargará de sus servicios de operaciones de infraestructura en el futuro debe estar incluido para definir qué personas, herramientas y procesos utilizará una vez que Accelerate deje de operar. AMS deja algunas de las herramientas de AMS, como las barandillas y los registros, para permitir el desarrollo de un entorno y un modelo operativos «futuros». Revisa detenidamente la siguiente documentación para entender las herramientas que puedes seguir utilizando y cómo solicitar la desactivación de una cuenta.

## AMS: acelera los efectos de desvinculación

Al prepararse para dejar de usar Accelerate, tenga en cuenta las siguientes consideraciones.

- Acceso: la `ams-access-management` CloudFormation pila que define la `ams-access-management` AWS Identity and Access Management función no se elimina. Tras la desvinculación, estos recursos permanecen, pero otros componentes que quedan atrás los utilizan. Puede eliminar la pila y el rol cuando lo desee.
- Retención de recursos de AMS: tras la desconexión, algunos recursos de AMS permanecen en tu cuenta. Para ver qué recursos se retienen y qué puede hacer con ellos, consulte la `resource_inventory.zip`hoja de cálculo (comprimida).
- Automatización: Tras la desconexión, los manuales de automatización de AWS SSM seleccionados por AMS y las funciones de AWS Lambda ya no están disponibles.
- Administración de copias de seguridad: AMS utiliza la administración de copias de seguridad para tomar instantáneas de sus recursos. Tras la desconexión, puede seguir utilizando los programas, la frecuencia y los períodos de retención de las copias de seguridad definidos en los planes AWS Backup de copia de seguridad de AMS; consulte. Seleccione un plan de respaldo de AMS Se eliminan los AWS Identity and Access Management recursos creados por AMS Backup Orchestrator, pero no los almacenes de backup creados por AMS ni la clave correspondiente. AWS KMS Accelerate ya no supervisa los trabajos de backup ni realiza acciones de restauración durante los incidentes.
- Optimización de costes: tras la desconexión, se elimina el programador de recursos de AMS. El programador de recursos de AMS le ayuda a reducir los costos operativos al detener los recursos que no están en uso y volver a ponerlos en marcha cuando se necesita su capacidad. AMS no sigue ofreciendo recomendaciones de optimización de costes. Para obtener más información sobre el programador de recursos, consulte Optimización de costos con el programador de recursos AMS.

- Expertos designados: tras la desvinculación, el administrador de prestación de servicios en la nube (CSDM) y el arquitecto de la nube (CA) designados dejarán de ofrecer orientación, informar sobre ellas ni impulsar la excelencia operativa y de seguridad en sus cuentas externas de Accelerate.
- Gestión de incidentes: la gestión de incidentes es el proceso que utiliza el servicio AMS para responder a los incidentes denunciados. Tras la desconexión, Accelerate ya no detecta los incidentes ni responde a ellos, ni ayuda a su equipo a resolver los problemas. No podrá intercambiar comunicaciones sobre incidentes y solicitudes de servicio con Accelerate y Accelerate desactivará el acceso a la consola de sus cuentas de Accelerate.
- Registro e informes: después de la desconexión, se conservan los registros almacenados como resultado de CloudWatch CloudTrail, y los registros de flujo de VPC. Puede dejar la configuración de esos servicios tal como están para seguir generando registros; sin embargo, AMS ya no supervisa dichas configuraciones. Accelerate ya no proporciona el informe de servicio mensual que resume las principales métricas de rendimiento de AMS. Usted conserva los datos generados por los informes de autoservicio (SSR) (consulteInformes de autoservicio), pero Accelerate no genera datos nuevos.
- Supervisión: la supervisión es el proceso que utiliza el servicio AMS para realizar un seguimiento de sus recursos. Durante la desconexión, AMS elimina las herramientas específicas de AMS, como el administrador de alarmas y el etiquetador de recursos, así como cualquier regla o alarma de EventBridge eventos que AMS haya implementado como parte de la línea base de monitoreo del AMS. CloudWatch Accelerate ya no responderá a las alarmas ni configurará otras nuevas tras la desconexión. Para obtener más información sobre el administrador de alarmas y el etiquetador de recursos, consulte el administrador de alarmas y el etiquetador de recursos basados en etiquetas.
- Herramientas de operaciones: AMS Accelerate puede proporcionar operaciones continuas para la infraestructura de su carga de trabajo en AWS. Tras cerrar una cuenta de Accelerate, ya no tendrá acceso a herramientas como Resource Tagger, que le ayudará a etiquetar sus recursos en función de las reglas, o a la configuración de instancias automatizada para instalar los agentes necesarios en sus instancias de EC2. CloudWatch y los agentes SSM de las instancias se mantienen en su lugar con las configuraciones existentes. El perfil de `AMSOSConfigurationCustomerInstanceRole` IAM y el `AMSInstanceProfileBasePolicy` se separan de sus instancias y se eliminan de sus cuentas de Accelerate.
- Administración de parches: la administración de parches es el proceso que utiliza el servicio AMS para actualizar las instancias de EC2. Tras la desconexión, AMS ya no crea una instantánea de la instancia antes de aplicar el parche, deja de instalar y monitorizar la instalación del parche y deja de notificarle el resultado. Conservas las líneas base y las instantáneas del parche creadas en el

pasado. Además, se mantiene la configuración de los períodos de mantenimiento de los parches, pero Accelerate ya no los instala.

- Gestión de problemas: una vez desactivado, Accelerate ya no realiza análisis para identificar e investigar los problemas ni para identificar la causa raíz.
- Seguridad: la gestión de la seguridad es el proceso que utiliza el servicio AMS para proteger sus recursos. Tras la salida, conservarás tu GuardDuty detector y tus hallazgos de Amazon, así como cualquier AWS Config regla que hayas creado. AWS Config se eliminan las reglas implementadas por Accelerate. Accelerate ya no supervisa, corrige ni informa sobre los hallazgos de estas herramientas.
- Fecha de finalización del servicio: la fecha de finalización del servicio es el último día del mes natural siguiente al final del período de preaviso de rescisión requerido de 30 días. Si el final del período de notificación de rescisión requerido cae después del día 20 del mes calendario, la fecha de finalización del servicio es el último día del mes calendario siguiente. Los siguientes son ejemplos de escenarios para las fechas de terminación.
  - Si el aviso de rescisión se proporciona el 12 de abril, el aviso de 30 días finaliza el 12 de mayo. La fecha de finalización del servicio es el 31 de mayo.
  - Si se proporciona un aviso de rescisión el 29 de abril, el aviso de 30 días finaliza el 29 de mayo. La fecha de finalización del servicio es el 30 de junio.

## Dejar de usar AMS Accelerate y depender de Alarm Manager y Resource Tagger

Las CloudFormation pilas personalizadas que implementan configuraciones relacionadas con Alarm Manager o Resource Tagger, junto con las pilas de configuración de Alarm Manager y Resource Tagger suministradas por AMS, permanecen en su cuenta cuando abandona AWS Managed Services.

Para eliminar las pilas de configuración de AMS durante el proceso de desvinculación, debe eliminar de las plantillas personalizadas todas las dependencias y referencias a Alarm Manager o Resource Tagger antes de iniciar el proceso de desvinculación. CloudFormation Eliminar las referencias ayuda a garantizar que las pilas se eliminen correctamente de tu cuenta cuando te desconectes de AMS.

> **Important**
>
> Revise detenidamente sus CloudFormation plantillas y elimine cualquier referencia a Alarm Manager y Resource Tagger antes de iniciar el proceso de exclusión. Si no lo hace, es

posible que estas pilas se conserven en su cuenta, incluso después de que se dé de baja de AMS. Ten en cuenta que, si bien estas pilas contienen información de configuración específica de Alarm Manager y Resource Tagger, su presencia no implica cargos ni comisiones continuas.

## Obtener asistencia para la desconexión de una cuenta de Accelerate

AMS cierra su cuenta después de recibir un aviso con al menos 30 días de antelación mediante una solicitud de cancelación del servicio de cuenta de AMS. La fecha de finalización del servicio es el último día del mes natural siguiente a la finalización del período de preaviso de rescisión obligatorio de 30 días; sin embargo, si el final del período de notificación de rescisión requerido cae después del día 20 del mes natural, la fecha de rescisión del servicio será el último día del mes natural siguiente.

Para solicitar la cancelación del embarque de una cuenta, debe:

1. Envíe una solicitud formal para cancelar la cuenta mediante una solicitud de servicio. Una solicitud de servicio (SR) en la que se documenten todas las cuentas que deseas cancelar o una SR por cuenta.

   En la solicitud, proporciona la lista de las cuentas IDs que deseas cancelar, el motivo de la cancelación y cualquier otra consideración adicional.
2. Informe a su CSDM sobre las cuentas que desea eliminar y solicite su ayuda para ejecutar el proceso de exclusión.

# Configuración de notificaciones en Accelerate

Las comunicaciones entre usted y AMS se producen por varios motivos:

- Eventos que se crean al monitorear las alertas
- Notificaciones del servicio de parches, si has activado el complemento Patch
- Solicitudes de servicio e informes de incidentes
- AWS Anuncios importantes ocasionales (su CSDM se pondrá en contacto con usted si es necesaria alguna acción por su parte)

Todas las notificaciones se envían mediante un correo electrónico que proporcionaste para las notificaciones de parches cuando te incorporaste. De lo contrario, las notificaciones se envían al

correo electrónico predeterminado que proporcionaste a AMS cuando te incorporaste. Como es difícil mantener actualizados los correos individuales, te recomendamos que utilices un correo de grupo que puedas actualizar por tu parte. El departamento de operaciones de AMS también recibe todas las notificaciones que se le envían y las analiza antes de responder.

Puedes usar listas de contactos con nombres para las notificaciones que no estén basadas en recursos, como las alertas basadas en GuardDuty o AWS Config. Por ejemplo, es posible que tengas una lista con un nombre `SecurityContacts` y otra con nombre`0perationsContacts`. AMS envía alarmas y notificaciones a estas listas.

Consulte AWS Config Informe de cumplimiento de controles para obtener más detalles.

# Etiquetado en AMS Accelerate

La mayoría de las funciones de Accelerate (aplicación de parches, copias de seguridad, supervisión) utilizan etiquetas y perfiles de configuración para decidir qué recursos gestionar, qué acciones aplicar y cuándo aplicarlas. Las etiquetas son etiquetas que se aplican a los recursos. Los perfiles de configuración contienen reglas basadas en esas etiquetas.

Cada función de Accelerate tiene sus propios requisitos de etiquetado. Algunas funciones requieren que utilices etiquetas específicas, mientras que otras te permiten usar cualquiera de las tuyas propias.

Para obtener información sobre las etiquetas obligatorias, consulteEtiquetas administradas por el cliente en Accelerate.

Para obtener información sobre las etiquetas que pueden definir los clientes, consulte Etiquetas proporcionadas por el cliente en Accelerate

Contenido


- Etiquetas en AMS Accelerate
  - ¿Qué son las etiquetas?
  - Cómo funciona el etiquetado
  - Etiquetas administradas por el cliente en Accelerate
    - Supervisión en Accelerate
    - Configuración de etiquetas para EC2 instancias en Accelerate
    - Administración de etiquetas para copias de seguridad en Accelerate
  - Acelere las etiquetas gestionadas
  - Etiquetas proporcionadas por el cliente en Accelerate
- Herramientas de administración de etiquetas para Accelerate
  - Acelere el etiquetador de recursos
    - ¿Qué es Resource Tagger?
    - Cómo funciona Resource Tagger
    - Perfiles de configuración del etiquetador de recursos en AMS Accelerate
      - Sintaxis y estructura
    - Casos de uso de Resource Tagger en AMS Accelerate

        - Visualización de las etiquetas aplicadas por Resource Tagger
        - Uso de Resource Tagger para crear etiquetas
        - Impedir que Resource Tagger modifique los recursos
        - Ejemplo de perfil de configuración
        - Fusión de la configuración predeterminada
        - Deshabilitar la configuración predeterminada
        - Eliminar las etiquetas aplicadas por Resource Tagger
        - Ver o realizar cambios en la configuración del etiquetador de recursos
        - Implementación de cambios de configuración
        - Configurar Terraform para ignorar las etiquetas de Resource Tagger
        - Visualización del número de recursos gestionados por Resource Tagger
    - Uso CloudFormation para crear etiquetas para AMS Accelerate
        - CloudFormation Casos de uso de AMS Accelerate
            - Etiquetar una EC2 instancia con CloudFormation for Accelerate
            - Etiquetar un AutoScaling grupo (ASG) con CloudFormation for Accelerate
            - Implementación de un perfil de configuración con CloudFormation for Accelerate
    - Uso de Terraform para crear etiquetas para AMS Accelerate


# Etiquetas en AMS Accelerate

Contenido


- ¿Qué son las etiquetas?
- Cómo funciona el etiquetado
- Etiquetas administradas por el cliente en Accelerate
    - Supervisión en Accelerate
    - Configuración de etiquetas para EC2 instancias en Accelerate
    - Administración de etiquetas para copias de seguridad en Accelerate
- Acelere las etiquetas gestionadas
- Etiquetas proporcionadas por el cliente en Accelerate

## ¿Qué son las etiquetas?

Una etiqueta es una etiqueta que se asigna a un AWS recurso. Cada etiqueta está formada por una clave y un valor opcional, ambos definidos por el usuario.

Las etiquetas se utilizan para clasificar AWS los recursos de diferentes maneras, por ejemplo, por propósito, propietario o entorno. Por ejemplo, puedes definir un conjunto de etiquetas para las EC2 instancias de Amazon de tu cuenta, lo que te ayudará a realizar un seguimiento del propietario y el nivel de pila de cada instancia.

Las etiquetas no tienen ningún significado semántico para Amazon EC2 y se interpretan estrictamente como una cadena de caracteres.

Para obtener más información, consulta los recursos de etiquetado. AWS

## Cómo funciona el etiquetado

Hay varias formas de aplicar etiquetas a los recursos. Puedes etiquetar los recursos directamente en la consola de cada AWS servicio al crear el recurso; usar el editor de AWS etiquetas para añadir, eliminar o editar las etiquetas de varios recursos; o utilizar herramientas de aprovisionamiento como la etiqueta de CloudFormation recursos. AMS Accelerate también incluye el etiquetador de recursos AMS Accelerate, que se utiliza para definir las reglas de un administrador automatizado del ciclo de vida de las etiquetas. Para obtener información sobre el uso del etiquetador de recursos en AMS Accelerate, consulte. Acelere el etiquetador de recursos AMS Accelerate también proporciona etiquetas proporcionadas por el cliente para añadir y eliminar etiquetas personalizadas en sus recursos de AMS. Para obtener más información sobre las etiquetas proporcionadas por el cliente, consulte. Etiquetas proporcionadas por el cliente en Accelerate

## Etiquetas administradas por el cliente en Accelerate

Algunas etiquetas son necesarias para activar varias acciones de AMS Accelerate.

Contenido

- Supervisión en Accelerate
- Configuración de etiquetas para EC2 instancias en Accelerate
- Administración de etiquetas para copias de seguridad en Accelerate

## Supervisión en Accelerate

AMS Accelerate monitorea los recursos compatibles para garantizar su estado, disponibilidad y confiabilidad. Para obtener más información sobre esta oferta de servicios, consulteSupervisión y gestión de eventos en AMS Accelerate.

AMS Accelerate incorpora periódicamente una monitorización adicional Servicios de AWS a la de referencia. Si utiliza la configuración predeterminada de Resource Tagger, estas actualizaciones se implementan automáticamente en sus cuentas y los cambios se reflejan en los recursos compatibles.

Para optar por que AMS Accelerate EC2 administre sus instancias de Amazon, debe aplicar la siguiente etiqueta a través del perfil de personalización en AppConfig; para obtener más información, consulte el paso 3: Crear una configuración y un perfil de configuración.

Aplique la siguiente etiqueta a sus recursos:

| Clave | Valor |
| --- | --- |
| ams:rt:ams-managed | true |

Por ejemplo, puede crear un documento de configuración personalizado como este para aplicar las etiquetas a todos los recursos compatibles con AMS: EC2

```
{
    "AWS::EC2::Instance": {
        "AllEC2": {
            "Enabled": true,
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Important**
>
> Recuerde implementar los cambios de configuración después de haberlos realizado. En SSM AppConfig, debe implementar una nueva versión de la configuración después de crearla.

Los servicios distintos de Amazon EC2 tendrán una supervisión de referencia predeterminada. Para optar por que AMS Accelerate no supervise sus recursos, puede utilizar el perfil de configuración personalizado para excluir recursos específicos o Servicios de AWS. Esto le permite controlar qué recursos deben tener etiquetas de supervisión para implementar las definiciones de alarma de referencia. Consulte Casos de uso de Resource Tagger en AMS Accelerate.

Uso de Resource Tagger

La configuración del etiquetador de recursos AMS Accelerate de su cuenta ayuda a garantizar que las siguientes etiquetas se implementen automáticamente, si aplica esta etiqueta (ams:rt:ams-managed).

Verá que las siguientes etiquetas se aplican a los recursos compatibles para la supervisión de referencia.

| Clave | Valor | Regla |
|---|---|---|
| ams:rt: ams-monitoring-policy | monitoreado por ams | Se aplica a todos los EC2 recursos compatibles con AMS |
| ams:rt: ams-monitoring-policy-platform | ams-monitored-linux | Se aplica a todas las EC2 instancias de Amazon que ejecutan el sistema operativo Linux |
| ams:rt: ams-monitoring-policy-platform | ams-monitored-windows | Se aplica a todas las EC2 instancias de Amazon que ejecutan el sistema operativo Windows |

Para otros servicios compatibles

Aplica las siguientes etiquetas a tus recursos, de acuerdo con las reglas indicadas:

| Clave | Valor | Regla |
| --- | --- | --- |
| ams:rt: ams-monitoring-policy | monitoreado por ams | Se aplica a todos los recursos compatibles con la monitoriz ación de AMS Accelerate. |
| ams:rt: ams-monitoring-with-kms | ams-monitored-with-kms | OpenSearch Dominio con KMS |
| ams:rt: ams-monitoring-with-master | ams-monitored-with-master | OpenSearch Dominio con nodo maestro dedicado |

Si no está utilizando Resource Tagger

Consulte Acelere las etiquetas sin el etiquetador de recursos para obtener ayuda sobre cómo aplicar las etiquetas de supervisión correctas mediante métodos distintos del AMS Resource Tagger.

## Configuración de etiquetas para EC2 instancias en Accelerate

AMS Accelerate administra los agentes en sus EC2 instancias de Amazon, como el agente SSM y el CloudWatch agente. Para obtener más información sobre esta oferta de servicios, consulte Configuración automatizada de instancias en AMS Accelerate

Para optar por que AMS Accelerate gestione tus EC2 instancias de Amazon, debes aplicar la siguiente etiqueta a tus EC2 instancias de Amazon:

| Clave | Valor |
| --- | --- |
| ams:rt:ams-managed | true |

## Administración de etiquetas para copias de seguridad en Accelerate

AMS Accelerate gestiona el respaldo de los recursos compatibles. Para obtener más información sobre esta oferta de servicios, consulteGestión de la continuidad en AMS Accelerate.

La administración de copias de seguridad de AMS Accelerate utiliza etiquetas para identificar los recursos de los que se debe realizar una copia de seguridad automática (y también ofrece funciones

de copia de seguridad manual). Puede usar cualquier combinación de etiqueta, clave y valor para asociar sus recursos a los planes de respaldo. Para optar por las copias de seguridad automatizadas mediante el ams-default-backup-plan AWS Backup plan, debe aplicar la siguiente etiqueta a los recursos compatibles:

| Clave | Valor |
| --- | --- |
| ams:rt:backup-orchestrator | true |

> **Note**
>
> Durante la incorporación, AMS Accelerate etiqueta todos los recursos con ams:rt: backup-orchestrator-onboarding con el valor true para las instantáneas con intervalos cortos y retención breves. Esto lo gestiona el plan de respaldo. ams-onboarding-backup-plan Para obtener más información sobre los AWS Backup planes gestionados por AMS Accelerate, consulte. Seleccione un plan de respaldo de AMS

## Acelere las etiquetas gestionadas

Durante la incorporación a AMS Accelerate, se desplegarán varios AWS recursos en su cuenta. Para que pueda identificarlos, estos recursos están etiquetados con lo siguiente:

| Clave | Valor |
| --- | --- |
| AMS: propietario del recurso | AMS |
| AMS: resourceOwnerService | Una descripción del servicio AMS Accelerate que ofrece este recurso proviene, por ejemplo, de AMS Deployment, Backup, Controls, Monitoring, Patch, etc. |
| AppId | AMSInfrastructure |
| AppName | |
| Entorno | |

> **Note**
>
> Estas etiquetas se aplican mediante etiquetas a CloudFormation nivel de pila y se basan en la CloudFormation propagación de las etiquetas a los recursos creados. Para obtener más información, consulte Etiqueta de recursos.

## Etiquetas proporcionadas por el cliente en Accelerate

¿Qué son las etiquetas proporcionadas por el cliente?

Las etiquetas proporcionadas por el cliente son una función del servicio AMS Accelerate que se utiliza para especificar las reglas que rigen la forma en que se etiquetan los recursos de AMS en su cuenta. Con las etiquetas proporcionadas por el cliente, puede añadir etiquetas personalizadas definidas por el usuario a los recursos de AMS desplegados en sus cuentas. La función de etiquetas proporcionadas por el cliente se añade automáticamente a las cuentas solicitadas cuando usted lo solicita a su administrador de prestación de servicios en la nube (CSDM) mediante un servicio automatizado. Ten en cuenta que no puedes anular las etiquetas AMS. Las etiquetas de AMS comienzan por «ams:».

Puede definir sus propias etiquetas (etiquetas) y especificar las funcionalidades de estas etiquetas para todos sus recursos de AMS Accelerate. Puede proporcionar estas etiquetas antes de incorporarlas a AMS para que las etiquetas AMS y sus etiquetas personalizadas se apliquen durante el proceso de incorporación. O bien, puedes proporcionar etiquetas después de la incorporación.

¿Cómo puedo añadir etiquetas proporcionadas por el cliente?

Para solicitar la adición de estas etiquetas a sus recursos, póngase en contacto con su CSDM. Estas etiquetas se aplicarán a los recursos de AMS de su cuenta.

¿Cuál es el alcance de las etiquetas?

Actualmente, esta función solo está disponible para los clientes de Accelerate y en las regiones AWS comerciales. Puede agregar etiquetas a todas las cuentas que posea o a una lista específica de cuentas.

> **Note**
>
> Estas etiquetas se aplican únicamente a los recursos de AMS y no afectan a los suyos propios.

# Herramientas de administración de etiquetas para Accelerate

Contenido


- Acelere el etiquetador de recursos
- Uso CloudFormation para crear etiquetas para AMS Accelerate
- Uso de Terraform para crear etiquetas para AMS Accelerate


## Acelere el etiquetador de recursos

Con Resource Tagger, puede especificar reglas que regulen la forma en que se etiquetan AWS los recursos en su cuenta. Al incorporar una cuenta, AMS Accelerate implementa su política de etiquetado para garantizar que los recursos de sus cuentas gestionadas estén etiquetados.

Contenido


- ¿Qué es Resource Tagger?
- Cómo funciona Resource Tagger
- Perfiles de configuración del etiquetador de recursos en AMS Accelerate
  - Sintaxis y estructura
- Casos de uso de Resource Tagger en AMS Accelerate
  - Visualización de las etiquetas aplicadas por Resource Tagger
  - Uso de Resource Tagger para crear etiquetas
  - Impedir que Resource Tagger modifique los recursos
  - Ejemplo de perfil de configuración
  - Fusión de la configuración predeterminada
  - Deshabilitar la configuración predeterminada
  - Eliminar las etiquetas aplicadas por Resource Tagger
  - Ver o realizar cambios en la configuración del etiquetador de recursos

- Implementación de cambios de configuración
- Configurar Terraform para ignorar las etiquetas de Resource Tagger
- Visualización del número de recursos gestionados por Resource Tagger

## ¿Qué es Resource Tagger?

Resource Tagger es un servicio de AMS Accelerate que le permite especificar reglas que rigen la forma en que se etiquetan AWS los recursos en su cuenta. Su objetivo es proporcionarle una visibilidad completa de cómo se aplican sus etiquetas a sus AWS recursos.

Resource Tagger crea, actualiza y elimina automáticamente las etiquetas de los AWS recursos compatibles, en función de las reglas de etiquetado que especifique en sus perfiles de configuración. Por ejemplo, puedes especificar una regla que aplique una etiqueta a una colección de EC2 instancias de Amazon e indique que deben ser gestionadas por AMS Accelerate, lo que hace que se supervisen o se hagan copias de seguridad de las instancias. Puede utilizar etiquetas como esta para identificar el estado de conformidad de los AWS recursos en función de la política definida en sus perfiles AWS AppConfig de configuración. Para obtener más información, consulte AWS AppConfig.

AMS Accelerate proporciona una configuración de etiquetado gestionado predeterminada para que AMS Accelerate supervise sus recursos. Usted define qué recursos debe gestionar AMS Accelerate y las reglas de etiquetado gestionado garantizan que AMS Accelerate supervise los recursos que tienen las etiquetas adecuadas.

Con Resource Tagger, si lo desea, puede anular o desactivar las etiquetas gestionadas por AMS Accelerate predeterminadas, establecer sus propias reglas de etiquetado para cumplir con sus políticas y utilizar otros mecanismos, como Terraform, para evitar desviaciones. Puede definir las excepciones para escalarlas en función de sus operaciones. Por ejemplo, puedes definir una política para aplicar etiquetas a todas las EC2 instancias de Amazon con plataformas compatibles (como Windows y Linux) y excluir del etiquetado una instancia IDs específica.

> **Important**
>
> Resource Tagger controla todas las etiquetas de tu cuenta que tienen el prefijo ams:rt:. Todas las etiquetas que comiencen con este prefijo se eliminan a menos que estén presentes en las reglas de configuración de Resource Tagger. En resumen, cualquier etiqueta de los recursos compatibles que comience por ams:rt: se considera propiedad de Resource Tagger. Si etiquetas algo manualmente con, por ejemplo, ams:rt:, esa etiqueta

se eliminará automáticamente si no se especificó en uno de los perfiles de configuración de Resource Tagger.

## Cómo funciona Resource Tagger

Cuando su cuenta se incorpora a AMS Accelerate, se implementan dos documentos de configuración JSON en su cuenta de. AWS AppConfig Los dos documentos, denominados perfiles de configuración, son AMSManagedetiquetas, denominadas perfil de configuración predeterminado y CustomerManagedTagsperfil de configuración de personalización. Utiliza el perfil de configuración de personalización para definir sus propias políticas y reglas para sus cuentas, y AMS Accelerate no las sobrescribe.

Ambos perfiles residen en la aplicación AMSResourceTagger y en el AMSInfrastructureentorno. Todas las etiquetas aplicadas por el etiquetador de recursos tienen el prefijo clave ams:rt:.

Perfil de configuración de personalización:

El perfil de configuración de personalización está vacío inicialmente en el momento de la incorporación de la cuenta; sin embargo, se aplican todas las reglas incluidas en el documento de perfil, además de las reglas del perfil de configuración predeterminado. Usted administra en su totalidad cualquier configuración del perfil de configuración de personalización y AMS Accelerate no la sobrescribe, excepto si así lo solicita usted.

Puede especificar las reglas de etiquetado personalizadas que desee en el perfil de configuración personalizado de los AWS recursos compatibles, y también puede especificar las modificaciones de la configuración predeterminada gestionada por AMS Accelerate aquí (consulte). Casos de uso de Resource Tagger en AMS Accelerate

**Important**

Si actualiza este perfil, el etiquetador de recursos aplicará automáticamente los cambios en todos los recursos relevantes del suyo. Cuenta de AWS Los cambios se implementan automáticamente, pero pueden tardar hasta 60 minutos en surtir efecto.

Puede actualizar este perfil mediante las Consola de administración de AWS herramientas AWS CLI/SDK o a través de ellas. Para obtener información sobre la actualización de un perfil de configuración de personalización, consulte la guía del AWS AppConfig usuario: ¿Qué es? AWS AppConfig

Perfil de configuración predeterminado:

El documento de perfil de configuración predeterminado es interno de AMS Accelerate y contiene las reglas predeterminadas proporcionadas por AMS Accelerate que no se pueden modificar ni eliminar permanentemente. AMS Accelerate puede actualizar este perfil en cualquier momento y ponerlo a su disposición para que lo revise; cualquier cambio que haya realizado en él se eliminará automáticamente. Si desea modificar o deshabilitar alguna de las reglas de configuración predeterminadas, utilice el perfil de configuración de personalización, consulteCasos de uso de Resource Tagger en AMS Accelerate.

## Perfiles de configuración del etiquetador de recursos en AMS Accelerate

Los perfiles de configuración ayudan a garantizar que las etiquetas se apliquen de manera uniforme a los recursos durante toda su vida útil.

Sintaxis y estructura

Un perfil de configuración es un objeto JSON con la siguiente estructura:

```
{
   "Options": {
      "ReadOnly": false
   },
   "ResourceType": {
      "ConfigurationID": {
      "Enabled": true,
      "Filter": { ... },
      "Tags": [  ...  ]
      },
      "ConfigurationID": {
      ...
      }
   },
   "ResourceType": {
     ...
   }
}
```

Opciones: (opcional) Especifique las opciones sobre cómo desea que se comporte. ResourceTagger Omitir el bloque equivale a configurar todas las opciones con sus valores predeterminados. Consulte a continuación los ajustes de opciones disponibles:

- ReadOnly: (opcional, el valor predeterminado es falso): especifica el ReadOnly modo del etiquetador de recursos. Configúrelo en true ReadOnly para deshabilitar la creación o eliminación de etiquetas de Resource Tagger en los recursos de AWS. Para obtener más información, consulte Impedir que Resource Tagger modifique los recursos.

ResourceType: Esta clave debe ser una de las siguientes cadenas admitidas y representa toda la configuración relacionada con el tipo de recurso indicado:

- AWS::AutoScaling::AutoScalingGrupo
- AWS::DynamoDB::Table
- AWS::EC2::Instance
- AWS::EC2::NatGateway
- AWS:EC2:: VPNConnection
- AWS::EFS::FileSystem
- AWS::EKS::Cluster
- AWS::ElasticLoadBalancing::LoadBalancer
- AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS::Elasticsearch::Domain
- AWS::FSx::FileSystem
- AWS::OpenSearch::Domain
- AWS: :RDS: DBCluster
- AWS: :RDS: DBInstance
- AWS::Redshift::Cluster
- AWS::S3::Bucket
- AWS::Synthetics::Canary

ID de configuración: esta clave debe ser única en el documento de perfil y debe dar un nombre exclusivo al siguiente bloque de configuración. Si dos bloques de configuración del mismo ResourceTypebloque tienen el mismo ID de configuración, surtirá efecto el que aparezca en último lugar en el perfil. Si especifica un ID de configuración en el perfil de personalización que sea el mismo que el especificado en el documento por defecto, surtirá efecto el bloque de configuración definido en el perfil de personalización.

> **Important**
>
> El ID de configuración debe ***not***superponerse al perfil AMS Accelerate; por ejemplo, no debe ser AMSMonitoringLinux o AMSMonitoringWindows; de lo contrario, deshabilita la configuración correspondiente del perfil de configuración de Tags. AMSManaged

Habilitado (opcional, el valor predeterminado es true): especifica si el bloque de configuración entra en vigor. Establézcalo en false para deshabilitar un bloque de configuración. Un bloque de configuración desactivado no tiene ningún efecto.

Filtro: especifica los recursos a los que se aplica la configuración. Cada objeto de filtro puede tener uno (pero solo uno) de los siguientes campos:

- AWS::AutoScaling::AutoScalingGrupo:
  - AutoScalingGroupName: El nombre del grupo de escalado automático. Este campo admite la coincidencia de caracteres comodín.
- AWS::DynamoDB::Table:
  - TableName: el nombre de la tabla de DynamoDB. Este campo admite la coincidencia de caracteres comodín.
- AWS::EC2::Instance:
  - AvailabilityZone: el filtro coincide con una EC2 instancia de la zona de disponibilidad especificada. Este campo admite la coincidencia de comodines, por lo que *a coincide con us-east-1a, ap-northeast-1a, etc.
  - InstanceId: El filtro hace coincidir una instancia con el ID de instancia especificado. EC2 Este campo admite la coincidencia de caracteres comodín, por lo que i-00000* coincidiría con cualquier instancia que tenga un ID de instancia que comience por i-00000.
  - Plataforma: el filtro hace coincidir una EC2 instancia con la plataforma especificada. Los valores válidos son Windows, Linux o el comodín * (para que coincidan con cualquier plataforma).
- AWS::EC2::NatGateway:
  - NatGatewayId: El ID de la puerta de enlace NAT. Este campo admite la coincidencia de caracteres comodín.
  - Estado: el estado de la puerta de enlace NAT (pendiente, fallido, disponible, borrado, eliminado o con el carácter comodín «*»)

  - VpcId: el ID de la VPC en la que reside la puerta de enlace NAT. Este campo admite la coincidencia de caracteres comodín.
  - SubnetId: el ID de la subred en la que reside la puerta de enlace NAT. Este campo admite la coincidencia de caracteres comodín
- AWS:EC2:: VPNConnection:
  - VpnConnectionId: El ID de la conexión. Este campo admite la coincidencia de caracteres comodín.
- AWS::EFS::FileSystem:
  - FileSystemId: el ID del sistema de archivos EFS. Este campo admite la coincidencia de caracteres comodín.
- AWS::EKS::Cluster:
  - ClusterName: el nombre del clúster. Este campo admite la coincidencia de caracteres comodín.
- AWS::ElasticLoadBalancing::LoadBalancer (Classic Load Balancer):
  - LoadBalancerName: El LoadBalancer nombre. Este campo admite la coincidencia de caracteres comodín.
  - Esquema: puede ser «orientado a Internet», «interno» o comodín «*».
  - VPCId: El campo VPCId en el que se despliega el balanceador de carga puede ser el comodín «*».
- AWS::ElasticLoadBalancingV2::LoadBalancer (Application Load Balancer (ALB)):
  - LoadBalancerArn: El nombre del recurso de LoadBalancer Amazon (ARN).
  - DNSName: El DNSName de. LoadBalancer Este campo admite la coincidencia de caracteres comodín.
  - LoadBalancerName: El LoadBalancer nombre. Este campo admite la coincidencia de caracteres comodín.
- AWS::Elasticsearch::Domain:
  - DomainId: El DomainId del ElasticSearch recurso. Este campo admite la coincidencia de caracteres comodín.
  - DomainName: El DomainName del ElasticSearch recurso. Este campo admite la coincidencia de caracteres comodín.
  - HasMasterNode: valor booleano verdadero o falso. Coincide si el dominio tiene un nodo maestro dedicado.

    - HasKmsKeyValor booleano verdadero o falso. Coincide si el dominio tiene una clave KMS para el cifrado en reposo.
- AWS::FSx::FileSystem:
    - FileSystemId: el ID del sistema de FSx archivos. Este campo admite la coincidencia de caracteres comodín.
- AWS::OpenSearch::Domain:
    - DomainId: El DomainId del OpenSearch recurso. Este campo admite la coincidencia de caracteres comodín.
    - DomainName: El DomainName del OpenSearch recurso. Este campo admite la coincidencia de caracteres comodín.
    - HasMasterNode: booleano; si el dominio tiene un nodo maestro dedicado, se puede establecer en verdadero.
    - HasKmsKey: Si el dominio tiene una clave KMS para el cifrado en reposo, se puede establecer en true.
- AWS: :RDS:: DBCluster
    - DBClusterIdentificador: el filtro hace coincidir un identificador de clúster de RDS con el identificador especificado. Este campo no admite la coincidencia de caracteres comodín, por lo que se debe especificar un identificador de clúster.
    - Motor: el motor que utiliza la instancia RDS. Este campo admite la coincidencia de caracteres comodín.
    - EngineVersion: La versión del motor. Este campo admite la coincidencia de caracteres comodín.
- AWS: :RDS:: DBInstance
    - DBInstanceIdentificador: el filtro hace coincidir una instancia de RDS con el ID de instancia especificado. Este campo no admite la coincidencia de caracteres comodín, por lo que se debe especificar un identificador de instancia.
    - Motor: el motor que utiliza la instancia RDS. Este campo admite la coincidencia de caracteres comodín.
    - EngineVersion: La versión del motor. Este campo admite la coincidencia de caracteres comodín.
- AWS::Redshift::Cluster:
    - ClusterIdentifier: el identificador del clúster. Este campo admite la coincidencia de caracteres comodín.
- AWS::S3::Bucket:

  - BucketName: el nombre del depósito de S3. Este campo admite la coincidencia de caracteres comodín.
- AWS::Synthetics::Canary:
  - CanaryName: El nombre del canario Synthetics.

Otras propiedades del filtro:

- Etiqueta: el filtro se aplica a cualquier recurso que ya tenga aplicada la etiqueta indicada. El valor de esta propiedad debe ser un objeto JSON con los siguientes campos:
  - Clave: debe ser una cadena exacta y especifica que los recursos deben tener una etiqueta con esa clave exacta.
  - Valor: especifica el valor coincidente de la etiqueta. Admite caracteres comodín, por lo que el valor de Sample coincide con cualquier valor que termine en la cadena Sample.
- Fn: :AND: matriz JSON de objetos JSON. Cada objeto sigue las mismas reglas que el bloque de configuración del filtro. Esto especifica que el filtro coincide con cualquier recurso que coincida con todos los subfiltros.
- Fn: :OR: Una matriz JSON de objetos JSON. Cada objeto sigue las mismas reglas que el bloque de configuración del filtro. Esto especifica que el filtro coincide con cualquier recurso que coincida con cualquiera de los subfiltros.
- Fn: :NOT: un objeto JSON que sigue las mismas reglas que el bloque de configuración del filtro. Esto especifica que el filtro no coincide explícitamente con ningún recurso que coincida con el subfiltro. Utilícelo para especificar las exclusiones de sus reglas de etiquetado.

Etiquetas: las etiquetas que se van a aplicar a los recursos coincidentes. (Consulte Convenciones de denominación y uso de las etiquetas). Este campo es una matriz de pares clave-valor:

- Clave: la clave de la etiqueta que se va a aplicar.
- Valor: el valor de la etiqueta que se va a aplicar.

> **Note**
>
> Las etiquetas que aplica Resource Tagger siempre tienen claves que comienzan por ams:rt:. Si no especificas este prefijo en tu perfil, Resource Tagger lo insertará automáticamente. Así

es como Resource Tagger distingue las etiquetas que posee y administra de las etiquetas utilizadas por otras herramientas para otros fines.

## Casos de uso de Resource Tagger en AMS Accelerate

En esta sección se enumeran las acciones que se realizan con más frecuencia con Resource Tagger.

### Visualización de las etiquetas aplicadas por Resource Tagger

Todas las etiquetas aplicadas por Resource Tagger tienen el key prefijo ams:rt:. Por ejemplo, la siguiente definición de etiqueta da como resultado una etiqueta con la clave ams:rt:SampleKey y el valor sampleValue. Todas las etiquetas con este prefijo se consideran parte de Resource Tagger.

```
{
 "Key": "sampleKey",
 "Value": "sampleValue"
}
```

**Important**

Si creas tu propia etiqueta manualmente con el prefijo ams:rt:, Resource Tagger la considerará gestionada. Esto significa que si el recurso lo administra Resource Tagger, pero los perfiles de configuración no indican que se deba aplicar la etiqueta, Resource Tagger eliminará la etiqueta agregada manualmente. Si etiqueta manualmente los recursos gestionados por Resource Tagger, no utilice el prefijo ams:rt: para etiquetar las claves.

### Uso de Resource Tagger para crear etiquetas

El etiquetador de recursos AMS Accelerate es un componente que se implementa en su cuenta durante la incorporación de AMS Accelerate. Resource Tagger tiene un conjunto de reglas configurables que definen cómo deben etiquetarse los recursos y, a continuación, hace cumplir esas reglas y agrega y elimina automáticamente etiquetas en los recursos para garantizar que cumplan con sus reglas.

Si desea utilizar el etiquetador de recursos para etiquetar sus recursos, consulte. Acelere el etiquetador de recursos

A continuación, se muestra un ejemplo de un fragmento de configuración de Resource Tagger que añade la etiqueta ams:rt:ams-managed con el valor true a todas las instancias de Amazon. EC2 La etiqueta ams:rt:ams-managed permite que AMS Accelerate supervise sus recursos.

```
{
    "AWS::EC2::Instance": {
        "SampleConfigurationBlock": {
            "Enabled": true,
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Warning**
>
> Tenga cuidado al especificar el nombre de la nueva configuración (`SampleConfigurationBlock`en el ejemplo proporcionado), ya que podría anular inadvertidamente la configuración gestionada por AMS con el mismo nombre.

Impedir que Resource Tagger modifique los recursos

El etiquetador de recursos se puede configurar en un modo de solo lectura, lo que impide añadir o eliminar etiquetas en los recursos. Esto resulta útil si desea proporcionar su propio mecanismo de etiquetado.

En el modo de solo lectura, Resource Tagger sigue examinando las reglas de etiquetado que se especifican en los perfiles de configuración gestionados y del cliente, y busca los recursos que no cumplen estas reglas de etiquetado. Aparece cualquier recurso que no cumpla con los requisitos. AWS Config Los Reglas de AWS Config que puede buscar tienen el `AMSResourceTagger-` prefijo. Por ejemplo, la `AMSResourceTagger-EC2Instance` AWS Config regla evalúa si se

crean las etiquetas adecuadas para `AWS::EC2::Instance` los recursos en función del perfil de configuración.

El etiquetador de recursos se detiene en este punto y no realiza ningún cambio en los recursos (no añade ni elimina etiquetas).

Puede activar el modo de solo lectura modificando el perfil de configuración del cliente para incluir la ReadOnlyclave en el bloque de opciones. Por ejemplo, el siguiente fragmento de perfil de configuración muestra cómo se vería esto:

```
{
    "Options": {
        "ReadOnly": true
    },
    "AWS::EC2::Instance": {
        [... the rest of your configuration ...]
    }
}
```

Resource Tagger reaccionaría ante esta nueva configuración en cuanto terminara de implementarse y dejaría de añadir y eliminar etiquetas en los recursos.

> **Note**
>
> Para volver a habilitar la modificación de etiquetas, cambie el ReadOnlyvalor a false o elimine la clave por completo, ya que el valor predeterminado es false.

Para obtener más información sobre la configuración de las opcionesSintaxis y estructura, consulte a continuación.

Ejemplo de perfil de configuración

El siguiente documento de perfil de ejemplo especifica que AMS Accelerate administre todas las EC2 instancias de Windows que forman parte de una CloudFormation pila de stack-*; sin embargo, excluye explícitamente una EC2 instancia concreta con el ID i-00000000000000001.

```
{
    "AWS::EC2::Instance": {
```

```
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "Windows"
                    },
                    {
                        "Tag": {
                            "Key": "aws:cloudformation:stack-name",
                            "Value": "stack-*"
                        }
                    },
                    {
                        "Fn::NOT": {
                            "InstanceId": "i-00000000000000001"
                        }
                    }
                ]
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Warning**
>
> Tenga cuidado al especificar el nombre de la nueva configuración (`SampleConfigurationBlock`en el ejemplo proporcionado), ya que podría anular inadvertidamente la configuración administrada por AMS con el mismo nombre.

### Fusión de la configuración predeterminada

AMS Accelerate proporciona el perfil de configuración predeterminado en el momento de la incorporación de la cuenta. Este perfil proporciona las reglas predeterminadas que se implementan en su cuenta.

Si bien no puede modificar el perfil de configuración predeterminado, puede anular los valores predeterminados especificando un bloque de configuración en el perfil de configuración de personalización con el mismo ID de configuración que el bloque de configuración predeterminado. Si lo hace, el bloque de configuración sobrescribe el bloque de configuración predeterminado.

Por ejemplo, considere el siguiente documento de configuración predeterminado:

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "Windows"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
  }
 }
}
```

Para cambiar el valor de la etiqueta que se aplica aquí de `SampleValueA` a `SampleValueB` y hacer que la etiqueta se aplique a todas las instancias, no solo a las de Windows, debe proporcionar el siguiente perfil de configuración de personalización:

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "*"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueB"
   }]
  }
 }
}
```

> **Important**
>
> Recuerde implementar los cambios de configuración después de haberlos realizado. Para obtener más información, consulte Implementación de cambios de configuración. En SSM AppConfig, debe implementar una nueva versión de la configuración después de crearla.

Deshabilitar la configuración predeterminada

Para deshabilitar una regla de configuración predeterminada, añada un bloque de configuración con el mismo ID de configuración a su perfil de configuración de personalización y asigne al campo Activado un valor de false.

Por ejemplo, si la siguiente configuración estuviera presente en el perfil de configuración predeterminado:

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "Windows"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
  }
 }
}
```

Puede deshabilitar esta regla de etiquetado si incluye lo siguiente en su perfil de configuración de personalización:

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": false
  }
 }
}
```

> **Important**
>
> Recuerde implementar los cambios de configuración después de haberlos realizado; para obtener más información, consulteImplementación de cambios de configuración. En SSM AppConfig, debe implementar una nueva versión de la configuración después de crearla.

Eliminar las etiquetas aplicadas por Resource Tagger

Resource Tagger elimina todas las etiquetas con el prefijo ams:rt si las etiquetas no existen en los perfiles de configuración o, si existen, si el filtro no coincide. Esto significa que puede eliminar las etiquetas aplicadas por Resource Tagger de una de las siguientes maneras:

- Modificar la sección de configuración de personalización que define la etiqueta.
- Añadir una excepción para los recursos específicos para que ya no coincidan con el filtro.

Por ejemplo: si una instancia de Linux tiene las siguientes etiquetas:

```
"Tags": [{
    "Key": "ams:rt:MyOwnTag",
    "Value": true
},{
    "Key": "myTag",
    "Value": true
}]
```

Y despliega el siguiente perfil de configuración de Resource Tagger:

```
{
    "AWS::EC2::Instance": {
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Platform": "Windows"
            },
            "Tags": [{
                "Key": "ams:rt:ams-managed",
                "Value": "true"
            }]
        }
```

```
    }
}
```

Resource Tagger reacciona a los nuevos cambios de configuración y la única etiqueta de la instancia es:

```
"Tags": [{
    "Key": "myTag",
    "Value": true
}]
```

> **Warning**
>
> Tenga cuidado al especificar el nombre de la nueva configuración (`SampleConfigurationBlock`en el ejemplo proporcionado), ya que podría anular inadvertidamente la configuración administrada por AMS con el mismo nombre.

> **Important**
>
> Recuerde implementar los cambios de configuración después de haberlos realizado; para obtener más información, consulte. Implementación de cambios de configuración En SSM AppConfig, debe implementar una nueva versión de la configuración después de crearla.

Ver o realizar cambios en la configuración del etiquetador de recursos

Los dos perfiles de configuración de JSON, AMSManagedTags y CustomerManagedTags, implementados en su cuenta en AWS AppConfig al incorporarse y residir en la aplicación AMSResource Tagger, y en el AMSInfrastructureentorno, se pueden revisar a través AppConfig de la GetConfigurationAPI.

El siguiente es un ejemplo de esta GetConfiguration llamada:

```
aws appconfig get-configuration
 --application AMSResourceTagger
 --environment AMSInfrastructure
 --configuration AMSManagedTags
 --client-id ANY_STRING
```

```
outfile.json
```

Aplicación: unidad AppConfig lógica para proporcionar capacidades, para el etiquetador de recursos, es el AMSResource etiquetador.

- Entorno:. AMSInfrastructure
- Configuración: para ver las definiciones de etiquetas predeterminadas de AMS Accelerate, el valor es AMSManaged Etiquetas, mientras que para ver las definiciones de etiquetas de clientes, el valor es CustomerManagedTags.
- ID de cliente: el identificador único de la instancia de la aplicación, que puede ser cualquier cadena.
- A continuación, las definiciones de etiquetas se pueden ver en el archivo de salida especificado, en este caso, outfile.json.

Luego, las definiciones de alarmas se pueden ver en el archivo de salida especificado, en este caso, outfile.json.

Para ver qué versión de la configuración está implementada en su cuenta, consulte las implementaciones anteriores en el entorno. AMSInfrastructure

Para anular las reglas de etiquetas:

Se puede anular cualquiera de las reglas de etiquetas existentes actualizando el perfil de personalización con la API de CloudFormation by, Implementación de un perfil de configuración con CloudFormation for Accelerate o directamente mediante AppConfig la API del usuario. CreateHostedConfigurationVersion Si se utiliza el mismo ID de configuración como regla de etiquetas de configuración predeterminada, se anula la regla predeterminada y se aplica la regla personalizada en su lugar.

Para implementar los cambios realizados en el documento: CustomerManagedTags

Después de realizar cambios en el perfil de configuración de personalización, debe implementar los cambios para ellos. Para implementar los nuevos cambios, AppConfig la StartDeploymentAPI debe ejecutarse mediante la AWS AppConfig consola o la CLI.

Implementación de cambios de configuración

Una vez completada la personalización, estos cambios se deben implementar a través de la AWS AppConfig StartDeploymentAPI. En las siguientes instrucciones se muestra cómo realizar la

implementación mediante AWS CLI. Además, puede utilizar el Consola de administración de AWS para realizar estos cambios. Para obtener más información, consulte el paso 5: Implementar una configuración.

```
aws appconfig start-deployment
--application-id <application_id>
--environment-id <environment_id>
--deployment-strategy-id <deployment_strategy_id>
--configuration-profile-id <configuration_profile_id>
--configuration-version 1
```

- ID de aplicación: el ID de aplicación del AMSResource etiquetador de aplicaciones. Consíguelo con la llamada a la ListApplicationsAPI.
- ID de entorno: el ID de entorno; consíguelo con la llamada a la ListEnvironmentsAPI.
- ID de la estrategia de despliegue: el ID de la estrategia de despliegue; consíguelo con la llamada a la ListDeploymentStrategiesAPI.
- ID del perfil de configuración: el ID del perfil de configuración de CustomerManagedTags; consíguelo con la llamada a la ListConfigurationProfilesAPI.
- Versión de configuración: la versión del perfil de configuración que pretende implementar.

> **Important**
>
> Resource Tagger aplica las etiquetas tal como se especifica en los perfiles de configuración. Cualquier modificación manual que realices (con la Consola de administración de AWS CloudWatch CLI o el SDK) en las etiquetas de recursos se revierte automáticamente, así que asegúrate de que los cambios estén definidos mediante Resource Tagger. Para saber qué etiquetas crea el etiquetador de recursos, busca las claves de etiquetas con el prefijo `ams:rt:`

Limite el acceso a la implementación con las acciones StartDeploymenty las de la StopDeploymentAPI a los usuarios de confianza que entiendan las responsabilidades y las consecuencias de implementar una nueva configuración en sus objetivos.

Para obtener más información sobre cómo usar AWS AppConfig las características para crear e implementar una configuración, consulte la documentación en Trabajar con AWS AppConfig.

### Configurar Terraform para ignorar las etiquetas de Resource Tagger

Si utilizas Terraform para aprovisionar tus recursos y quieres usar Resource Tagger para etiquetarlos, Terraform podría identificar las etiquetas Resource Tagger como Drift.

Puede configurar Terraform para que ignore todas las etiquetas de Resource Tagger mediante el bloque de configuración del ciclo de vida o el bloque de configuración global ignore_tags. Para obtener más información, consulte la documentación de Terraform sobre el etiquetado de recursos en Resource Tagging.

El siguiente ejemplo muestra cómo crear una configuración global para ignorar todas las etiquetas que comiencen por el prefijo de etiqueta Resource Tagger: `ams:rt:`

```
provider "aws" {
  # ... potentially other configuration ...

  ignore_tags {
    key_prefixes = ["ams:rt:"]
  }
}
```

### Visualización del número de recursos gestionados por Resource Tagger

Resource Tagger envía métricas cada hora a Amazon CloudWatch, en el `AMS/ResourceTagger` espacio de nombres. Las métricas se emiten solo para los tipos de recursos compatibles con Resource Tagger.

| Nombre de métrica | Dimensiones | Descripción |
|---|---|---|
| ResourceCount | Componente, ResourceType | Número de recursos (del tipo de recurso especificado) desplegados en esta región.<br><br>Unidades: recuento |
| ResourcesMissingManagedTags | Componente, ResourceType | Número de recursos (del tipo de recurso especificado) que requieren etiquetas administradas, según los perfiles de configuración, pero que Resource Tagger aún no los ha etiquetado. |

| Nombre de métrica | Dimensiones | Descripción |
| --- | --- | --- |
| | | Unidades: recuento |
| Unmanaged Resources | Componente, ResourceType | Número de recursos (del tipo de recurso especificado) a los que Resource Tagger no ha aplicado etiquetas administradas. Por lo general, estos recursos no coincidían con ningún bloque de configuración de Resource Tagger o se excluyen explícitamente de los bloques de configuración.<br><br>Unidades: recuento |
| MatchingResourceCount | Componente, ResourceType ConfigClauseName | Número de recursos (del tipo de recurso especificado) que coinciden con el bloque de configuración del etiquetador de recursos. Para que un recurso coincida con el bloque de configuración, el bloque debe estar habilitado y el recurso debe coincidir con el filtro del bloque.<br><br>Unidades: recuento |

Estas métricas también se pueden ver en forma de gráficos en el panel de control de informes de AMS-Resource-Tagger-Reporting. Para ver el panel, desde la consola de CloudWatch administración de Amazon, selecciona AMS-Resource-Tagger-Reporting-Dashboard. De forma predeterminada, los gráficos de este panel muestran los datos del período anterior de 12 horas.

AMS Accelerate despliega CloudWatch alarmas en su cuenta para detectar un aumento significativo en la cantidad de recursos no gestionados, por ejemplo, los recursos que AMS Resource Tagger excluye de la gestión. AMS Operations investigará los aumentos de recursos no gestionados que superen: tres recursos del mismo tipo o un aumento del 50% con respecto a todos los recursos del mismo tipo. Si el cambio no parece ser deliberado, AMS Operations podría ponerse en contacto con usted para revisar el cambio.

# Uso CloudFormation para crear etiquetas para AMS Accelerate

Puedes utilizarlas CloudFormation para aplicar etiquetas a nivel de pila (consulta la CloudFormation documentación, etiqueta de recursos) o a nivel de recurso individual (por ejemplo, consulta Etiquetar tus EC2 recursos de Amazon).

> **Important**
>
> Algunos componentes del servicio AMS Accelerate requieren etiquetas con el prefijo ams:rt:. Resource Tagger cree que es el propietario de estas etiquetas y las eliminará si ninguna regla de configuración de Resource Tagger lo permite. Siempre debe implementar un perfil de configuración de Resource Tagger para estas etiquetas, incluso si utiliza CloudFormation Terraform.

## CloudFormation Casos de uso de AMS Accelerate

En esta sección se enumeran las acciones que se realizan habitualmente con CloudFormation.

Temas

- Etiquetar una EC2 instancia con CloudFormation for Accelerate
- Etiquetar un AutoScaling grupo (ASG) con CloudFormation for Accelerate
- Implementación de un perfil de configuración con CloudFormation for Accelerate

### Etiquetar una EC2 instancia con CloudFormation for Accelerate

A continuación, se muestra un ejemplo de cómo puedes aplicar la etiqueta ams:rt:ams-managed con el valor true a una instancia de Amazon gestionada por. EC2 CloudFormation La etiqueta ams:rt:ams-managed permite que AMS Accelerate supervise sus recursos.

```
 Type: AWS::EC2::Instance

Properties:
  InstanceType: "t3.micro"

  # ...other properties...
```

```
  Tags:
    - Key: "ams:rt:ams-managed"
      Value: "true"
```

Etiquetar un AutoScaling grupo (ASG) con CloudFormation for Accelerate

El siguiente es un ejemplo de cómo puede aplicar la etiqueta ams:rt:ams-managed con el valor true a un grupo de Auto Scaling administrado por. CloudFormation Tenga en cuenta que el grupo Auto Scaling propagará sus etiquetas a EC2 las instancias de Amazon que cree. La etiqueta ams:rt:ams-managed permite que AMS Accelerate supervise sus recursos.

```
  Type: AWS::AutoScaling::AutoScalingGroup
Properties:
  AutoScalingGroupName: "SampleASG"

  # ...other properties...

  Tags:
    - Key: "ams:rt:ams-managed"
      Value: "true"
```

Implementación de un perfil de configuración con CloudFormation for Accelerate

Si desea implementar su perfil de `CustomerManagedTags` configuración mediante CloudFormation, puede usar las siguientes CloudFormation plantillas. Coloque la configuración JSON que desee en el `AMSResourceTaggerConfigurationVersion.Content` campo.

Al implementar las plantillas en una CloudFormation pila o conjunto de pilas, la implementación del `AMSResourceTaggerDeployment` recurso fallará si no se ha seguido el formato JSON requerido para la configuración. Consulte Sintaxis y estructura para obtener más información sobre el formato esperado.

Para obtener ayuda sobre cómo implementar estas plantillas como una CloudFormation pila o conjunto de pilas, consulta la AWS CloudFormation documentación correspondiente que aparece a continuación:

- Crear una pila en la AWS CloudFormation consola
- Crear una pila con AWS CLI
- Crear un conjunto de pilas

> **Note**
>
> Si despliega una versión de configuración mediante una de estas plantillas y, posteriormente, elimina la CloudFormation pila o el conjunto de pilas, la versión de configuración de la plantilla permanecerá como la versión implementada actualmente y no se realizará ningún despliegue adicional. Si desea volver a la configuración predeterminada, tendrá que implementar manualmente una configuración vacía (es decir, simplemente`{}`) o actualizar la pila a una configuración vacía, en lugar de eliminar la pila.

JSON

```
{
  "Description": "Custom configuration for the AMS Resource Tagger.",
  "Resources": {
    "AMSResourceTaggerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-CustomerManagedTags-
ProfileID"
        },
        "Content": "{\"Options\": {\"ReadOnly\": false}}",
        "ContentType": "application/json"
      }
    },
    "AMSResourceTaggerDeployment": {
      "Type": "AWS::AppConfig::Deployment",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-CustomerManagedTags-
ProfileID"
        },
        "ConfigurationVersion": {
          "Ref": "AMSResourceTaggerConfigurationVersion"
        },
```

```
        "DeploymentStrategyId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-Deployment-StrategyID"
        },
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-EnvironmentId"
        }
      }
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Resource Tagger.
Resources:
  AMSResourceTaggerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
      Content: |
        {
          "Options": {
            "ReadOnly": false
          }
        }
      ContentType: application/json
  AMSResourceTaggerDeployment:
    Type: AWS::AppConfig::Deployment
    Properties:
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
      ConfigurationVersion:
        !Ref AMSResourceTaggerConfigurationVersion
      DeploymentStrategyId:
        !ImportValue AMS-ResourceTagger-Configuration-Deployment-StrategyID
      EnvironmentId:
        !ImportValue AMS-ResourceTagger-Configuration-EnvironmentId
```

# Uso de Terraform para crear etiquetas para AMS Accelerate

Si no quiere usar AMS Accelerate Resource Tagger, puede aplicar sus propias etiquetas con Terraform. Sin embargo, si no quieres usar el etiquetador de recursos porque se aleja de las definiciones de Terraform, hay una forma de usar el etiquetador de recursos e ignorar la desviación que provoca; consulta. Configurar Terraform para ignorar las etiquetas de Resource Tagger

> **Important**
>
> Algunos componentes del servicio AMS Accelerate requieren etiquetas con el prefijo ams:rt:. Resource Tagger cree que es el propietario de estas etiquetas y las elimina si ninguna regla de configuración de Resource Tagger lo permite. Debe implementar un perfil de configuración de Resource Tagger para estas etiquetas, incluso si utiliza Terraform. CloudFormation

El siguiente es un ejemplo de cómo puedes aplicar la etiqueta ams:rt:ams-managed con el valor true a una instancia de Amazon gestionada por Terraform. EC2 La etiqueta ams:rt:ams-managed permite que AMS Accelerate supervise sus recursos.

```
  resource "aws_instance" "sample_linux_instance" {
    # ...ami and other properties...

    instance_type = "t3.micro"

    tags = {
        "ams:rt:ams-managed" = "true"
    }
}
```

El siguiente es un ejemplo de cómo puede aplicar la etiqueta ams:rt:ams-managed con el valor true a un grupo de Auto Scaling administrado por Terraform. Tenga en cuenta que el grupo Auto Scaling propaga sus etiquetas a las EC2 instancias de Amazon que crea. La etiqueta ams:rt:ams-managed permite que AMS Accelerate supervise sus recursos.

```
  resource "aws_autoscaling_group" "sample_asg" {
    # ...other properties...
```

```
    name = "terraform-sample"

    tags = {
        "ams:rt:ams-managed" = "true"
    }
}
```

Para obtener una descripción de cómo administrar las etiquetas de recursos creadas por Terraform, consulte. Configurar Terraform para ignorar las etiquetas de Resource Tagger

# Informes de incidentes, solicitudes de servicio y preguntas sobre facturación en AMS Accelerate

Con AMS Accelerate, puede solicitar ayuda con problemas y solicitudes operativas en cualquier momento a través del AWS Support Center del Consola de administración de AWS. Los ingenieros de operaciones de AMS Accelerate están disponibles para responder a sus incidentes y solicitudes de servicio round-the-clock, con acuerdos de nivel de servicio (SLAs) con plazos de respuesta para el servicio. Los ingenieros de operaciones de AMS Accelerate le notifican de forma proactiva las alertas y preguntas importantes mediante los mismos mecanismos.

AMS Accelerate ofrece una gama de servicios operativos para ayudarlo a alcanzar la excelencia operativa en AWS. Para comprender rápidamente cómo AMS ayuda a sus equipos a alcanzar la excelencia operativa general Nube de AWS con algunas de nuestras capacidades operativas clave, como el servicio de round-the-clock asistencia, la supervisión proactiva, la seguridad, la aplicación de parches, el registro y la copia de seguridad, consulte los diagramas de arquitectura de referencia de AMS.

Temas


- Gestión de incidentes en AMS Accelerate
- Gestión de solicitudes de servicio en Accelerate
- Pruebas de informes de incidentes y solicitudes de servicio en Accelerate
- Preguntas sobre facturación para AMS Accelerate


## Gestión de incidentes en AMS Accelerate

En AMS Accelerate, se utiliza AWS Support Center Consolepara presentar informes de incidentes. Los incidentes son problemas de Servicio de AWS rendimiento que afectan a su entorno gestionado, según lo determine AMS Accelerate o usted. Los incidentes identificados por el equipo de AMS Accelerate se reciben primero como eventos (un cambio en el estado del sistema registrado mediante la supervisión). Si se supera un umbral configurado, el evento activa una alarma, también denominada alerta. El equipo de operaciones de AMS Accelerate determina si el evento no ha tenido ningún impacto, si se trata de un incidente (una interrupción o degradación del servicio) o de un problema (la causa raíz subyacente de uno o más incidentes).

> **Note**
>
> El equipo de AMS Accelerate también recibe los incidentes creados por usted mediante programación mediante la API de AWS Support con el código de servicio. `service-ams-operations-report-incident`

Para obtener información sobre su uso Soporte, consulte Cómo empezar con. Soporte

## ¿Qué es la gestión de incidentes?

La gestión de incidentes es el proceso que utiliza AMS para registrar los incidentes activos, actuar en consecuencia, comunicar el progreso y notificar los incidentes activos.

El objetivo del proceso de gestión de incidentes es garantizar que el funcionamiento normal del servicio gestionado se restablezca lo antes posible, que se minimice el impacto empresarial y que todas las partes interesadas estén informadas.

Algunos ejemplos de incidentes incluyen (pero no se limitan a) la pérdida o la degradación de la conectividad de la red, un proceso o API que no responde o una tarea programada que no se está realizando (por ejemplo, una copia de seguridad fallida).

El siguiente gráfico muestra el flujo de trabajo de un incidente que usted notifique a AMS.

Este gráfico muestra el flujo de trabajo de un incidente que AMS le notifica.

### Prioridad de incidentes

Los incidentes creados en el centro de soporte de AWS, la consola o la API de soporte (SAPI) tienen clasificaciones diferentes a las de los incidentes creados en la consola AMS.

- Bajo: las funciones no críticas de su servicio o aplicación empresarial relacionadas con los recursos de AWS o AMS se ven afectadas.
- Medio: un servicio o una aplicación empresarial relacionados con los recursos de AWS and/or AMS se ve afectado moderadamente y funciona en un estado degradado.
- Alto: su empresa se ve afectada de forma significativa. Las funciones esenciales de su aplicación relacionadas con los recursos de AWS and/or AMS no están disponibles. Reservado para las interrupciones más críticas que afectan a los sistemas de producción.

> **Note**
>
> La consola de AWS Support ofrece cinco niveles de prioridad de incidentes que traducimos a los tres niveles de AMS.

## Cómo funcionan la respuesta y la resolución de incidentes

AMS Accelerate utiliza las mejores prácticas de gestión de incidentes de la gestión de servicios de TI (ITSM) para restablecer el servicio, cuando es necesario, lo más rápido posible.

Brindamos follow-the-sun asistencia las 24 horas del día, los 7 días de la semana, los 365 días del año a través de centros de operaciones de todo el mundo, con operadores especializados que vigilan activamente los paneles de control y las colas de incidentes.

Nuestros ingenieros de operaciones utilizan herramientas internas de seguimiento de incidentes para identificar, registrar, clasificar, priorizar, diagnosticar, resolver y cerrar incidentes; le proporcionamos actualizaciones sobre todas estas actividades a través del Centro de AWS soporte y la API de AWS soporte. Nuestros operadores utilizan una variedad de herramientas de AWS soporte interno para ayudar en todas esas actividades. Estos operadores están muy familiarizados con la infraestructura compatible con AMS Accelerate y tienen habilidades técnicas de nivel experto para abordar los problemas de soporte identificados. En caso de que nuestros operadores necesiten asistencia, los equipos de soporte y AWS servicio Premium están disponibles.

Una vez que el equipo de operaciones de AMS Accelerate reciba su incidente, validaremos la prioridad y la clasificación trabajando con usted si necesitamos alguna aclaración. Por ejemplo, si es mejor clasificar el informe del incidente como una solicitud de servicio, se reclasifica y el equipo de solicitudes de servicio de AMS Accelerate asume el control y se le notifica. Si el operador receptor puede resolver el incidente, se toman medidas para resolverlo rápidamente. Los operadores de AMS Accelerate consultan la documentación interna para encontrar una solución y, si es necesario, trasladan el incidente a otros recursos de soporte hasta que se resuelva. Una vez resuelto, el equipo de operaciones de AMS Accelerate documenta el incidente y la resolución para su uso futuro.

En los casos en que los incidentes de gravedad crítica estén afectando a sus cargas de trabajo críticas, AMS Accelerate puede recomendar la restauración de la infraestructura. Suele haber un equilibrio entre la solución de un problema y la simple restauración a partir de una copia de seguridad funcional conocida, y los riesgos e impactos derivados del tiempo de inactividad del servicio son los factores decisivos. Si dispone de tiempo para resolver problemas, AMS Accelerate le ayudará

y su gestor de prestación de servicios en la nube (CSDM) podría intervenir. Sin embargo, si la restauración es urgente, AMS Accelerate puede iniciar una restauración de inmediato.

## Trabajar con incidentes en AMS Accelerate

Desde AWS Support Center, puede realizar las siguientes tareas:

- Informe y actualice un incidente. Para denunciar un incidente de AMS Accelerate, seleccione AMS Operations: Report Incident en el menú Servicios.
- Obtenga una lista de todos los incidentes que haya enviado e información detallada sobre ellos.
- Limite la búsqueda de incidentes por estado y otros filtros.
- Añada comunicaciones y archivos adjuntos a sus incidentes y añada destinatarios de correo electrónico para la correspondencia entre casos.
- Inicie un chat en vivo o solicite que le devuelvan la llamada en relación con su incidente.

> **Note**
>
> La función de chat en vivo no es para eventos de seguridad; para problemas de seguridad, cree un caso de soporte de alta prioridad (P1 o P2).

- Resuelva los incidentes.
- Califica las comunicaciones sobre incidentes.

Los siguientes ejemplos describen el uso del Support Center para enviar un incidente. Una vez enviado, el equipo de AMS Accelerate trabajará con usted para resolver el incidente según el SLA estándar de AMS Accelerate.

### Enviar un incidente a Accelerate

Para informar de un incidente a través del Support Center, consulte la documentación de soporte: Creación de un caso de soporte

Para denunciar un incidente mediante el Soporte centro:

1. Haz clic en Crear caso. Se abre la página de creación de un caso de incidente.
2. Abra el menú de tipos de problema de soporte técnico y seleccione AMS Operations -- Report Incident. Proporcione información sobre el incidente y seleccione Crear.

3. Para mantenerse informado por correo electrónico en cada paso del proceso de resolución de incidentes, asegúrese de rellenar la opción CC Emails; si se conecta por federación, inicie sesión antes de seguir el enlace del correo electrónico que AMS Accelerate le envíe sobre el incidente.

> **Note**
>
> Incluya una descripción lo más detallada posible. Incluya la información pertinente de los recursos, junto con cualquier otra información que pudiera contribuir a entender el problema. Por ejemplo, para resolver los problemas de rendimiento, incluya marcas temporales y registros. Para solicitudes de características o preguntas de orientación general, incluya una descripción de su entorno y el propósito. En todos los casos, siga la guía de Descripción orientativa que aparece en el formulario de envío de caso.
> Si proporciona la máxima información posible, aumenta la probabilidad de que su caso se pueda resolver rápidamente.

También puede utilizar la API de AWS Support con el código de servicio `service-ams-operations-report-incident` para informar de un incidente.

## Supervisión y actualización de un incidente de Accelerate

Puede actualizar, supervisar y revisar los informes de incidentes y las solicitudes de servicio, ambos denominados casos, mediante Support Center o mediante programación mediante la operación Soporte API. `DescribeCases`

Para monitorear un caso, incidente o solicitud de servicio mediante el Soporte Centro, sigue estos pasos.

1. En la consola AWS de administración, vaya a Support.
2. En el panel de navegación de la izquierda, selecciona Tus casos de asistencia, busca un caso y selecciona el enlace Asunto para abrir una página de detalles con el estado actual y las correspondencias.

   Si desea utilizar el teléfono o el chat en este momento, haga clic en Abrir caso en Support Center para abrir la página Crear caso en el Soporte Centro, que se rellena automáticamente con el tipo de servicio AMS.

Cuando el equipo de operaciones de Accelerate actualiza un incidente o un caso de solicitud de servicio denunciado, recibirá un correo electrónico y un enlace al incidente en el Support Center para que pueda responder.

> **Note**
>
> No puede responder a la correspondencia sobre el caso respondiendo al correo electrónico.

Si hay muchos casos en el panel de control, puedes usar la opción de filtro:

- Asunto: utilice este filtro para buscar palabras clave relacionadas con el asunto del caso.
- Gravedad: utilice esta opción para filtrar los casos por gravedad seleccionando una gravedad de la lista.
- Tipo de caso: utilice esta opción para ver todos los casos de un tipo de caso concreto. Los incidentes y las solicitudes de servicio de Accelerate aparecen en el tipo de caso de Technical Support junto con cualquier caso específico del servicio.
- Estado: utilice esta opción para filtrar los casos por estado seleccionando un estado específico de la lista.

3. Para comprobar el estado más reciente, actualiza la página.
4. Si hay tantas correspondencias que no aparecen todas en la página, selecciona Cargar más.
5. Para actualizar el estado del caso, selecciona Responder, introduce la nueva correspondencia y, a continuación, selecciona Enviar.
6. Para cerrar el caso una vez que se haya resuelto satisfactoriamente, selecciona Cerrar caso.

   Asegúrese de calificar el servicio con una calificación de 1 a 5 estrellas para que AMS sepa cómo lo estamos haciendo.

## Gestión de incidentes de Accelerate con la API de soporte

Puedes usar la Soporte API para crear incidentes y añadir correspondencia con el Soporte personal durante la investigación de tus problemas. La Soporte API modela gran parte del comportamiento del AWS Support Center.

Para obtener información sobre cómo utilizar este servicio de AWS soporte, consulte Programming the Life of an AWS Support Case.

> **Note**
>
> El equipo de AMS Accelerate recibe las incidencias creadas por usted mediante programación mediante el código de servicio. `service-ams-operations-report-incident`

### Respuesta a un incidente generado por AMS Accelerate

AMS Accelerate monitorea sus recursos de forma proactiva. Para obtener más información, consulte Supervisión y gestión de eventos en AMS Accelerate . A veces, AMS Accelerate identifica y crea un incidente, la mayoría de las veces para notificarle un evento. Si es necesario que tomes medidas para resolver un incidente, el equipo de AMS Accelerate envía una notificación a la información de contacto que proporcionaste para la cuenta. Usted responde a esta notificación de la misma manera que a cualquier otro incidente, normalmente a través del Support Center, aunque en algunos casos es necesario ponerse en contacto por correo electrónico o por teléfono.

> **Important**
>
> Para recibir notificaciones de cambio de estado en relación con un incidente o una solicitud de servicio, introduce una dirección de correo electrónico en el campo de direcciones.

Vea el vídeo de Akshay para obtener más información (4:15)

## Gestión de solicitudes de servicio en Accelerate

Temas

- Cuándo utilizar una solicitud de servicio para Accelerate
- Cómo funciona la administración de solicitudes de servicio en Accelerate
- Crear una solicitud de servicio en Accelerate
- Supervisión y actualización de una solicitud de servicio para Accelerate
- Gestión de las solicitudes de servicio con la API de soporte de Accelerate

- Respuesta a una solicitud de servicio generada por AMS Accelerate

AMS Accelerate utiliza la gestión de solicitudes de servicio para registrar las solicitudes de servicio activas, tramitarlas, comunicarlas y notificarlas.

El objetivo del proceso de gestión de solicitudes de servicio es garantizar que su servicio gestionado le ofrezca lo que necesita.

Para consultas relacionadas con la facturación, cree una solicitud de servicio.

> **Note**
>
> El equipo de AMS Accelerate recibe las solicitudes de servicio creadas por usted mediante programación mediante la API de AWS Support con el código de servicio. `service-ams-operations-service-request`

Con el AWS Support Center, puede realizar las siguientes tareas:

- Informe y actualice una solicitud de servicio. Para una solicitud de servicio de AMS Accelerate, seleccione AMS Operation -- Service Request en el menú Servicios.
- Obtenga una lista de todas las solicitudes de servicio enviadas e información detallada sobre ellas.
- Limite la búsqueda de solicitudes de servicio por estado y otros filtros.
- Añada comunicaciones y archivos adjuntos a sus solicitudes y añada destinatarios de correo electrónico para la correspondencia entre casos.
- Resuelva las solicitudes de servicio.
- Califique las comunicaciones de solicitud de servicio.

## Cuándo utilizar una solicitud de servicio para Accelerate

Los siguientes ejemplos describen una solicitud de servicio. Tras enviar una solicitud de servicio, el equipo de AMS Accelerate trabajará con usted para resolver la solicitud según el SLA de AMS.

- AMS u orientación AWS general
- Preguntas relacionadas con Patch MW
- Preguntas relacionadas con el cronograma de Backup
- Preguntas sobre la funcionalidad de los AWS servicios

Los siguientes son ejemplos de lo que no debería plantearse en una solicitud de servicio:

- Problemas de acceso
- Fallo del parche
- Fallo de Backup

## Cómo funciona la administración de solicitudes de servicio en Accelerate

Las solicitudes de servicio son gestionadas por el equipo de operaciones de AMS Accelerate, que está de guardia.

Una vez que el equipo de operaciones de AMS Accelerate recibe su solicitud de servicio, la revisa para asegurarse de que está debidamente clasificada como solicitud de servicio o incidente. Si se reclasifica como incidente, se inicia el proceso de gestión de incidentes de AMS Accelerate y se te envía una notificación.

Si el operador de AMS Accelerate puede resolver la solicitud de servicio, se toman las medidas necesarias de inmediato. Por ejemplo, si la solicitud de servicio es para obtener asesoramiento sobre arquitectura u otro tipo de información, el operador le remite a los recursos adecuados o responde directamente a la pregunta.

Si el análisis de su solicitud de servicio identifica un error o una solicitud de función, AMS le envía una notificación a través de la solicitud de servicio. Como no hay una ETA para las solicitudes de funciones o las correcciones de errores, la solicitud de servicio original está cerrada. Póngase en contacto con su CSDM si tiene preguntas de seguimiento relacionadas con la solicitud de servicio original.

Si la solicitud de servicio está fuera del alcance de las operaciones de AMS Accelerate, el operador envía la solicitud a su gerente de prestación de servicios en la nube, para que pueda comunicarse con usted, o al equipo de AWS soporte correspondiente, junto con un correo electrónico indicándole las medidas que se están tomando.

La solicitud de servicio no se resuelve hasta que haya indicado que está satisfecho con el resultado.

> **Note**
>
> Le recomendamos que proporcione un correo electrónico de contacto, un nombre y un número de teléfono en todos los casos para facilitar las comunicaciones.

# Crear una solicitud de servicio en Accelerate

Para crear una solicitud de servicio, sigue estos pasos:

1. Desde la consola AMS Accelerate, vaya al panel de control.
2. Seleccione Abrir una solicitud de servicio y aparecerá preseleccionada la opción AMS: solicitud de servicio.
3. Elija una categoría.
4. Elige la gravedad (solo en los niveles Plus o Premium).
5. Introduzca la información de:
   - Asunto: un título descriptivo para la solicitud de servicio.
   - Descripción: una descripción completa de la solicitud de servicio, los sistemas afectados y el resultado esperado de la resolución.
6. Para añadir un adjunto, seleccione Adjuntar archivos, busque el adjunto que desee y pulse Abrir.

   Para eliminar el adjunto, selecciona el icono de borrado
7. Póngase en contacto con nosotros: la opción predeterminada es contactar con AMS a través de la web. Para seleccionar otras opciones:
   - Idioma de contacto preferido: el inglés es el idioma admitido para las solicitudes de servicio de AMS Accelerate.
   - Web: su solicitud de servicio se envía a través de la web y es gestionada por el equipo de operaciones de AMS.
   - Chat: chatee en línea con un representante de operaciones de AMS Accelerate. Esta opción lo añade a la cola de chat.
   - Teléfono: un representante de operaciones de AMS le devuelve la llamada. Introduzca su región, número de teléfono y extensión de AWS, si corresponde.
   - Contactos adicionales: introduzca cualquier dirección de correo electrónico adicional que desee copiar en su solicitud de servicio.
8. Seleccione Enviar.

   Se abre una página de detalles del caso con información sobre la solicitud de servicio, como el tipo, el asunto, la creación, el identificador y el estado. Además, hay un área de correspondencia que incluye la descripción de la solicitud que ha creado.

Para abrir un área de correspondencia y proporcionar detalles adicionales o actualizaciones de estado, selecciona Responder.

Una vez resuelta la solicitud de servicio, selecciona Resolver caso.

Si hay tantas correspondencias que no aparecen todas en la página, selecciona Cargar más.

Asegúrese de calificar el servicio con una calificación de 1 a 5 estrellas para que AMS sepa cómo lo estamos haciendo.

> **Note**
>
> Si va a probar la funcionalidad de la solicitud de servicio, le recomendamos que añada una señal de no acción al asunto de la solicitud de servicio, como por ejemplo. `AMSTestNoOpsActionRequired` A continuación, puede realizar la prueba sin iniciar el proceso de resolución de la solicitud de servicio.
> El equipo de AMS Accelerate recibe las solicitudes de servicio creadas por usted mediante programación mediante la API de AWS Support con el código de servicio. `service-ams-operations-service-request`

## Supervisión y actualización de una solicitud de servicio para Accelerate

Para supervisar un caso, incidente o solicitud de servicio mediante Soporte Center, sigue estos pasos.

1. En la consola AWS de administración, vaya a Support.
2. En la barra de navegación de la izquierda, selecciona Tus casos de asistencia, busca un caso y selecciona el enlace Asunto para abrir una página de detalles con el estado actual y las correspondencias.

   Si desea utilizar el teléfono o el chat en este momento, haga clic en Abrir caso en Support Center para abrir la página Crear caso en el Soporte Centro, que se rellena automáticamente con el tipo de servicio AMS.

Cuando el equipo de operaciones de Accelerate actualiza un incidente o un caso de solicitud de servicio denunciado, recibirá un correo electrónico y un enlace al incidente en el Support Center para que pueda responder.

> **Note**
>
> No puede responder a la correspondencia sobre el caso respondiendo al correo electrónico.

Si hay muchos casos en el panel de control, puedes usar la opción de filtro:

- Asunto: utilice este filtro para buscar palabras clave relacionadas con el asunto del caso.
- Gravedad: utilice esta opción para filtrar los casos por gravedad seleccionando una gravedad de la lista.
- Tipo de caso: utilice esta opción para ver todos los casos de un tipo de caso concreto. Los incidentes y las solicitudes de servicio de Accelerate aparecen en el tipo de caso de Technical Support junto con cualquier caso específico del servicio.
- Estado: utilice esta opción para filtrar los casos por estado seleccionando un estado específico de la lista.

3. Para comprobar el estado más reciente, actualiza la página.
4. Si hay tantas correspondencias que no aparecen todas en la página, selecciona Cargar más.
5. Para actualizar el estado del caso, selecciona Responder, introduce la nueva correspondencia y, a continuación, selecciona Enviar.
6. Para cerrar el caso una vez que se haya resuelto satisfactoriamente, selecciona Cerrar caso.

   Asegúrese de calificar el servicio con una calificación de 1 a 5 estrellas para que AMS sepa cómo lo estamos haciendo.

## Gestión de las solicitudes de servicio con la API de soporte de Accelerate

Puede usar la API AWS Support para crear solicitudes de servicio y agregarles correspondencia durante las investigaciones de sus problemas y las interacciones con el personal de AWS soporte. La API de AWS soporte modela gran parte del comportamiento del AWS Support Center.

El equipo de AMS también recibe las solicitudes de servicio creadas por usted mediante programación mediante la API de AWS Support con el código service-ams-operations-service de servicio -request.

Para obtener más información sobre cómo puede utilizar este servicio de AWS soporte, consulte Programming the Life of an AWS Support Case.

## Respuesta a una solicitud de servicio generada por AMS Accelerate

AMS Accelerate supervisa sus recursos de forma proactiva; para obtener más información, consulte. Supervisión y gestión de eventos en AMS Accelerate A veces, AMS Accelerate crea una solicitud de servicio o una notificación de servicio para usted, normalmente si es necesaria una acción por su parte para resolver una solicitud de servicio. En ese caso, el equipo de AMS Accelerate envía una notificación al contacto que has indicado para la cuenta. Usted responde a esta solicitud de servicio de la misma manera que en cualquier otro caso, normalmente a través del Support Center, aunque en algunos casos se requiere correspondencia por correo electrónico o teléfono.

> **Important**
>
> Para recibir notificaciones de cambios de estado en relación con una solicitud de servicio o un incidente, debe haber introducido una dirección de correo electrónico en el campo de direcciones. Las notificaciones se envían únicamente a la dirección de correo electrónico que se agregó al caso cuando se creó.

El enlace del correo electrónico de notificación solo funciona si utiliza un servidor de correo electrónico en su red federada AMS Accelerate. De lo contrario, puede responder a la correspondencia accediendo a su consola AMS Accelerate y utilizando la página de detalles del caso.

> **Note**
>
> AMS Accelerate envía las comunicaciones a la dirección de correo electrónico principal de tu AWS cuenta; te recomendamos añadir un alias de correo electrónico de contacto de operaciones alternativo para facilitar el proceso request/notification de gestión del servicio. Esto se explica durante el proceso de incorporación de AMS Accelerate y en la documentación de incorporación correspondiente.

# Pruebas de informes de incidentes y solicitudes de servicio en Accelerate

Al probar los informes de incidentes o las solicitudes de servicio, te pedimos que lo incluyas AMSTestNoOpsActionRequireden el asunto. Esto permite a AMS saber que el incidente o la solicitud son únicamente para realizar pruebas. Cuando los ingenieros de operaciones de AMS lo vean, no responderán de ninguna manera.

# Preguntas sobre facturación para AMS Accelerate

Para enviar una pregunta relacionada con la facturación, complete los siguientes pasos:

1. Abre el AWS Support Centro en casa#/. https://console.aws.amazon.com/support/
2. Selecciona Cuenta y facturación.

3. Seleccione Crear caso.

4. Selecciona Cuenta y facturación y, a continuación, sigue las instrucciones para enviar tu caso.

# Administración de eventos planificados en AWS Managed Services

La gestión de eventos planificados (PEM) de AWS Managed Services (AMS) es una oferta de servicios de AMS. PEM interactúa, coordina y ayuda durante los eventos y proyectos de los clientes mediante los servicios de AMS. El PEM ayuda a coordinar un conjunto de actividades relacionadas que se alinean con el alcance y el cronograma acordados del evento o proyecto del PEM.

## Criterios AMS PEM

Un evento planificado es un proyecto con un alcance y un plazo determinados. AMS utiliza los detalles que usted proporciona (incluidos el plan y el alcance, los resultados esperados y los cambios que se espera que realicen las operaciones de AMS) para ayudarlo de manera eficaz durante la actividad de PEM. Luego, sus arquitectos de nube (CAs) revisan y evalúan la actividad de PEM para comprobar su integridad, implementación técnica y participación en las operaciones de AMS. Tras la revisión de CA, AMS Operations revisa los planes y coordina con su gerente de prestación de servicios en la nube (CSDM) la participación del equipo de operaciones.

## Tipos de PEM

Los tipos de PEM disponibles son los siguientes:

- Días de juego
  - Operational Gameday: un enfoque de juego basado en escenarios para la respuesta operativa, destinado a validar la integración de procesos, personas y sistemas.
  - Security Gameday: estrategia de respuesta a incidentes de seguridad que emplea un enfoque de juego basado en escenarios para evaluar la integración de los sistemas, los procesos y el personal.
- Evento de seguridad para el cliente: eventos de seguridad planificados. Por ejemplo, pruebas de penetración.
- Migration Support: Soporte para la actividad planificada de incorporación y migración.

Este flujo de trabajo facilita la colaboración con AMS para coordinar los eventos planificados y las actividades de migración relacionadas con el soporte de AMS. Para obtener ayuda con sus requisitos específicos, póngase en contacto con su CSDM.

# El proceso AMS PEM

El proceso PEM consta de las siguientes fases:

- Inicio del PEM: trabajas con tu CSDM para definir el objetivo del evento planificado y determinar qué es lo que AMS Operations necesita. Los AMS CAs revisan los aspectos técnicos del plan PEM. CAs Trabajan con AMS Security and Operations en materia de cumplimiento, optimización de la ejecución y automatización, y en la definición de las tareas y los resultados previos a la ejecución del PEM. A continuación, su CSDM crea el ticket de PEM y proporciona a AMS la información del proyecto y los detalles técnicos. El AMS requiere un plazo de 14 días naturales para que el equipo de operaciones del AMS tenga tiempo de planificar, realizar una revisión técnica y asignar los recursos.
- Revisión de la PEM: el equipo de operaciones de AMS revisa la solicitud de PEM y trabaja con su CSDM para comprobar que la información del plan de PEM es correcta y completa.
- Aceptación del PEM: AMS revisa la información proporcionada y comunica al CSDM cuál será el nivel de apoyo durante la actividad del PEM. Si el PEM contiene información completa y su CSDM está de acuerdo con el alcance del trabajo, se aprueba el PEM.
- Preparación y ejecución: AMS se asegura de que se completen las tareas necesarias antes de que comience el PEM y facilita la comunicación interna y con los clientes. AMS se asegura de que el plan PEM funcione correctamente y proporciona informes de estado y progreso.

# PEM FAQs

¿Cómo interactúo con AMS mediante casos: solicitud de servicio (SRs) o incidente durante un evento de PEM?

- Utilice el ID de PEM compartido por su CSDM en la línea de RFC/SR asunto del formato. *`PEM-ID`*

  Cuando proceda, puede utilizar la opción de contacto en vivo.
- También puede crear una solicitud de servicio (SR) para analizar sus casos de uso o para responder a preguntas sobre el evento planificado. Si utilizas un SR, el PEM no tiene por qué ser válido.

¿Qué validaciones se realizan cuando se presenta un caso relacionado con el PEM?

- Verificación de que el identificador de cuenta figura en el PEM.

- Verificación de que el estado de PEM esté aprobado y activo entre las fechas de inicio y finalización indicadas.
- Se proporciona internamente a los ingenieros de AMS un enlace a los detalles del PEM.

¿Existen solicitudes de PEM SLAs o SLOs para solicitarlas?

- PEMs no están asociados a SLAs o. SLOs
- SLAs y en SLOs el caso del PEM, los elementos de trabajo relacionados con el PEM (solicitud de servicio, incidentes) los define AMS. SLOs

  Para obtener más información, consulte los informes de incidentes, las solicitudes de servicio y las preguntas sobre facturación en AMS Accelerate.

¿Podemos crear un PEM a través de una solicitud de servicio (SR)?

- No, la creación del PEM debe gestionarla el administrador de prestación de servicios en la nube (CSDM).

# Operaciones bajo demanda

Operations on Demand (OOD) es una función de AWS Managed Services (AMS) que amplía el alcance estándar de su plan de operaciones de AMS al proporcionar servicios operativos que actualmente no ofrecen de forma nativa los planes de operaciones de AMS o AWS. Una vez seleccionada, la oferta del catálogo se ofrece mediante una combinación de automatización y recursos de AMS altamente cualificados. No hay compromisos a largo plazo ni contratos adicionales, lo que le permite ampliar su AMS, sus AWS operaciones y capacidades actuales según sea necesario. Aceptas comprar bloques de horas (bloques OOD), 20 horas por bloque, mensualmente.

Puede seleccionar una oferta del catálogo estandarizada e iniciar una nueva contratación de OOD mediante una solicitud de servicio. Algunos ejemplos de ofertas de OOD incluyen la asistencia con el mantenimiento de Amazon EKS, las operaciones y la AWS Control Tower administración de los clústeres de SAP. Las nuevas ofertas de catálogo se añaden periódicamente en función de la demanda y de los casos de uso operativo que vemos con más frecuencia.

El OOD está disponible para los planes de operaciones AMS Advanced y AMS Accelerate y está disponible en todos los Regiones de AWSlugares donde AMS esté disponible.

AMS gestiona los riesgos de seguridad del cliente (CSRM) mientras implementa los cambios solicitados. Para obtener más información sobre el proceso de CSRM, consulte las revisiones de seguridad de las solicitudes de cambio.

Catálogo de ofertas de Operations on Demand

Operations on Demand (OOD) le ofrece los servicios que se describen en la siguiente tabla.

> **Note**
>
> Para obtener las definiciones de los términos clave, consulte los términos clave de la documentación de AWS Managed Services.

| Plan de operaciones | Title (Título) | Descripción | Resultados esperados |
|---|---|---|---|

| | | | |
|---|---|---|---|
| AMS Advanced y AMS Accelerate | Mantenimiento del clúster de Amazon EKS | AMS libera a sus desarrolladores de contenedores al gestionar el mantenimiento continuo de las implementaciones de Amazon Elastic Kubernetes Service (Amazon EKS). AMS lleva a cabo los end-to-end procedimientos necesarios para actualizar un clúster abordando los component es del plano de control, los complementos y los nodos. AMS realiza la actualización de los tipos de nodos gestionados, así como de un conjunto seleccionado de complementos de Amazon EKS y Kubernetes. | Los equipos de clientes ayudaron con las operacion es subyacentes de actualización de los clústeres de Amazon EKS. |

| | | | |
|---|---|---|---|
| AMS Accelerate | Edificio AMI y máquinas expendedoras | AMS proporciona una gestión continua de la construcción y venta de AMI para los clientes.<br><br>Nuestros ingenieros publican mensualmente las AMI suscritas, publican AMI bajo demanda para las actividades de aplicación de parches emergentes, gestionan los cambios mediante manuales de ejecución y supervisan las compilaciones de las AMI mediante la supervisión. CloudWatch También ofrecemos asistencia para la solución de problemas e informes detallados sobre todas las AMI utilizadas en las cuentas designadas. Esta oferta requiere que las canalizaciones de compilación de AMI se implement en mediante el generador de imágenes de EC2. AMS no admite ningún otro servicio o automatiz ación que interactúe con el generador de imágenes de EC2. | La postura de seguridad de los clientes mejoró y se redujo el tiempo que los clientes dedicaban a construir y vender. AMIs |

| | | | |
|---|---|---|---|
| AMS Accelerate | Ejecución de cambios selecta | Trabaje con nuestros expertos ingenieros de operaciones para traducir los requisitos de su empresa en solicitudes de cambio validadas que puedan ejecutars e de forma segura en su AWS entorno. Aproveche nuestro enfoque único de automatización y nuestro conocimiento de las mejores prácticas operativas (por ejemplo, la evaluación del impacto, las anulaciones o la regla de dos personas), tanto si se trata de un simple cambio a gran escala como de una acción compleja con repercusiones posteriores. | Los clientes ayudaron a definir, crear y ejecutar las solicitud es de cambio personalizadas. Los cambios pueden ser manuales o automáticos (CloudFormation, SSM). Incluye consultas con nosotros Soporte para obtener orientación sobre la configura ción cuando sea necesario. No está diseñado para cambios en el código de la aplicación, la instalación o implementación de la aplicación, la migración de datos o los cambios en la configuración del sistema operativo. |

| | | | |
|---|---|---|---|
| AMS Accelerate | AWS Network Firewall Operaciones | AMS colabora con usted para integrar su firewall e implementar y administrar las políticas y reglas para las operaciones continuas del firewall. Para ello, nuestros ingenieros aprovechan nuestras mejores prácticas operativas y la automatización para configurar políticas y reglas estandarizadas, y permiten la supervisión para detectar los cambios realizados fuera del proceso de automatización. AMS le notifica rápidamente los cambios no deseados y le ofrece opciones para incluirlos, si así lo solicita, o restaurar la cuenta a una configuración anterior para garantizar la estabilidad general de sus sistemas. | Los equipos de clientes ayudaron a reducir la sobrecarga de administración al detectar rápidamente los cambios involuntarios en el firewall de la red, lo que mejoró la resolución de incidentes y redujo el tiempo de análisis de la causa raíz de los problemas esperados e imprevistos. |
| AMS Accelerate | AWS Control Tower operaciones | Operaciones y administración continuas de su zona de AWS Control Tower aterrizaje, incluida AWS Transit Gateway, que proporciona una solución integral de zona de aterrizaje. AWS Organizations Nos encargamos de la venta de cuentas, la gestión de los SCP y las unidades organizativas, la corrección de los errores de tráfico, la gestión de los usuarios del SSO y AWS Control Tower las actualizaciones con nuestra biblioteca de controles y barandas personalizados. | Los equipos de clientes ayudaron con algunas de las operaciones subyacentes de administración AWS Control Tower de AWS Transit Gateway y AWS Organizations. |

| | | | |
|---|---|---|---|
| AMS Accelerate | AWS landing zone Acelera las operaciones | AMS ofrece operaciones continuas en las zonas de AWS aterrizaje desplegadas a través del AWS Landing Zone Accelerator (LZA).<br><br>Nuestros ingenieros se encargan de los cambios en los archivos de configuración, AWS Control Tower de la gestión del entorno (venta de cuentas, creación de unidades organizativas, barreras de control de los sistemas de control de servicios (SCP), de la detección y corrección de desviaciones de los sistemas de TC, de la gestión de la configuración de la red y de las actualizaciones de CT y del marco LZA. AWS LZA proporcio na un medio para configurar y gobernar un AWS entorno seguro y multicuenta utilizando las mejores prácticas y servicios operativos, tales como: AWS Control Tower | Los equipos de clientes ayudaron con las operacion es continuas y la administración de la solución AWS Landing Zone Accelerator. |

| | | | |
|---|---|---|---|
| AMS Accelerate | SAP Cluster Assist | Alarmas, monitorización, parches de clústeres, copias de seguridad y solución de incidentes dedicados a sus clústeres de SAP. Este elemento del catálogo le permite delegar parte del trabajo operativo continuo de su equipo de operaciones de SAP para que pueda centrarse en la gestión de la capacidad y el ajuste del rendimiento. | Los equipos de SAP, clientes o socios, ayudaron con algunas de las operaciones subyacentes. Aún así, requiere que el cliente proporcione otras capacidades de SAP, como la administración de la capacidad, el ajuste del rendimiento, la administración de bases de datos y la administración de bases de SAP. |
| AMS Advanced | Ejecución prioritaria de RFC | Capacidad de ingeniero de operaciones designada por AMS para priorizar la ejecución de sus solicitudes de cambio (RFC). Todos los envíos reciben un mayor nivel de respuesta y el orden de prioridad se puede ajustar interactuando directamente con los ingenieros a través de una sala de reuniones de Amazon Chime. | Los clientes reciben un SLO de respuesta de 8 horas durante. RFCs |

| | | | |
|---|---|---|---|
| AMS Advanced y AMS Accelerate | Actualización del sistema operativo anterior | Evite la migración de instancias actualizándolas a una versión de sistema operativo compatible. Podemos realizar una actualización in situ en las instancias seleccionadas aprovechando la automatización y las capacidades de actualización de los proveedores de software (por ejemplo, Microsoft Windows 2008 R2 a Microsoft Windows 2012 R2). Este enfoque es ideal para las aplicaciones heredadas que no se pueden volver a instalar fácilmente en una nueva instancia y proporciona protección adicional contra las amenazas de seguridad conocidas y sin paliativos en las versiones anteriores del sistema operativo.<br><br>Se admiten los siguientes sistemas operativos para las actualizaciones locales:<br><br>• Microsoft Windows 2012 R2 a Microsoft Windows 2016 y versiones posteriores<br>• Microsoft Windows 2016 a Microsoft Windows 2022 y versiones posteriores<br>• De Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8<br>• De Red Hat Enterprise Linux 8 a Red Hat Enterprise Linux 9<br>• De Oracle Linux 7 a Oracle Linux 8 | Esta solución se proporciona para aplicaciones que ya no se pueden volver a instalar en una instancia nueva (por ejemplo, si se pierde el código fuente, si el ISV deja de funcionar, etc.). Puede devolver las actualizaciones fallidas a su estado original. Desde un punto de vista operativo, se prefiere la reversión, ya que permite que la instancia quede en un estado más compatible con los últimos parches de seguridad. |

Temas


- Solicitar AMS Operations On Demand
- Realizar cambios en las ofertas de Operations on Demand


# Solicitar AMS Operations On Demand

Las operaciones bajo demanda (OOD) de AWS Managed Services (AMS) están disponibles para todos los Cuentas de AWS usuarios que se hayan incorporado a AMS. Para aprovechar las ventajas de Operations on Demand, solicite información adicional a su administrador de prestación de servicios en la nube (CSDM), arquitecto de soluciones (SA), administrador de cuentas o arquitecto de nube (CA). Las ofertas de OOD disponibles figuran en la tabla anterior del catálogo de ofertas de Operations on Demand. Una vez finalizado el análisis del alcance de la contratación, envíe una solicitud de servicio a AMS Operations para iniciar la contratación de OOD.

Cada solicitud de servicio de OOD debe contener la siguiente información detallada relativa a la contratación:

- Las ofertas de OOD específicas solicitadas y para cada oferta de OOD específica:
  - El número de bloques (un bloque equivale a 20 horas de recursos operativos en un mes natural determinado, que se cobrarán según la tarifa estándar vigente en AWS ese momento para la oferta de operaciones bajo demanda aplicable) que se van a asignar a la oferta de OOD específica.
  - El ID de cuenta de cada cuenta de AWS Managed Services para la que se solicita la oferta de OOD específica.

Debe enviar las solicitudes de servicio de OOD a través de uno de los siguientes medios:

- La cuenta de AWS Managed Services que recibe las ofertas de Operations on Demand correspondientes, o
- Una cuenta de AWS Managed Services que es una cuenta AWS Organizations de administración en el modo de todas las funciones, en nombre de cualquiera de sus cuentas de miembros que sean cuentas de AWS Managed Services.

Una vez recibida la solicitud de servicio OOD, AMS Operations revisa y actualiza las cuentas con su aprobación, aprobación parcial o denegación.

Una vez aprobada la solicitud de servicio que ofrece OOD, AMS y usted se coordinan para iniciar la contratación. No se inicia ninguna oferta de OOD hasta que se apruebe la solicitud de servicio y se acuerde una fecha de inicio de la contratación.

AMS utiliza una asignación de suscripción mensual de bloques de OOD. Asignamos mensualmente el número aprobado de bloques, a partir de la fecha de inicio de la contratación, hasta que solicites la exclusión mediante una nueva solicitud de servicio. Los bloques OOD son válidos durante un mes natural. Los bloques no utilizados, o las partes de bloques, no se acumulan ni se trasladan a futuros meses.

Se le facturará un mínimo de un bloque de OOD cada mes, independientemente de la cantidad de horas realmente utilizadas. No se facturará ningún bloque de OOD adicional asignado en el que no se hayan utilizado horas.

## Realizar cambios en las ofertas de Operations on Demand

Para solicitar cambios en las contrataciones continuas de las ofertas de Operations on Demand (OOD), envíe una solicitud de servicio que contenga la siguiente información:

- Las modificaciones que se solicitan y
- La fecha solicitada para que las modificaciones entren en vigor.

Tras recibir la solicitud de servicio OOD, AMS Operations la revisa y la actualiza con su aprobación, o bien solicita al CSDM asignado que colabore con usted para determinar el alcance y las implicaciones de la modificación. Si se determina que la modificación requiere un esfuerzo de análisis con el CSDM, debe enviar una segunda solicitud de servicio de OOD para iniciar la contratación modificada una vez finalizado el ejercicio de análisis.

Una vez aprobada, la asignación de bloques modificada más recientemente pasará a estar activa y permanecerá activa, sustituyendo cualquier asignación de bloques anterior, a menos que usted y usted acuerden lo contrario. AWS

# Informes y opciones

AWS Managed Services (AMS) recopila datos de varios servicios nativos de AWS para proporcionar informes con valor añadido sobre las principales ofertas de AMS.

AMS ofrece dos tipos de informes detallados:

- Informes a pedido: puede solicitar determinados informes ad hoc a través de su Cloud Service Delivery Manager (CSDM). Estos informes no tienen un límite porque es posible que tengas que solicitarlos varias veces durante la fase de incorporación o en algún momento crítico. Sin embargo, ten en cuenta que estos informes no están diseñados para proporcionarse siguiendo un cronograma, como los informes semanales. Para comprender mejor sus necesidades o para obtener más información sobre el uso de los informes de autoservicio, póngase en contacto con su CSDM.
- Informes de autoservicio: los informes de autoservicio de AMS le permiten consultar y analizar datos directamente con la frecuencia que necesite. Utilice los informes de autoservicio para acceder a los informes desde la consola AMS y genere informes sobre los conjuntos de datos mediante grupos de S3 (un grupo por cuenta). Esto le permite integrar los datos en su herramienta de inteligencia empresarial (BI) favorita para poder personalizar los informes según sus necesidades.

Temas


- Informes a petición
- Informes de autoservicio


# Informes a petición

Temas


- Informes de gestión de hosts de AMS
- Informes de AMS Backup
- AWS Config Informe de cumplimiento de controles
- Informe de configuración de respuesta de AMS Config Rules
- Informes de Top Talkers prevenidos y seguimiento
- Informe de detalles de cargos de facturación

- Informes de Trusted Remediator

AMS recopila datos de varios servicios nativos de AWS para proporcionar informes de valor añadido sobre las principales ofertas de AMS. Para obtener una copia de estos informes, solicite a su administrador de prestación de servicios en la nube (CSDM).

## Informes de gestión de hosts de AMS

Informes disponibles

- Informe de cobertura de SSM Agent

### Informe de cobertura de SSM Agent

El informe de cobertura del agente SSM de AMS le informa si las EC2 instancias de la cuenta tienen el agente SSM instalado o no.

| Nombre del campo | Definición |
|---|---|
| Nombre del cliente | Nombre del cliente para situaciones en las que hay varios subclientes |
| Región de recursos | AWS Región donde se encuentra el recurso |
| Nombre de cuenta | El nombre de la cuenta |
| AWS ID de cuenta | El ID de la AWS cuenta |
| ID de recurso | ID de la EC2 instancia |
| Nombre del recurso | Nombre de la EC2 instancia |
| Bandera compatible | Indica si el recurso tiene el agente SSM instalado («compatible») o no («NO CUMPLE») |

## Informes de AMS Backup

Informes disponibles

- Informe de éxito o fracaso de Backup Job
- Informe resumido de Backup
- Summary/Coverage Informe de Backup

## Informe de éxito o fracaso de Backup Job

El Success/Failure informe Backup Job proporciona información sobre las copias de seguridad ejecutadas en las últimas semanas. Para personalizar el informe, especifique el número de semanas durante las que desea recuperar los datos. El número predeterminado de semanas es 12. En la siguiente tabla se enumeran los datos incluidos en el informe:

| Nombre del campo | Definición |
| --- | --- |
| ID de la cuenta de AWS | ID de cuenta de AWS a la que pertenece el recurso |
| Nombre de la cuenta | Nombre de la cuenta de AWS |
| ID de trabajo de Backup | El ID del trabajo de Backup |
| ID de recurso | El ID del recurso del que se ha hecho una copia de seguridad |
| Tipo de recurso | El tipo de recurso del que se está haciendo una copia de seguridad |
| Región de recursos | La AWS región del recurso respaldado |
| Estado de Backup | El estado de la copia de seguridad. Para obtener más información, consulte Estados de los trabajos de Backup |
| ID del punto de recuperación | El identificador único del punto de recuperación |
| Mensaje de estado | Descripción de los errores o advertencias que se produjeron durante el trabajo de copia de seguridad |
| Tamaño del Backup | Tamaño de la copia de seguridad en GB |

| Nombre del campo | Definición |
| --- | --- |
| Punto de recuperación ARN | El ARN de la copia de seguridad creada |
| Antigüedad del punto de recuperación en días | Número de días transcurridos desde que se creó el punto de recuperación |
| Hace menos de 30 días | Indicador de copias de seguridad con menos de 30 días |

## Informe resumido de Backup

| Nombre del campo | Definición |
| --- | --- |
| Nombre del cliente | Nombre del cliente para situaciones en las que hay varios subclientes |
| Mes del Backup | Mes de la copia de seguridad |
| Año de Backup | Año de la copia de seguridad |
| Tipo de recurso | El tipo de recurso del que se está haciendo la copia de seguridad |
| Número de recursos | La cantidad de recursos de los que se hizo una copia de seguridad |
| Número de puntos de recuperación | Número de instantáneas distintas |
| Copias de seguridad con menos de 30 días | El recuento de copias de seguridad que tienen menos de 30 días |
| Antigüedad máxima de los puntos de recuperación | El punto de recuperación más antiguo en días |
| Edad mínima de puntos de recuperación | Edad del punto de recuperación más reciente en días |

### Summary/Coverage Informe de Backup

El Summary/Coverage informe Backup indica cuántos recursos no están protegidos actualmente por ningún AWS Backup plan. Hable con su CDSM sobre un plan adecuado para aumentar la cobertura, siempre que sea posible, y reducir el riesgo de pérdida de datos.

| Nombre del campo | Definición |
|---|---|
| Nombre del cliente | Nombre del cliente para situaciones en las que hay varios subclientes |
| Región | AWS región donde se encuentra el recurso |
| Nombre de cuenta | El nombre de la cuenta |
| AWS ID de cuenta | El ID de la AWS cuenta |
| Tipo de recurso | Tipo del recurso. Los recursos son compatibl es con AWS Backup (Aurora, DocumentDB, DynamoDB, EBS, EC2 EFS, RDS y S3) FSx |
| ARN de recurso | ARN del recurso |
| ID de recurso | ID del recurso |
| Cobertura | Indica si el recurso está cubierto o no («CUBIERTO» o «NOT_COVERED») |
| Número de recursos | Número de recursos compatibles en la cuenta |
| perc_coverage | Porcentaje de recursos compatibles con una copia de seguridad ejecutada en los últimos 30 días. |

## AWS Config Informe de cumplimiento de controles

El informe AWS Config Control Compliance proporciona una visión detallada del cumplimiento de los recursos y las AWS Config reglas de las cuentas AMS. Filtra el informe por la gravedad de las reglas

de Config para priorizar los hallazgos más importantes. En la siguiente tabla se enumeran los datos proporcionados por este informe:

| campo | Descripción |
| --- | --- |
| Date | Fecha del informe |
| Nombre del cliente | Nombre del cliente |
| AWS ID de cuenta | ID AWS de cuenta asociada al cliente |
| Identificador de origen | AWS Config identificador de fuente único de la regla |
| Descripción de la regla | AWS Config descripción de la regla |
| Tipo de regla | AWS Config tipo de regla |
| Indicador de conformidad | AWS Config estado de cumplimiento de la regla |
| Tipo de recurso | AWS tipo de recurso |
| Nombre del recurso | AWS nombre del recurso |
| Gravedad | Gravedad recomendada predeterminada definida por AMS para la AWS Config regla |
| Categoría de remediación | Categoría de respuesta de remediación asociada a una regla AWS Config |
| Descripción de la remediación | Explicación de la acción correctiva para garantizar que AWS Config la regla sea compatible |
| Acción del cliente | El cliente debe tomar las medidas necesarias para que la AWS Config regla sea conforme |
| Informe de métricas de Delta | Cambios relacionados con el cumplimiento de una regla entre dos fechas determinadas |

# Informe de configuración de respuesta de AMS Config Rules

El informe de configuración de respuesta de las reglas de configuración de AMS Config ofrece una visión detallada de cómo Accelerate está configurado actualmente para responder a las reglas de configuración de AMS que no cumplen con las normas. Para obtener más información sobre cómo cambiar la respuesta de las reglas de configuración de AMS, consulte AMS Accelerate Customized findings & response.

Este informe solo muestra las configuraciones que ha cambiado y excluye las configuraciones predeterminadas de AMS que aparecen en la biblioteca de reglas de configuración de AMS. El informe proporciona datos sobre los recursos y la configuración de respuesta a las reglas de configuración de AMS de las cuentas de AMS, incluidos los siguientes:

- La lista de AWS cuentas para las que ha cambiado la respuesta predeterminada para las reglas de configuración de AMS.
- La lista de etiquetas a las que ha asociado una respuesta para las reglas de configuración de AMS.
- La lista de configuraciones de respuesta para cada regla, cuenta y etiqueta.
- La lista de recursos para los que ha cambiado la respuesta predeterminada para las reglas de configuración de AMS.

## Informe de configuraciones de respuesta más reciente

| campo | Descripción |
| --- | --- |
| Date | Fecha en la que se generó el informe |
| Nombre del cliente | Nombre del cliente |
| AWS ID de cuenta | El ID de AWS cuenta asociado a la configura ción |
| Nombre de la cuenta | AWS nombre de cuenta del grupo de recursos a nivel de cuenta |
| Tipo de búsqueda | Tipo de hallazgo identificado. En este caso, AWS Config |

| campo | Descripción |
| --- | --- |
| Identificador de fuente | AWS Config Identificador de fuente único de la regla |
| ID de grupo de recursos | El ID del grupo de recursos asociado a la configuración de respuesta |
| Acción de respuesta configurada | Tipo de acción desencadenado por AMS |
| SSM Runbook Associate | El manual de remediación que se ejecutará, si lo hay |
| Tipo de grupo de recursos | Puede ser una cuenta o una etiqueta |

## Recursos con respuesta predeterminada personalizada de Config Rules

| Nombre del campo | Definición |
| --- | --- |
| Nombre del cliente | Nombre del cliente |
| Date | Fecha en la que se generó el informe |
| AWS Nombre de la cuenta | AWS nombre de cuenta |
| ID de cuenta | ID AWS de cuenta asociada |
| Regla de configuración AMS | Regla de configuración de AMS que apunta al recurso y se aplica con una configuración |
| Resource ID (ID de recurso) | El ID de recurso de la cuenta de cliente a la que se dirige la regla de configuración de AMS |
| Región de recursos | La AWS región en la que se aplica la configura ción |
| Tipo de recurso | AWS tipo de recurso |

| Nombre del campo | Definición |
| --- | --- |
| ID de grupo de recursos | El ID del grupo de recursos asociado a la configuración de respuesta |
| Indicador AMS del recurso | Si AMS despliega el AWS recurso, este campo se establece en `True` |
| Tipo de disparador | El tipo de respuesta configurado para el recurso |
| Indicador de conformidad | Estado de cumplimiento de las reglas de configuración de AMS |

## Informes de Top Talkers prevenidos y seguimiento

Informes disponibles

- Informe de incidentes evitados
- Monitoreando el informe de Top Talkers

### Informe de incidentes evitados

El informe Incidentes prevenidos enumera las CloudWatch alarmas de Amazon que se corrigieron automáticamente, lo que evitó un posible incidente. Para obtener más información, consulte Corrección automática. En la siguiente tabla se muestra la información incluida en este informe:

| Nombre del campo | Definición |
| --- | --- |
| execution_start_time_utc | Fecha en la que se ejecutó la automatización |
| customer_name | Nombre del cliente de la cuenta |
| account_name | El nombre de la cuenta |
| AwsAccountId | El ID de la cuenta de AWS |

| Nombre del campo | Definición |
| --- | --- |
| nombre_documento | El nombre del documento SSM o de la automatización ejecutada |
| duración_en_minutos | La duración de la automatización en minutos |
| Región | AWS Región en la que se encuentra el recurso |
| automation_execution_id | El ID de la ejecución |
| automation_execution_status | El estado de la ejecución |

## Monitoreando el informe de Top Talkers

El informe Monitoring Top Talkers presenta el número de CloudWatch alertas de Amazon generadas durante un período de tiempo específico y proporciona visualizaciones de los recursos que generan el mayor número de alertas. Este informe le ayuda a identificar los recursos que generan el mayor número de alertas. Estos recursos pueden ser adecuados para realizar un análisis de la causa raíz a fin de solucionar el problema o para modificar los umbrales de alarma a fin de evitar que se activen innecesariamente cuando no se trata de un problema real. En la siguiente tabla se muestra la información incluida en este informe:

| Nombre del campo | Definición |
| --- | --- |
| Nombre del cliente | Nombre del cliente |
| AccountId | El ID de la AWS cuenta |
| Categoría de alerta | El tipo de alerta que se ha activado |
| Descripción | Descripción de la alerta |
| ID de recurso | ID del recurso que activó la alerta |
| Nombre del recurso | Nombre del recurso que activó la alerta |
| Región | AWS Región en la que se encuentra el recurso |

| Nombre del campo | Definición |
| --- | --- |
| Estado del incidente | Estado más reciente del incidente generado por la alarma |
| Primera aparición | La primera vez que se activó la alerta |
| Incidencia reciente | La última vez que se activó la alerta |
| Recuento de alertas | Número de alertas generadas entre la primera aparición y la reciente |

## Informe de detalles de cargos de facturación

El informe de detalles de los cargos de facturación de AWS Managed Services (AMS) proporciona detalles sobre los cargos de facturación de AMS con las cuentas vinculadas y los servicios de AWS correspondientes, que incluyen:

- Cargos a nivel de servicio de AMS, porcentajes de aumento, niveles de servicio de AMS a nivel de cuenta y tarifas de AMS.
- Cuentas vinculadas y cargos AWS por uso

| Nombre del campo | Definición |
| --- | --- |
| Mes de facturación | El mes y el año del servicio facturado |
| ID de la cuenta del pagador | El identificador de 12 dígitos que identifica la cuenta que será responsable de pagar los cargos de AMS |
| ID de cuenta vinculada | El identificador de 12 dígitos que identifica la cuenta AMS que consume los servicios que generan gastos |
| AWS Nombre del servicio | El AWS servicio que se utilizó |

| Nombre del campo | Definición |
| --- | --- |
| AWS Cargos | Los AWS cargos del nombre del AWS servicio que figuran en el nombre del AWS servicio |
| Plan de precios | El nombre del plan de precios asociado a la cuenta vinculada |
| Aumenta la proporción | El porcentaje de aumento (expresado en V.WXYZ decimal) basado en pricing_plan, SLA y el servicio de AWS |
| Cargos ajustados AWS | AWS uso ajustado para AMS |
| Aumento de los cargos de AWS | El porcentaje de cargos de AWS que se cobrará por AMS; adjusted_aws_charges * uplift_percent |
| EC2 Instancias gastadas por RDS | Invierta en instancias EC2 de RDS |
| Cargos de AMS | Cargos totales de AMS del producto: uplifted_ aws_charges + instance_ec2_rds_spend + uplifted_ris + uplifted_sp |
| Tarifa mínima prorrateada | El importe que cobramos para cumplir con el mínimo contractual |
| Tarifa mínima | Tarifas mínimas de AMS (si corresponde) |
| Cargos totales de AMS por cuenta vinculada | Suma de todos los cargos de la linked_account |
| Cargos totales de AMS de la cuenta del pagador | Suma de todos los cargos de la cuenta del pagador |

## Informes de Trusted Remediator

Informes disponibles

- Informe resumido de Trusted Remediator Remediation

- Informe resumido de la configuración de Trusted Remediator
- Trusted Advisor Compruebe el informe resumido

## Informe resumido de Trusted Remediator Remediation

El informe sobre el estado de las correcciones de Trusted Remediator proporciona información sobre las correcciones que se produjeron durante los ciclos de remediación anteriores. El número predeterminado de semanas es 1. Para personalizar el informe, especifique el número de semanas en función de su programa de remediación.

| Nombre del campo | Definición |
|---|---|
| Date | Fecha en la que se recopilaron los datos. |
| ID de cuenta | El identificador de AWS cuenta al que pertenece el recurso |
| Nombre de la cuenta | El nombre AWS de la cuenta |
| Compruebe la categoría | La categoría de AWS Trusted Advisor verificac ión |
| Nombre del cheque | El nombre de la comprobación corregida Trusted Advisor |
| ID de la verificación | El identificador de la comprobación corregida Trusted Advisor |
| Modo de ejecución | El modo de ejecución que se configuró para la Trusted Advisor comprobación específica |
| OpsItem ID | El ID del OpsItem creado por Trusted Advisor para su corrección |
| OpsItem Estado | El estado del objeto OpsItem creado por Trusted Advisor en el momento de elaborar el informe |
| ID de recurso | El ARN del recurso creado para la remediación |

## Informe resumido de la configuración de Trusted Remediator

El informe resumido de la configuración de Trusted Remediator proporciona información sobre las configuraciones actuales de Trusted Remediator Remediation para cada comprobación. Trusted Advisor

| Nombre del campo | Definición |
| --- | --- |
| Date | Fecha en la que se recopilaron los datos. |
| ID de cuenta | El ID de AWS cuenta al que se aplica la configuración |
| Nombre de la cuenta | El nombre AWS de la cuenta |
| Compruebe la categoría | La categoría de AWS Trusted Advisor verificac ión |
| Nombre del cheque | El nombre de la Trusted Advisor comprobación corregida a la que se aplica la configuración |
| ID de la verificación | El ID de la Trusted Advisor comprobación corregida a la que se aplica la configuración |
| Modo de ejecución | El modo de ejecución que se configuró para la Trusted Advisor comprobación específica |
| Sustituir a automatizado | El patrón de etiquetas, si está configurado, para anular el modo de ejecución a Automatiz ado |
| Sustituir a Manual | El patrón de etiquetas, si está configurado, para anular el modo de ejecución a Manual |

## Trusted Advisor Compruebe el informe resumido

El informe resumido de Trusted Advisor comprobaciones proporciona información sobre las Trusted Advisor comprobaciones actuales. Este informe recopila datos después de cada programa de

remediación semanal. El número predeterminado de semanas es 1. Para personalizar el informe, especifique el número de semanas en función del ciclo de corrección.

| Nombre del campo | Definición |
| --- | --- |
| Date | Fecha en la que se recopilaron los datos. |
| ID de cuenta | El ID de AWS cuenta al que se aplica la configuración |
| Nombre del cliente | El nombre AWS de la cuenta |
| Compruebe la categoría | La categoría de AWS Trusted Advisor verificación |
| Nombre del cheque | El nombre de la Trusted Advisor comprobación corregida a la que se aplica la configuración |
| ID de la verificación | El ID de la Trusted Advisor comprobación corregida a la que se aplica la configuración |
| Estado | El estado de alerta de la comprobación.<br>Los estados posibles son correcto (verde), advertencia (amarillo), error (rojo) o not_available |
| Recursos marcados | El número de AWS recursos que se marcaron (enumeraron) en la Trusted Advisor lista. |
| Recursos ignorados | El número de AWS recursos que se ignoraron Trusted Advisor porque los marcaste como suprimidos. |
| Recursos en estado crítico | El número de recursos en estado crítico |
| Recursos en estado de advertencia | El número de recursos en estado de advertencia |

# Informes de autoservicio

Los informes de autoservicio (SSR) de AWS Managed Services (AMS) son una función que recopila datos de varios AWS servicios nativos y proporciona acceso a informes sobre las principales ofertas de AMS. El SSR proporciona información que puede utilizar para respaldar las operaciones, la administración de la configuración, la administración de activos, la administración de la seguridad y el cumplimiento.

Utilice SSR para acceder a los informes desde la consola AMS y genere informes a los conjuntos de datos a través de buckets de Amazon S3 (un bucket por cuenta). Puede conectar los datos a su herramienta de inteligencia empresarial (BI) favorita para personalizar los informes en función de sus necesidades específicas. AMS crea este depósito de S3 (nombre del depósito de S3: (ams-reporting-data-a<Account_ID>) en su AWS región principal y los datos se comparten desde el plano de control de AMS alojado en la región us-east-1.

Para que sus usuarios puedan ver los informes de AMS Accelerate en la consola de AMS, debe conceder permisos explícitos en AWS Identity and Access Management (IAM) para realizar esas acciones. Para ver, por ejemplo, las políticas de IAM, consulte Permisos para usar las funciones de AMS.

> **Important**
>
> Uso de claves personalizadas con AWS Glue
> Para cifrar sus AWS Glue metadatos con una clave KMS administrada por el cliente, debe realizar los siguientes pasos adicionales para permitir que AMS agregue datos de la cuenta:
>
> 1. Abra la AWS Key Management Service consola en https://console.aws.amazon.com/kms y, a continuación, elija Claves gestionadas por el cliente.
> 2. Seleccione el ID de clave que planea usar para cifrar los AWS Glue metadatos.
> 3. Seleccione la pestaña Alias y, a continuación, elija Crear alias.
> 4. En el cuadro de texto, introduzca y AmsReportingFlywheelCustomKey, a continuación, seleccione Crear alias.

Temas


- Operaciones de API internas
- Informe de parches (diario)

- Informe de Backup (diario)
- Informe de incidentes (semanal)
- Informe de facturación (mensual)
- Informes agregados
- Paneles de informes de autoservicio de AMS
- Política de conservación de los datos
- Fuera de SSR

## Operaciones de API internas

Si supervisas las operaciones de la API, es posible que veas llamadas a las siguientes operaciones únicamente internas:

- `GetDashboardUrl`
- `ListReportsV2`

### Funcionamiento interno de la API: GetDashboardUrl

Esta operación aparece en los registros del sistema cuando la consola AMS la invoca. No tiene otro caso de uso. No está disponible para su uso directo.

Devuelve la URL del panel de control incrustado para el informe correspondiente. Esta operación acepta un mensaje `dashboardName` devuelto por`ListReports`.

Sintaxis de la solicitud

```
HTTP/1.1 200
Content-type: application/json
{
    "dashboardName": "string"
}
```

Elementos de la solicitud

**`dashboardName`**: el nombre del panel rápido para el que se solicita la URL. El nombre del panel se devuelve en la ListReports versión 2.

Tipo: cadena

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json
{
  "url": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200. El servicio devuelve los datos siguientes en formato JSON.

**`url`**: Devuelve la URL rápida de la solicitud`dashboardName`.

Tipo: cadena

Errores

Para obtener información sobre los errores comunes a todas las acciones, consulte Errores comunes.

**`BadRequestException`**:

La solicitud presentada no es válida. Por ejemplo, si la entrada está incompleta o es incorrecta. Consulte el mensaje de error adjunto para obtener más información.

Código de estado HTTP: 400

**`NotFoundException`**:

No se encuentra el recurso solicitado. Asegúrese de que el URI de la solicitud sea correcto.

Código de estado HTTP: 404

**`TooManyRequestsException`**:

La solicitud ha alcanzado su límite máximo. Vuelva a intentarlo una vez transcurrido el período de tiempo especificado.

Código de estado HTTP: 429

**`UnauthorizedException`**:

La solicitud se deniega porque la persona que llama no tiene permisos suficientes.

Código de estado HTTP: 401

## Funcionamiento de la API interna: V2 ListReports

Esta API aparece en los registros del sistema cuando la consola AMS la invoca. No tiene otro caso de uso. No está disponible para su uso directo.

Devuelve una lista de los informes operativos que están disponibles para una cuenta específica.

Sintaxis de la solicitud

La solicitud no tiene un cuerpo de solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json
{
  "reportsList": [
    {
        "dashboard": "string",
        "lastUpdatedTime": "string",
    }
  ],
  "reportsType": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200. El servicio devuelve los datos siguientes en formato JSON.

**`reportsList`**: La lista de informes operativos disponibles.

Tipo: matriz de objetos del panel

**`reportsType`**: Indica si un informe está agregado en varias cuentas o no.

Tipo: cadena

Errores

Para obtener información sobre los errores comunes a todas las acciones, consulte Errores comunes.

**`BadRequestException`**:

La solicitud presentada no es válida. Por ejemplo, la entrada está incompleta o es incorrecta. Consulte el mensaje de error adjunto para obtener más información.

Código de estado HTTP: 400

**`NotFoundException`**:

No se encuentra el recurso solicitado. Asegúrese de que el URI de la solicitud sea correcto.

Código de estado HTTP: 404

**`TooManyRequestsException`**:

La solicitud ha alcanzado su límite máximo. Vuelva a intentarlo una vez transcurrido el período de tiempo especificado.

Código de estado HTTP: 429

**`UnauthorizedException`**:

La solicitud se deniega porque la persona que llama no tiene permisos suficientes.

Código de estado HTTP: 401

## Informe de parches (diario)

Informes disponibles

- Resumen de los detalles de la instancia para la aplicación de parches en AMS
- Detalles del parche

- Instancias en las que no se incluyeron parches

## Resumen de los detalles de la instancia para la aplicación de parches en AMS

Se trata de un informe informativo que ayuda a identificar todas las instancias incorporadas a AMS Patching, el estado de la cuenta, los detalles de la instancia, la cobertura del período de mantenimiento, el tiempo de ejecución del período de mantenimiento, los detalles de la pila y el tipo de plataforma.

Este conjunto de datos proporciona:

- Datos sobre la producción y Non-Production las instancias de una cuenta. La producción y Non-Production la fase se derivan del nombre de la cuenta y no de las etiquetas de las instancias.
- Datos sobre la distribución de las instancias por tipo de plataforma. El tipo de plataforma N/A " se produce cuando AWS Systems Manager (SSM) no puede obtener la información de la plataforma.
- Datos sobre la distribución del estado de las instancias y el número de instancias en ejecución, detenidas o finalizadas.

| Nombre del campo de la consola | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Restricciones de acceso | access_restrictions | Regiones a las que está restringido el acceso |
| ID de cuenta | aws_account_id | AWS ID de cuenta al que pertenece el ID de instancia |
| ID de cuenta de administrador | aws_admin_account_id | Cuenta de confianza habilitad a por usted. AWS Organizat ions |
| Nombre de la cuenta | account_name | AWS nombre de la cuenta |
| Estado de la cuenta | estado_de la cuenta | Estado de la cuenta AMS |
| | account_sla | Compromiso de servicio de la cuenta AMS |

| Nombre del campo de la consola | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Account Type | malz_role | Función MALZ |
| Nombre del grupo de escalado automático | instance_asg_name | Nombre del Grupo de Auto Scaling (ASG) que contiene la instancia |
| ID de instancia | instance_id | ID de la instancia EC2 |
| Nombre de instancia | instance_name | Nombre de la instancia EC2 |
| Grupo de parches de instancias | instance_patch_group | Nombre del grupo de parches utilizado para agrupar las instancias y aplicar el mismo período de mantenimiento |
| Tipo de grupo de parches de instancias | instance_patch_group_type | Tipo de grupo de parches |
| Tipo de plataforma de instancia | instance_platform_type | Tipo de sistema operativo (SO) |
| Nombre de la plataforma de la instancia | instance_platform_name | Nombre del sistema operativo (SO) |
| Estado de la instancia | instance_state | Estado dentro del ciclo de vida de la instancia EC2 |
| Etiquetas de instancia | ec2_tags | Las etiquetas asociadas al ID de instancia de Amazon EC2 |
| Zona de aterrizaje | malz_flag | Marcar para la cuenta MALZ-related |

| Nombre del campo de la consola | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Cobertura del período de mantenimiento | mw_covered_flag | Si una instancia tiene al menos una ventana de mantenimiento habilitada con una fecha de ejecución futura, se considera cubierta y, de lo contrario, no está cubierta |
| Fecha y hora de ejecución de la ventana de mantenimiento | hora_de_ejecución de la ventana más temprana | La próxima vez se espera que se ejecute la ventana de mantenimiento |
| Fecha y hora de ejecución de la ventana de mantenimiento | hora_de_ejecución de la ventana más temprana | La próxima vez se espera que se ejecute la ventana de mantenimiento |
| Cuenta de producción | prod_account | Identificador de las cuentas AMS prod y no prod, en función de si el nombre de la cuenta incluye el valor «PROD» o «NONPROD». |
| Fecha y hora del informe | dataset_datetime | La fecha y la hora en que se generó el informe. |
| Nombre de la pila | instance_stack_name | Nombre de la pila que contiene la instancia |
| Tipo de pila | instance_stack_type | Pila de AMS (infraestructura de AMS dentro de la cuenta del cliente) o pila de clientes (infraestructura gestionada por AMS que admite las aplicacio nes de los clientes) |

## Detalles del parche

Este informe proporciona los detalles del parche y la cobertura del período de mantenimiento de varias instancias.

Este informe proporciona:

- Datos sobre los grupos de parches y sus tipos.
- Datos sobre las ventanas de mantenimiento, la duración, el límite, las fechas futuras de ejecución de las ventanas de mantenimiento (programación) y las instancias afectadas en cada ventana.
- Datos sobre todos los sistemas operativos de la cuenta y el número de instancias en las que está instalado el sistema operativo.

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Fecha y hora del informe | dataset_datetime | La fecha y la hora en que se generó el informe. |
| ID de cuenta | aws_account_id | AWS ID de cuenta al que pertenece el ID de instancia |
| Nombre de la cuenta | account_name | AWS nombre de la cuenta |
| Estado de la cuenta | estado_de la cuenta | Estado de la cuenta AMS |
| Cumple con las normas: crítico | compliant_crítico | Recuento de parches compatibles con una gravedad «crítica» |
| Cumple con las normas: alta | compliant_high | Recuento de parches compatibles con una gravedad «alta» |
| Cumple con las normas: media | compliant_medium | Recuento de parches compatibles con una gravedad «media» |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Cumple con las normas: bajo | compliant_low | Recuento de parches compatibles con una gravedad «baja» |
| Cumple con los requisitos: informativo | compliant_informativo | Recuento de parches compatibles con una gravedad «informativa» |
| Cumple con las normas: sin especificar | compliant_unspecified | Número de parches compatibles con una gravedad «no especificada» |
| Cumple con las normas: total | compliant_total | Recuento de parches compatibles (todos los niveles de gravedad) |
| ID de instancia | instance_id | ID de la instancia EC2 |
| Nombre de instancia | instance_name | Nombre de la instancia EC2 |
| | account_sla | Nivel de servicio de cuentas AMS |
| Tipo de plataforma de instancia | instance_platform_type | Tipo de sistema operativo (SO) |
| Nombre de la plataforma de la instancia | instance_platform_name | Nombre del sistema operativo (SO) |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
| --- | --- | --- |
| Tipo de grupo de parches de instancias | instance_patch_group_type | PREDETERMINADO: grupo de parches predeterminado con ventana de mantenimiento predeterminada, determinada por la etiqueta de la instancia AMSDefaultPatchGroup:True<br><br>CLIENTE: grupo de parches creado por el cliente<br><br>NOT_ASSIGNED: no se ha asignado ningún grupo de parches |
| Grupo de parches de instancias | instance_patch_group | Nombre del grupo de parches utilizado para agrupar las instancias y aplicar el mismo período de mantenimiento |
| Estado de la instancia | instance_state | Estado dentro del ciclo de vida de la instancia EC2 |
| Etiquetas de instancia | ec2_tags | Las etiquetas asociadas al ID de instancia de Amazon EC2 |
| Ventana de mantenimiento de última ejecución | last_execution_window | La última vez que se ejecutó la ventana de mantenimiento |
| ID de la ventana de mantenimiento | window_id | ID de la ventana de mantenimiento |
| Estado de la ventana de mantenimiento | window_state | Estado de la ventana de mantenimiento |
| Tipo de ventana de mantenimiento | tipo_ventana | Tipo de ventana de mantenimiento |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
| --- | --- | --- |
| Fecha y hora de la próxima ejecución de la ventana de mantenimiento | window_next<br>execution_time | La próxima vez se espera que se ejecute la ventana de mantenimiento |
| Duración del período de mantenimiento (horas) | duración de la ventana | La duración del período de mantenimiento en horas |
| Cobertura del período de mantenimiento | mw_covered_flag | Si una instancia tiene al menos una ventana de mantenimiento habilitada con una fecha de ejecución futura, se considera cubierta y, de lo contrario, no está cubierta |
| No compatible: crítico | noncompliant_critical | Recuento de parches no conformes con una gravedad «crítica» |
| No conformes: alto | noncompliant_high | Recuento de parches no conformes con una gravedad «alta» |
| No conforme: medio | noncompliant_medium | Recuento de parches no conformes con una gravedad «media» |
| No conformes: bajo | noncompliant_low | Recuento de parches no conformes con una gravedad «baja» |
| No conformes: informativo | no conforme<br>_informativo | Recuento de parches no conformes con una gravedad «informativa» |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
| --- | --- | --- |
| No conforme: sin especificar | no conforme<br>_sin especificar | Recuento de parches no conformes con una gravedad «no especificada» |
| No conformes: total | noncompliant_total | Recuento de parches no conformes (todos los grados de gravedad) |
| ID de referencia del parche | patch_baseline_id | La línea base del parche está actualmente conectada a la instancia |
| Estado del parche | patch_status | Estado general de cumplimie nto de los parches. Si falta al menos un parche, la instancia se considera no compatible; de lo contrario, es compatible. |
| Cuenta de producción | prod_account | Identificador de las cuentas AMS prod y no prod, en función de si el nombre de la cuenta incluye el valor «PROD» o «NONPROD». |
| Tipo de pila | instance_stack_type | Pila de AMS (infraestructura de AMS dentro de la cuenta del cliente) o pila de clientes (infraestructura gestionada por AMS que admite las aplicacio nes de los clientes) |
| | window_next_exec_yyyyy | El año forma parte de window_next_execution_time |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| | window_next_exec_mm | El mes forma parte de window_next_execution_time |
| | Window_Next_Exec_D | Día: parte de window_ne xt_execution_time |
| | window_next<br>_exec_HHMI | Hour:Minute parte de window_next_execution_time |

## Instancias en las que no se incluyeron parches

Este informe proporciona detalles sobre las instancias a las que no se les aplicaron los parches durante la última ejecución del período de mantenimiento.

Este informe proporciona:

- Datos sobre los parches faltantes a nivel de ID de parche.
- Datos sobre todas las instancias a las que les falta al menos un parche y atributos como la gravedad del parche, los días sin corregir, el intervalo y la fecha de lanzamiento del parche.

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Fecha y hora del informe | dataset_datetime | La fecha y la hora en que se generó el informe |
| ID de cuenta | aws_account_id | AWS ID de cuenta al que pertenece el ID de instancia |
| Nombre de cuenta | account_name | AWS nombre de la cuenta |
| Nombre del cliente: padre | customer_name_parent | |
| Nombre del cliente | customer_name | |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Cuenta de producción | prod_account | Identificador de las cuentas AMS prod o no prod, en función de si el nombre de la cuenta incluye el valor «PROD» o «NONPROD». |
| Estado de la cuenta | estado_de la cuenta | Estado de la cuenta AMS |
| Account Type | tipo_cuenta | |
| | account_sla | Nivel de servicio de cuentas AMS |
| ID de instancia | instance_id | ID de su instancia de EC2 |
| Nombre de instancia | instance_name | Nombre de su instancia EC2 |
| Tipo de plataforma de instancia | instance_platform_type | Tipo de sistema operativo (SO) |
| Estado de la instancia | instance_state | Estado dentro del ciclo de vida de la instancia EC2 |
| Etiquetas de instancia | ec2_tags | Las etiquetas asociadas al ID de instancia de Amazon EC2 |
| ID del parche | patch_id | ID del parche publicado |
| Gravedad del parche | patch_sev | Gravedad del parche por editor |
| Clasificación de los parches | patch_class | Clasificación del parche según el editor del parche |
| Fecha y hora de lanzamiento del parche (UTC) | release_dt_utc | Fecha de lanzamiento del parche por editor |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Estado de instalación del parche | install_state | Estado de instalación del parche en cada instancia por SSM |
| Días sin parches | days_unpatched | Número de días sin parchear la instancia desde el último escaneo de SSM |
| Rango de días sin parchear | days_unpatched_bucket | Grupo de días sin parchear |

## Informe de Backup (diario)

El informe de respaldo cubre las regiones principales y secundarias (cuando corresponda). Abarca el estado de las copias de seguridad (éxito o error) y los datos sobre las instantáneas realizadas.

Este informe proporciona:

- Estado de Backup
- Número de instantáneas tomadas
- Punto de recuperación
- Información sobre el plan de Backup y el almacén

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Fecha y hora del informe | dataset_datetime | La fecha y la hora en que se generó el informe. |
| ID de cuenta | aws_account_id | ID de cuenta de AWS a la que pertenece el ID de instancia |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| ID de cuenta de administrador | aws_admin_account_id | Cuenta de confianza habilitad a por usted. AWS Organizat ions |
| Nombre de la cuenta | account_name | Nombre de la cuenta de AWS |
| SLA de la cuenta | account_sla | Compromiso de servicio de la cuenta AMS |
| | malz_flag | Marcar para una cuenta relacionada con Malz |
| | malz_role | Función MALZ |
| | access_restrictions | Regiones a las que está restringido el acceso |
| Snapshot de backup: fecha y hora de inicio programadas | start_by_dt_utc | Marca de tiempo en la que está previsto que comience la instantánea |
| Fecha y hora de inicio reales de la instantánea de backup | creation_dt_utc | Marca de tiempo en que comienza realmente la instantánea |
| Fecha y hora de finalización de la instantánea de Backup | completion_dt_utc | Marca de tiempo en que se completa la instantánea |
| Fecha y hora de caducidad de la instantánea de Backup | expiration_dt_utc | Fecha y hora de caducidad de la instantánea |
| Estado de Backup Job | backup_job_status | Estado de la instantánea |
| Tipo de Backup | backup_type | Tipo de copia de seguridad |
| ID del trabajo de Backup | backup_job_id | El identificador único del trabajo de copia de seguridad |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Tamaño del Backup en bytes | tamaño_de_copia de seguridad en bytes | El tamaño de la copia de seguridad en bytes |
| Plan de Backup (ARN) | backup_plan_arn | El plan de respaldo (ARN) |
| ID del plan de Backup | backup_plan_id | Identificador único del plan de Backup |
| Nombre del plan de copias de seguridad | backup_plan_name | El nombre del plan de Backup |
| Versión del plan de Backup | backup_plan_version | La versión del plan de respaldo |
| ID de regla de Backup | backup_rule_id | El identificador de la regla de respaldo |
| ARN de Backup Vault | backup_vault_arn | ARN de Backup Vault |
| Nombre del almacén de copias de seguridad | backup_vault_name | El nombre del almacén de respaldo |
| ARN del rol de IAM | iam_role_arn | El rol de IAM (ARN) |
| ID de instancia | instance_id | ID de instancia único |
| Estado de la instancia | instance_state | Estado de la instancia |
| Etiquetas de instancia | ec2_tags | Las etiquetas asociadas al ID de instancia EC2 |
| ARN de recurso | resource_arn | El nombre del recurso de Amazon |
| ID de recurso | resource_id | El identificador único del recurso |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Región de recursos | región_recurso | Las regiones principales (y secundarias, cuando proceda) del recurso. |
| Tipo de recurso | resource_type | El tipo de recurso |
| Punto de recuperación (ARN) | recovery_point_arn | El ARN del punto de recuperación |
| ID del punto de recuperación | recovery_point_id | El identificador único del punto de recuperación |
| Estado del punto de recuperación | recovery_point_status | Estado del punto de recuperación |
| El punto de recuperación se elimina después de días | recovery_point_delete_after_days | El punto de recuperación se elimina después de días |
| El punto de recuperación se traslada a una cámara frigorífica después de días | recovery_point_move_to_cold_storage_after_days | Número de días transcurridos desde la fecha de finalización en que la instantánea de la copia de seguridad se traslada a una cámara frigorífica |
| Estado de cifrado del punto de recuperación | recovery_point_is_encrypted | Estado de cifrado del punto de recuperación |
| Clave de cifrado de punto de recuperación (ARN) | recovery_point_encryption_key_arn | Clave de cifrado del punto de recuperación (ARN) |
| ID de pila | stack_id | Identificador único de la pila de Cloudformation |
| Nombre de la pila | stack_name | Nombre de la pila |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Etiqueta: Grupo de parches predeterminado de AMS | tag_ams_default_patch_group | Valor de etiqueta: Grupo de parches predeterminado de AMS |
| Etiqueta: ID de aplicación | tag_app_id | Valor de etiqueta: ID de aplicación |
| Etiqueta: Nombre de la aplicación | tag_app_name | Valor de etiqueta: nombre de la aplicación |
| Etiqueta: Backup | tag_backup | Valor de etiqueta: Backup |
| Etiqueta: Marco de cumplimiento | tag_compliance_framework | Valor de etiqueta: Marco de cumplimiento |
| Etiqueta: Centro de costos | tag_cost_center | Valor de etiqueta: Centro de costes |
| Etiqueta: Cliente | tag_customer | Valor de etiqueta: Cliente |
| Etiqueta: Clasificación de datos | tag_data_classification | Valor de etiqueta: Clasificación de datos |
| Etiqueta: Tipo de entorno | tag_environment_type | Valor de etiqueta: Tipo de entorno |
| Etiqueta: Horas de operación | tag_horas_de_operación | Valor de etiqueta: Horas de operación |
| Etiqueta: Equipo propietario | tag_owner_team | Valor de etiqueta: equipo propietario |
| Etiqueta: Correo electrónico del equipo propietario | tag_owner_team_email | Valor de etiqueta: correo electrónico del equipo propietario |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Etiqueta: Patch Group | tag_patch_group | Valor de etiqueta: Patch Group |
| Etiqueta: Support Priority | tag_support_priority | Valor de etiqueta: Support Priority |
| Estado del volumen | estado_volumen | Estado del volumen |

## Informe de incidentes (semanal)

Este informe proporciona la lista agregada de incidentes junto con su prioridad, gravedad y estado más reciente, e incluye:

- Datos sobre los casos de soporte clasificados como incidentes en la cuenta gestionada
- Información sobre incidentes necesaria para visualizar las métricas de incidentes de la cuenta gestionada
- Datos sobre las categorías de incidentes y el estado de la solución de cada incidente

Tanto la visualización como los datos están disponibles para el informe semanal de incidentes.

- Se puede acceder a la visualización a través de la consola AMS de la cuenta a través de la página de informes.
- Se puede acceder al conjunto de datos con el siguiente esquema a través del bucket de S3 de la cuenta gestionada.
- Utilice los campos de fecha proporcionados para filtrar los incidentes según el mes, el trimestre, la semana y el and/or día en que se creó o resolvió el incidente.

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Fecha y hora del informe | dataset_datetime | La fecha y la hora en que se generó el informe. |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| ID de cuenta | aws_account_id | AWS ID de cuenta a la que pertenece el incidente. |
| ID de cuenta de administrador | aws_admin_account_id | Cuenta de confianza habilitad a por usted. AWS Organizat ions |
| Nombre de la cuenta | account_name | AWS nombre de cuenta. |
| ID de caso | case_id | El identificador del incidente. |
| Mes de creación | created_month | El mes en que se creó el incidente. |
| Prioridad | priority | La prioridad del incidente. |
| Gravedad | severity | La gravedad del incidente. |
| Estado | status | El estado del incidente. |
| Categoría | yuma_category | La categoría del incidente. |
| Día de creación | created_day | El día en que se creó el incidente en el formato. YYYY-MM-DD |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
| --- | --- | --- |
| Semana de creación | created_wk | La semana en que se creó el incidente en formato YYYY-WW. De domingo a sábado se contabilizan el principio y el final de la semana. La semana es del 01 al 25. La semana 01 es siempre la semana que contiene el primer día del año. Por ejemplo, el 31 de diciembre de 2021 y el 1 de enero de 2022 corresponden a la semana 2024-01. |
| Trimestre creado | created_qtr | El trimestre en el que se creó el incidente en formato AAAA. Del 01/01 al 31/03 se definen como Q1, y así sucesivam ente. |
| Día resuelto | resolved_day | El día en que se resolvió el incidente en el formato. YYYY-MM-DD |
| Semana resuelta | resolved_wk | La semana en que se resolvió el incidente en formato YYYY-WW. De domingo a sábado se contabilizan el principio y el final de la semana. La semana es del 01 al 25. La semana 01 es siempre la semana que contiene el primer día del año. Por ejemplo, el 31-12-2021 y el 2024-01-01 están en la semana 2024-01. |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Mes resuelto | mes_resuelto | El mes en que se resolvió el incidente en formato AAAA-MM. |
| Trimestre resuelto | resolved_qtr | El trimestre en el que se resolvió el incidente en formato AAAA. Del 01/01 al 31/03 se definen como Q1, y así sucesivamente. |
| Se creó la regla de agrupación | regla_agrupamiento | La regla de agrupación que se aplica al incidente. Ya sea «no_grouping» o «instance _grouping». |
| Instancia IDs | instance_ids | La instancia asociada al incidente. |
| Número de alertas | número_de_alertas | El número de alertas asociadas a ese incidente. Si tiene habilitada la agrupación, este número puede ser mayor que 1. Si no tiene habilitada la agrupación, siempre será 1. |
| Creado en | created_at | La marca de tiempo en que se creó el incidente. |
| Alarma ARNs | alarm_arns | El nombre del recurso de Amazon («arn») de las alarmas asociadas al incidente . |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Alarmas relacionadas | alarmas_relacionadas | Los nombres legibles para el ser humano de todas las alarmas asociadas al incidente . |

# Informe de facturación (mensual)

## Detalles de los cargos de facturación

Este informe proporciona detalles sobre los cargos de facturación de AMS con las cuentas vinculadas y los servicios de AWS correspondientes.

Este informe proporciona:

- Datos sobre los cargos a nivel de servicio de AMS, los porcentajes de aumento, los niveles de servicio de AMS a nivel de cuenta y las tarifas de AMS.
- Datos sobre las cuentas vinculadas y los cargos por uso de AWS.

> **Important**
>
> El informe de facturación mensual solo está disponible en su cuenta de administrador pagador (MPA) o en la cuenta de cargos definida. Estas son las cuentas a las que se envía la factura mensual de AMS. Si no puede localizar estas cuentas, póngase en contacto con su administrador de prestación de servicios en la nube (CSDM) para obtener ayuda.

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Fecha de facturación | date | El mes y el año del servicio facturado |
| ID de la cuenta del pagador | payer_account_id | El identificador de 12 dígitos que identifica la cuenta |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| | | responsable del pago de los cargos de AMS |
| ID de la cuenta vinculada | linked_account_id | El identificador de 12 dígitos que identifica la cuenta AMS que consume los servicios que generan expansiones |
| AWS Nombre del servicio | product_name | El AWS servicio que se utilizó |
| AWS Cargos | aws_charges | Los AWS cargos por el nombre del AWS servicio en AWS el nombre del servicio |
| Plan de precios | plan_de precios | El plan de precios asociado a la cuenta vinculada |
| Grupo de servicios AMS | tier_uplifting_groups | Código de grupo de servicios AMS que determina el porcentaje de aumento |
| Proporción de elevación | porcentaje de aumento | El porcentaje de aumento (expresado como V.WXYZ decimal) se basa en el pricing_plan, el SLA y el servicio AWS |
| Cargos ajustados AWS | ajusted_aws_usage | AWS uso ajustado para AMS |
| Cargos elevados AWS | Uplifted_aws_charges | El porcentaje de cargos que se cobrarán AWS por AMS; adjusted_aws_charges * uplift_percent |
| EC2 Instancias gastadas por RDS | instances_ec2_rds_spend | Invierta en instancias de RDS EC2 |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
| --- | --- | --- |
| Cargos por instancia reservada | ris_charges | Cargos por instancia reservada |
| Aumento de los cargos por instancia reservada | uplifted_ris | El porcentaje de cargos de instancia reservada que se cobrará por AMS; ris_charges * uplift_percent |
| Cargos del Savings Plan | sp_charges | SavingsPlan cargos de uso |
| Cargos elevados del Plan de Ahorros | uplifted_sp | El porcentaje de cargos de los planes de ahorro que se cobrarán por el AMS; sp_charges * uplift_percent |
| Cargos de AMS | ams_charges | Costos totales de ams del producto: uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris + uplifted_sp |
| Tarifa mínima prorrateada | mínimo prorrateado | El importe que cobramos para cumplir con el mínimo contractual |
| Cargos totales de AMS en la cuenta vinculada | linked_account_total<br><br>ams_charges | Suma de todos los cargos de la linked_account |
| Cargos totales de AMS de la cuenta del pagador | pays_account_total<br><br>ams_charges | Suma de todos los cargos de la cuenta del pagador |
| Cuota mínima | tarifas_mínimas | Tarifas mínimas de AMS (si corresponde) |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
| --- | --- | --- |
| Reserved Instance y Savings Plan discount | adj_ri_sp_charges | RI/SP discount to be applied against RI/SPcargos (aplicables en determinadas circunstancias) |

## Informes agregados

Los informes de autoservicio agregados (SSR) le proporcionan una vista de los informes de autoservicio existentes agregados a nivel de la organización y de forma transversal. Esto le permite ver los indicadores operativos clave, como el cumplimiento de los parches, la cobertura de respaldo y los incidentes, en todas las cuentas gestionadas por AMS dentro de su empresa. AWS Organizations

El SSR agregado está disponible en todos los anuncios comerciales en los Regiones de AWS que AWS Managed Services esté disponible. Para obtener una lista completa de las regiones disponibles, consulte la tabla de regiones.

### Habilite los informes agregados

Debe gestionar la SSR agregada desde una cuenta de AWS Organizations administración. La cuenta de administración es la AWS cuenta que utilizó para crear su organización.

Para habilitar el SSR agregado en una cuenta de AWS Organizations administración integrada en AMS, acceda a la consola de AMS y vaya a Informes. Seleccione Organization Access en la top-right-hand esquina para abrir el panel AWS Managed Services Console: Organization View. Desde este panel, puede administrar la funcionalidad de SSR agregado.

AWS Organizations Las cuentas de administración que no están integradas en AMS no tienen acceso a la consola AMS. Para habilitar el SSR agregado para una cuenta AWS Organizations de administración que no esté integrada en AMS, primero autentifíquese en su cuenta Cuenta de AWS, vaya a la AWS consola y busque Managed Services. Se abrirá la página de marketing de AMS. En esta página, seleccione el enlace Organization Access en la barra de navegación para abrir la consola de AWS Managed Services: Organization View, donde puede administrar la funcionalidad de SSR agregada.

La primera vez que acceda a AWS Managed Services Console: Organization View, complete los siguientes pasos:

1. Si aún no lo ha hecho AWS Organizations, seleccione Activar en AWS Organizations la consola. Para obtener información adicional sobre la configuración AWS Organizations, consulta la Guía del AWS Organizations usuario. Puede omitir este paso si ya lo utiliza AWS Organizations.
2. Para habilitar el servicio agregado de informes de autoservicio, seleccione Habilitar el acceso confiable en la consola.
3. (Opcional) Registre a un administrador delegado para que tenga acceso de lectura a la vista de la organización.

## Vea los informes agregados como administrador delegado

Un administrador delegado es la cuenta que usted elige para tener acceso de lectura a los informes agregados. El administrador delegado debe ser una cuenta incorporada a AMS y ser la única cuenta que tenga acceso de lectura a los informes agregados.

Para elegir un administrador delegado, introduzca el ID de la cuenta en el paso 3 de la AWS Managed Services Console: Organization View. Solo puede tener registrada una cuenta de administrador delegado a la vez. Tenga en cuenta que la cuenta de administrador delegado debe ser una cuenta administrada por AMS.

Para actualizar una cuenta de administrador delegado, vaya a la AWS Managed Services Console: Organization View y seleccione Eliminar el administrador delegado. La consola le pide que introduzca un nuevo ID de cuenta para registrarse como administrador delegado.

## Lea los informes agregados

Si no registras a un administrador delegado y tu cuenta de AWS Organizations administración está integrada en AMS, la cuenta de AWS Organizations administración tendrá acceso de lectura a los informes agregados de forma predeterminada. Si AMS no administra la cuenta de AWS Organizations administración, debe elegir una cuenta de administrador delegado para tener acceso de lectura a los informes agregados.

En cualquier momento, solo una cuenta incorporada a AMS tiene acceso de lectura a los informes agregados, ya sea la cuenta de AWS Organizations administración o el administrador delegado registrado. Todas las demás cuentas de miembros de su organización (e incorporadas a AMS) seguirán teniendo acceso únicamente a los informes de una sola cuenta para cada cuenta individual.

Después de activar el SSR agregado, navegue hasta sus informes. Todos los informes de autoservicio existentes aparecen en esta sección y una etiqueta azul indica que se han agregado. Tenga en cuenta que debe acceder a la consola AMS desde la cuenta que eligió para tener acceso

de lectura a los informes agregados. Se trata de la cuenta AWS Organizations de administración o de administrador delegado.

Tras activar la SSR agregada, los informes agregados estarán disponibles a partir del siguiente ciclo de elaboración de informes.

### Deshabilite los informes agregados

Para deshabilitar el SSR agregado, abra la consola de AWS Managed Services: Organization View. Seleccione Inhabilitar el acceso de confianza. Tras deshabilitar el acceso de confianza para el SSR agregado, los informes de autoservicio de AMS dejarán de agregarse a nivel de la organización, en todas las cuentas. Tenga en cuenta también que la desactivación se efectuará a partir del siguiente ciclo de presentación de informes.

Tras desactivar el SSR agregado, hay que esperar hasta que los informes de la consola AMS aparezcan como informes de una sola cuenta. Este retraso se debe a que la desactivación de la función se produce a partir del siguiente ciclo de generación de informes.

## Paneles de informes de autoservicio de AMS

Los informes de autoservicio de AMS ofrecen dos paneles: y. Panel de control de Resource Tagger Panel de reglas de configuración de seguridad

### Panel de control de Resource Tagger

El panel de control del etiquetador de recursos de AMS proporciona información detallada sobre los recursos compatibles con Resource Tagger, así como el estado actual de las etiquetas que Resource Tagger está configurado para aplicar a esos recursos.

Cobertura del etiquetador de recursos por tipo de recurso

Este conjunto de datos consta de una lista de recursos que tienen etiquetas administradas por Resource Tagger.

La cobertura de recursos por tipo de recurso se visualiza en cuatro gráficos de líneas que describen las siguientes métricas:

- Recuento de recursos: el número total de recursos de la región, por tipo de recurso.
- Recursos a los que les faltan etiquetas administradas: el número total de recursos de la región, por tipo de recurso, que requieren etiquetas administradas pero que no están etiquetados por el etiquetador de recursos.

- Recursos no gestionados: el número total de recursos de la región, por tipo de recurso, a los que Resource Tagger no les ha aplicado etiquetas gestionadas. Por lo general, esto significa que estos recursos no coinciden con ninguna configuración de Resource Tagger o que están excluidos explícitamente de las configuraciones.
- Recursos gestionados: métrica equivalente a la de recursos no gestionados (recuento de recursos: recursos no gestionados).

En la siguiente tabla se enumeran los datos proporcionados por este informe.

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Fecha y hora del informe | dataset_datetime | La fecha y la hora en que se generó el informe (hora UTC) |
| Cuenta de AWS ID | aws_account_id | Cuenta de AWS ID |
| ID de cuenta de administrador | aws_admin_account_id | Cuenta de confianza habilitada por usted. AWS Organizations |
| Region | region | Región de AWS |
| Tipo de recurso | resource_type | Este campo identifica el tipo de recurso. Solo se incluyen los tipos de recursos compatibles con Resource Tagger. |
| Recuento de recursos | conteo de recursos | Número de recursos (del tipo de recurso especificado) desplegados en esta región. |
| ResourcesMissingManagedTags | resource_missing_managed_tags_count | Número de recursos (del tipo de recurso especificado) que requieren etiquetas administradas, según los perfiles de configuración, pero que |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| | | Resource Tagger aún no los ha etiquetado. |
| UnmanagedResources | unmanaged_resource_count | Número de recursos (del tipo de recurso especificado) a los que Resource Tagger no ha aplicado etiquetas administr adas. Por lo general, estos recursos no coincidían con ningún bloque de configura ción de Resource Tagger o se excluyen explícitamente de los bloques de configuración. |

Cumplimiento de las reglas de configuración de Resource Tagger

Este conjunto de datos consiste en una lista de recursos Región de AWS, clasificados por tipo de recurso, a los que se les ha aplicado un perfil de configuración determinado. Se visualiza como un gráfico de líneas.

En la siguiente tabla se enumeran los datos proporcionados por este informe.

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Fecha y hora del informe | dataset_datetime | La fecha y la hora en que se generó el informe (hora UTC) |
| Cuenta de AWS ID | aws_account_id | Cuenta de AWS ID |
| ID de cuenta de administrador | aws_admin_account_id | Cuenta de confianza habilitad a por usted. AWS Organizat ions |
| Region | region | Región de AWS |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
| --- | --- | --- |
| Tipo de recurso | resource_type | Este campo identifica el tipo de recurso. Solo se incluyen los tipos de recursos compatibles con Resource Tagger. |
| ID del perfil de configuración | configuration_profile_id | El ID del perfil de configuración del etiquetador de recursos. Se utiliza un perfil de configuración para definir las políticas y reglas que se utilizan para etiquetar los recursos. |
| MatchingResourceCount | resource_count | Número de recursos (del tipo de recurso especificado) que coinciden con el ID del perfil de configuración del etiquetador de recursos. Para que un recurso coincida con el perfil de configuración, el perfil debe estar habilitado y el recurso debe coincidir con la regla del perfil. |

Resource Tagger: recursos no compatibles

Este conjunto de datos consta de una lista de recursos que no son compatibles con una única configuración de Resource Tagger. Estos datos son un resumen diario del cumplimiento de los recursos y muestran el estado de los recursos de los clientes en el momento en que se envían estos informes a las cuentas de los clientes (no hay una vista histórica). Se visualiza como una tabla dinámica que consta de recursos que no cumplen con los requisitos de una configuración determinada.

En la siguiente tabla se enumeran los datos proporcionados por este informe.

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| Fecha y hora del informe | dataset_datetime | La fecha y la hora en que se generó el informe (hora UTC) |
| Cuenta de AWS ID | aws_account_id | Cuenta de AWS ID |
| ID de cuenta de administrador | aws_admin_account_id | Cuenta de confianza habilitada por usted. AWS Organizations |
| Region | region | Región de AWS |
| Tipo de recurso | resource_type | Este campo identifica el tipo de recurso. Solo se incluyen los tipos de recursos compatibles con Resource Tagger. |
| Resource ID (ID de recurso) | resource_id | El identificador único de los recursos compatibles con Resource Tagger. |
| Estado de cobertura | estado_de cobertura | Este campo indica si el recurso está etiquetado como lo configuró el ID de configuración del etiquetador de recursos. |
| ID del perfil de configuración | configuration_profile_id | El ID del perfil de configuración del etiquetador de recursos. Se utiliza un perfil de configuración para definir las políticas y reglas que se |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
| --- | --- | --- |
| | | utilizan para etiquetar los recursos. |

## Panel de reglas de configuración de seguridad

El panel de reglas de Security Config ofrece una visión detallada del cumplimiento de los recursos y las AWS Config reglas de las cuentas AMS. Puede filtrar el informe por el nivel de severidad de las reglas para priorizar los hallazgos más importantes. En la siguiente tabla se enumeran los datos proporcionados por este informe.

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
| --- | --- | --- |
| Cuenta de AWS ID | Cuenta de AWS ID | El identificador de la cuenta vinculado a los recursos relacionados. |
| ID de cuenta de administrador | aws_admin_account_id | Cuenta de confianza habilitad a por usted. AWS Organizat ions |
| fecha y hora del informe | Fecha del informe | La fecha y la hora en que se generó el informe. |
| customer_name | Nombre del cliente | El nombre del cliente. |
| account_name | Nombre de la cuenta | El nombre asociado al ID de la cuenta |
| resource_id | Resource ID (ID de recurso) | Un identificador de un recurso. |
| resource_region | Región de recursos | El Región de AWS lugar donde se encuentra el recurso. |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
|---|---|---|
| resource_type | Tipo de recurso | El tipo de recurso Servicio de AWS or. |
| nombre_recurso | Nombre del recurso | El nombre del recurso. |
| resource_ams_flag | Indicador AMS del recurso | Si el recurso es propiedad de AMS, este indicador se establece en TRUE. Si el recurso es propiedad del cliente, este indicador se establece en FALSE. Si no se conoce la propiedad, este indicador se establece en DESCONOCIDO. |
| config_rule | Regla de configuración | El nombre no personalizable de la regla de configuración. |
| config_rule_description | Descripción de la regla de configuración | Una descripción de la regla de configuración. |
| source_identifier | Identificador de fuente | Un identificador único para la regla de configuración gestionada y ningún identific ador para una regla de configuración personalizada. |
| compliance_flag | Indicador de cumplimiento | Muestra si los recursos cumplen o no con las reglas de configuración. |
| tipo_regla | Tipo de regla | Indica si la regla está predefini da o personalizada. |

| Nombre del campo | Nombre del campo del conjunto de datos | Definición |
| --- | --- | --- |
| exception_flag | Bandera de excepción | El indicador de excepción del recurso muestra la aceptación del riesgo en relación con un recurso que no cumple con las normas. Si el indicador de excepción del recurso es VERDADERO para un recurso, entonces el recurso está exento. Si el indicador de excepción es NULL, el recurso no está exento. |
| cal_dt | Date | La fecha de evaluación de la regla. |
| descripción_de_remediación | Descripción de la remediación | Una descripción de cómo corregir el cumplimiento de las normas. |
| severity | Gravedad | La gravedad de la regla de configuración indica el impacto del incumplimiento. |
| customs_action | Acción del cliente | Debe tomar las medidas necesarias para corregir esta regla. |
| recommendation | Recomendación | Una descripción de lo que comprueba la regla de configuración. |
| categoría_remediación | Categoría de remediación | Las acciones predeterminadas que adopta AMS cuando esta regla deja de ser compatible. |

## Política de conservación de los datos

AMS SSR tiene una política de retención de datos por informe después del período reportado, cuando los datos se borran y dejan de estar disponibles.

| Nombre del informe | Consola SSR de retención de datos | Cubeta SSR S3 de retención de datos |
|---|---|---|
| Resumen de los detalles de la instancia para la aplicación de parches en AMS | 2 meses | 2 años |
| Detalles del parche | 2 meses | 2 años |
| Instancias en las que se omitieron parches durante la ejecución del período de mantenimiento | 2 meses | 2 años |
| Detalles de los cargos de facturación de AMS | 2 años | 2 años |
| Informe de Backup Diario | 1 mes | 2 años |
| Informe semanal de incidentes | 2 meses | 2 años |
| Panel de reglas de configura ción de seguridad | 3 meses | 2 años |
| Panel de control de Resource Tagger | 1 año | 2 años |

## Fuera de SSR

Para desconectarse del servicio SSR, cree una solicitud de servicio (SR) a través de la consola AMS. Tras enviar la SR, un ingeniero de operaciones de AMS le ayudará a abandonar el SSR. En el SR, indique el motivo por el que desea dejar el servicio.

Para eliminar una cuenta y limpiar los recursos, crea una SR a través de la consola AMS. Tras enviar el SR, un ingeniero de operaciones de AMS le ayudará a eliminar el bucket de Amazon S3 del SSR.

Si se desconecta de AMS, se desconectará automáticamente de la consola AMS SSR. AMS deja de enviar datos a tu cuenta automáticamente. AMS borra tu bucket de SSR S3 como parte del proceso de desconexión.

# Gestión de acceso en AMS Accelerate

La gestión del acceso es la forma en que se protegen sus recursos, ya que solo permite el acceso autorizado y autenticado. Con AMS Accelerate, usted es responsable de administrar el acceso a sus recursos Cuentas de AWS y a los recursos subyacentes, como las soluciones de administración de acceso, las políticas de acceso y los procesos relacionados. Para ayudarle a gestionar su solución de acceso, AMS Accelerate implementa AWS Config reglas que detectan los errores de configuración más comunes de la IAM y, a continuación, envían notificaciones de corrección. Un error común de configuración de IAM es que el usuario raíz tiene claves de acceso. La regla de `iam-root-access-key-check` configuración comprueba si la clave de acceso del usuario raíz está disponible y es compatible o si la clave de acceso no existe. Para obtener una lista de las reglas de configuración implementadas por AMS, consulte la biblioteca de AWS Config reglas de AMS.

Temas


- Obtenga acceso a la consola Accelerate
- Permisos para usar las funciones de AMS
- Por qué y cuándo AMS accede a tu cuenta
- Cómo accede AMS a tu cuenta
- Cómo y cuándo usar la cuenta de usuario root en AMS


## Obtenga acceso a la consola Accelerate

Cuando incorpore Accelerate, tendrá acceso automáticamente a la consola Accelerate. Para acceder a la consola, busque Managed Services en la consola de administración de AWS. La consola Accelerate le ofrece una vista resumida de las funciones de las que dispone con Accelerate. Esta vista incluye los componentes individuales que se presentan en el panel de control y en las páginas de configuración.

## Permisos para usar las funciones de AMS

Para que los usuarios puedan leer y configurar las funciones de AMS Accelerate, como acceder a la consola AMS o configurar las copias de seguridad, debe conceder permisos explícitos a sus funciones de IAM para que realicen esas acciones. La siguiente CloudFormation plantilla contiene las políticas necesarias para leer y configurar los servicios asociados a AMS de forma

que pueda asignarlos a sus funciones de IAM. Están diseñadas para ajustarse estrechamente a las responsabilidades laborales habituales en el sector de TI, donde se requieren permisos de administrador o de solo lectura; sin embargo, si necesita conceder permisos diferentes a los usuarios, puede editar la política para incluir o excluir permisos específicos. También puede crear su propia política personalizada.

La plantilla proporciona dos políticas. La `AMSAccelerateAdminAccess` política está destinada a utilizarse para configurar y operar los componentes de AMS Accelerate. Por lo general, esta política la asume un administrador de TI y otorga permisos para configurar las funciones de AMS, como la aplicación de parches y las copias de seguridad. `AMSAccelerateReadOnly`Otorga los permisos mínimos necesarios para ver los recursos relacionados con AMS Accelerate.

```
AWSTemplateFormatVersion: 2010-09-09
Description: AMSAccelerateCustomerAccessPolicies

Resources:
  AMSAccelerateAdminAccess:
    Type: 'AWS::IAM::ManagedPolicy'
    Properties:
      ManagedPolicyName: AMSAccelerateAdminAccess
      Path: /
      PolicyDocument:
        Fn::Sub:
        - |
          {
            "Version": "2012-10-17",
            "Statement": [
              {
                 "Sid": "AmsSelfServiceReport",
                 "Effect": "Allow",
                 "Action": "amsssrv:*",
                 "Resource": "*"
              },
              {
                "Sid": "AmsBackupPolicy",
                "Effect": "Allow",
                "Action": "iam:PassRole",
                "Resource": "arn:aws:iam::${AWS::AccountId}:role/ams-backup-iam-role"
              },
              {
                "Sid": "AmsChangeRecordKMSPolicy",
                "Effect": "Allow",
```

```
                "Action": [
                  "kms:Encrypt",
                  "kms:Decrypt",
                  "kms:GenerateDataKey"
                ],
                "Resource": [
                  "arn:aws:kms:${AWS::Region}:${AWS::AccountId}:key/*"
                ],
                "Condition": {
                  "ForAnyValue:StringLike": {
                    "kms:ResourceAliases": "alias/AMSCloudTrailLogManagement"
                  }
                }
              },
              {
                "Sid": "AmsChangeRecordAthenaReadPolicy",
                "Effect": "Allow",
                "Action": [
                  "athena:BatchGetNamedQuery",
                  "athena:Get*",
                  "athena:List*",
                  "athena:StartQueryExecution",
                  "athena:UpdateWorkGroup",
                  "glue:GetDatabase*",
                  "glue:GetTable*",
                  "s3:GetAccountPublicAccessBlock",
                  "s3:ListAccessPoints",
                  "s3:ListAllMyBuckets"
                ],
                "Resource": "*"
              },
              {
                "Sid": "AmsChangeRecordS3ReadPolicy",
                "Effect": "Allow",
                "Action": [
                  "s3:Get*",
                  "s3:List*"
                ],
                "Resource": [
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/
*",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}/*"
```

```
        ]
      },
      {
        "Sid": "AmsChangeRecordS3WritePolicy",
        "Effect": "Allow",
        "Action": [
          "s3:PutObject",
          "s3:PutObjectLegalHold",
          "s3:PutObjectRetention"

        ],
        "Resource": [
          "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*"
        ]
      },
      {
        "Sid": "MaciePolicy",
        "Effect": "Allow",
        "Action": [
          "macie2:GetFindingStatistics"
        ],
        "Resource": "*"
      },
      {
        "Sid": "GuardDutyPolicy",
        "Effect": "Allow",
        "Action": [
          "guardduty:GetFindingsStatistics",
          "guardduty:ListDetectors"
        ],
        "Resource": "*"
      },
      {
        "Sid": "SupportPolicy",
        "Effect": "Allow",
        "Action": "support:*",
        "Resource": "*"
      },
      {
        "Sid": "ConfigPolicy",
        "Effect": "Allow",
        "Action": [
          "config:Get*",
          "config:Describe*",
```

```
                "config:Deliver*",
                "config:List*",
                "config:StartConfigRulesEvaluation"
              ],
              "Resource": "*"
            },
            {
              "Sid": "AppConfigReadPolicy",
              "Effect": "Allow",
              "Action": [
                "appconfig:List*",
                "appconfig:Get*"
              ],
              "Resource": "*"
            },
            {
              "Sid": "AppConfigPolicy",
              "Effect": "Allow",
              "Action": [
                "appconfig:StartDeployment",
                "appconfig:StopDeployment",
                "appconfig:CreateHostedConfigurationVersion",
                "appconfig:ValidateConfiguration"
              ],
              "Resource": [
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}/configurationprofile/
${AMSAlarmManagerConfigurationCustomerManagedAlarmsProfileID}",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}/environment/*",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}/configurationprofile/
${AMSResourceTaggerConfigurationCustomerManagedTagsProfileID}",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}/environment/*",
                "arn:aws:appconfig:*:${AWS::AccountId}:deploymentstrategy/*"
              ]
            },
            {
              "Sid": "CloudFormationStacksPolicy",
```

```
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EC2Policy",
      "Action": [
        "ec2:DescribeInstances"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Sid": "SSMPolicy",
      "Effect": "Allow",
      "Action": [
        "ssm:AddTagsToResource",
        "ssm:CancelCommand",
        "ssm:CancelMaintenanceWindowExecution",
        "ssm:CreateAssociation",
        "ssm:CreateAssociationBatch",
        "ssm:CreateMaintenanceWindow",
        "ssm:CreateOpsItem",
        "ssm:CreatePatchBaseline",
        "ssm:DeleteAssociation",
        "ssm:DeleteMaintenanceWindow",
        "ssm:DeletePatchBaseline",
        "ssm:DeregisterPatchBaselineForPatchGroup",
        "ssm:DeregisterTargetFromMaintenanceWindow",
        "ssm:DeregisterTaskFromMaintenanceWindow",
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "ssm:PutConfigurePackageResult",
        "ssm:RegisterDefaultPatchBaseline",
        "ssm:RegisterPatchBaselineForPatchGroup",
        "ssm:RegisterTargetWithMaintenanceWindow",
        "ssm:RegisterTaskWithMaintenanceWindow",
        "ssm:RemoveTagsFromResource",
        "ssm:SendCommand",
        "ssm:StartAssociationsOnce",
        "ssm:StartAutomationExecution",
```

```
            "ssm:StartSession",
            "ssm:StopAutomationExecution",
            "ssm:TerminateSession",
            "ssm:UpdateAssociation",
            "ssm:UpdateAssociationStatus",
            "ssm:UpdateMaintenanceWindow",
            "ssm:UpdateMaintenanceWindowTarget",
            "ssm:UpdateMaintenanceWindowTask",
            "ssm:UpdateOpsItem",
            "ssm:UpdatePatchBaseline"
          ],
          "Resource": "*"
        },
        {
          "Sid": "AmsPatchRestrictAMSResources",
          "Effect": "Deny",
          "Action": [
            "ssm:DeletePatchBaseline",
            "ssm:UpdatePatchBaseline"
          ],
          "Resource": [
            "arn:aws:ssm:${AWS::Region}:${AWS::AccountId}:patchbaseline/*"
          ],
          "Condition": {
            "StringLike": {
              "aws:ResourceTag/ams:resourceOwner": "*"
            }
          }
        },
        {
          "Sid": "AmsPatchRestrictAmsTags",
          "Effect": "Deny",
          "Action": [
            "ssm:AddTagsToResource",
            "ssm:RemoveTagsFromResource"
          ],
          "Resource": "*",
          "Condition": {
            "ForAnyValue:StringLike": {
              "aws:TagKeys": [
                "AMS*",
                "Ams*",
                "ams*"
              ]
```

```
            }
          }
        },
        {
          "Sid": "TagReadPolicy",
          "Effect": "Allow",
          "Action": [
            "tag:GetResources",
            "tag:GetTagKeys"
          ],
          "Resource": "*"
        },
        {
          "Sid": "CloudtrailReadPolicy",
          "Effect": "Allow",
          "Action": [
            "cloudtrail:DescribeTrails",
            "cloudtrail:GetTrailStatus",
            "cloudtrail:LookupEvents"
          ],
          "Resource": "*"
        },
        {
          "Sid": "EventBridgePolicy",
          "Effect": "Allow",
          "Action": [
            "events:Describe*",
            "events:List*",
            "events:TestEventPattern"
          ],
          "Resource": "*"
        },
        {
          "Sid": "IAMReadOnlyPolicy",
          "Action": [
              "iam:ListRoles",
              "iam:GetRole"
          ],
          "Effect": "Allow",
          "Resource": "*"
        },
        {
          "Sid": "AmsResourceSchedulerPassRolePolicy",
          "Effect": "Allow",
```

```
                "Action": "iam:PassRole",
                "Resource": "arn:aws:iam::${AWS::AccountId}:role/
ams_resource_scheduler_ssm_automation_role",
                "Condition": {
                    "StringEquals": {
                        "iam:PassedToService": "ssm.amazonaws.com"
                    }
                }
              }
            ]
          }
        - AMSAlarmManagerConfigurationApplicationId: !ImportValue "AMS-Alarm-Manager-
Configuration-ApplicationId"
          AMSAlarmManagerConfigurationCustomerManagedAlarmsProfileID: !ImportValue
 "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID"
          AMSResourceTaggerConfigurationApplicationId: !ImportValue "AMS-
ResourceTagger-Configuration-ApplicationId"
          AMSResourceTaggerConfigurationCustomerManagedTagsProfileID: !ImportValue
 "AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID"

  AMSAccelerateReadOnly:
    Type: 'AWS::IAM::ManagedPolicy'
    Properties:
      ManagedPolicyName: AMSAccelerateReadOnly
      Path: /
      PolicyDocument: !Sub |
        {
          "Version": "2012-10-17",
          "Statement": [
          {
                "Sid": "AmsSelfServiceReport",
                "Effect": "Allow",
                "Action": "amsssrv:*",
                "Resource": "*"
              },
            {
              "Sid": "AmsBackupPolicy",
              "Effect": "Allow",
              "Action": [
                "backup:Describe*",
                "backup:Get*",
                "backup:List*"
              ],
              "Resource": "*"
```

```
            },
            {
                "Action": [
                    "rds:DescribeDBSnapshots",
                    "rds:ListTagsForResource",
                    "rds:DescribeDBInstances",
                    "rds:describeDBSnapshots",
                    "rds:describeDBEngineVersions",
                    "rds:describeOptionGroups",
                    "rds:describeOrderableDBInstanceOptions",
                    "rds:describeDBSubnetGroups",
                    "rds:DescribeDBClusterSnapshots",
                    "rds:DescribeDBClusters",
                    "rds:DescribeDBParameterGroups",
                    "rds:DescribeDBClusterParameterGroups",
                    "rds:DescribeDBInstanceAutomatedBackups"
                ],
                "Effect": "Allow",
                "Resource": "*"
            },
            {
                "Action": [
                    "dynamodb:ListBackups",
                    "dynamodb:ListTables"
                ],
                "Effect": "Allow",
                "Resource": "*"
            },
            {
                "Action": [
                    "elasticfilesystem:DescribeFilesystems"
                ],
                "Resource": "arn:aws:elasticfilesystem:*:*:file-system/*",
                "Effect": "Allow"
            },
            {
                "Action": [
                    "ec2:DescribeSnapshots",
                    "ec2:DescribeVolumes",
                    "ec2:describeAvailabilityZones",
                    "ec2:DescribeVpcs",
                    "ec2:DescribeAccountAttributes",
                    "ec2:DescribeSecurityGroups",
                    "ec2:DescribeImages",
```

```
                "ec2:DescribeSubnets",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:GetResources"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:DescribeCachediSCSIVolumes",
                "storagegateway:DescribeStorediSCSIVolumes"
            ],
            "Resource": "arn:aws:storagegateway:*:*:gateway/*/volume/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Resource": "arn:aws:storagegateway:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:DescribeGatewayInformation",
                "storagegateway:ListVolumes",
                "storagegateway:ListLocalDisks"
            ],
            "Resource": "arn:aws:storagegateway:*:*:gateway/*"
        },
        {
            "Action": [
                "iam:ListRoles",
```

```
                "iam:GetRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "organizations:DescribeOrganization",
            "Resource": "*"
        },
        {
            "Action": "fsx:DescribeBackups",
            "Effect": "Allow",
            "Resource": "arn:aws:fsx:*:*:backup/*"
        },
        {
            "Action": "fsx:DescribeFileSystems",
            "Effect": "Allow",
            "Resource": "arn:aws:fsx:*:*:file-system/*"
        },
        {
            "Action": "ds:DescribeDirectories",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
          "Sid": "AmsChangeRecordKMSPolicy",
          "Effect": "Allow",
          "Action": [
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:GenerateDataKey"
          ],
          "Resource": [
            "arn:aws:kms:${AWS::Region}:${AWS::AccountId}:key/*"
          ],
          "Condition": {
            "ForAnyValue:StringLike": {
              "kms:ResourceAliases": "alias/AMSCloudTrailLogManagement"
            }
          }
        },
        {
          "Sid": "AmsChangeRecordAthenaReadPolicy",
```

```
            "Effect": "Allow",
            "Action": [
              "athena:BatchGetNamedQuery",
              "athena:Get*",
              "athena:List*",
              "athena:StartQueryExecution",
              "athena:UpdateWorkGroup",
              "glue:GetDatabase*",
              "glue:GetTable*",
              "s3:GetAccountPublicAccessBlock",
              "s3:ListAccessPoints",
              "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
          },
          {
            "Sid": "AmsChangeRecordS3ReadPolicy",
            "Effect": "Allow",
            "Action": [
              "s3:Get*",
              "s3:List*"
            ],
            "Resource": [
              "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}",
              "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*",
              "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}",
              "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}/*"
            ]
          },
          {
            "Sid": "AmsChangeRecordS3WritePolicy",
            "Effect": "Allow",
            "Action": [
              "s3:PutObject",
              "s3:PutObjectLegalHold",
              "s3:PutObjectRetention"
            ],
            "Resource": [
              "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*"
            ]
          },
          {
            "Sid": "MaciePolicy",
            "Effect": "Allow",
```

```
            "Action": [
              "macie2:GetFindingStatistics"
            ],
            "Resource": "*"
          },
          {
            "Sid": "GuardDutyReadPolicy",
            "Effect": "Allow",
            "Action": [
              "guardduty:GetFindingsStatistics",
              "guardduty:ListDetectors"
            ],
            "Resource": "*"
          },
          {
            "Sid": "SupportReadPolicy",
            "Effect": "Allow",
            "Action": "support:Describe*",
            "Resource": "*"
          },
          {
            "Sid": "ConfigReadPolicy",
            "Effect": "Allow",
            "Action": [
              "config:Get*",
              "config:Describe*",
              "config:List*"
            ],
            "Resource": "*"
          },
          {
            "Sid": "AppConfigReadPolicy",
            "Effect": "Allow",
            "Action": [
              "appconfig:List*",
              "appconfig:Get*"
            ],
            "Resource": "*"
          },
          {
            "Sid": "CloudFormationReadPolicy",
            "Effect": "Allow",
            "Action": [
              "cloudformation:DescribeStacks"
```

```
            ],
            "Resource": "*"
          },
          {
            "Sid": "EC2ReadPolicy",
            "Effect": "Allow",
            "Action": [
              "ec2:DescribeInstances"
            ],
            "Resource": "*"
          },
          {
            "Sid": "SSMReadPolicy",
            "Effect": "Allow",
            "Action": [
              "ssm:Describe*",
              "ssm:Get*",
              "ssm:List*"
            ],
            "Resource": "*"
          },
          {
            "Sid": "TagReadPolicy",
            "Effect": "Allow",
            "Action": [
              "tag:GetResources",
              "tag:GetTagKeys"
            ],
            "Resource": "*"
          },
          {
            "Sid": "CloudtrailReadPolicy",
            "Effect": "Allow",
            "Action": [
              "cloudtrail:DescribeTrails",
              "cloudtrail:GetTrailStatus",
              "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
          },
          {
            "Sid": "EventBridgePolicy",
            "Effect": "Allow",
            "Action": [
```

```
                "events:Describe*",
                "events:List*",
                "events:TestEventPattern"
            ],
            "Resource": "*"
        }
    ]
}
```

# Por qué y cuándo AMS accede a tu cuenta

Los operadores de AMS Accelerate (Accelerate) pueden acceder a la consola y a las instancias de su cuenta, en determinadas circunstancias, para gestionar sus recursos. Estos eventos de acceso están documentados en sus registros AWS CloudTrail (CloudTrail). Para obtener más información sobre cómo el equipo de AMS Accelerate Operations y la automatización de AMS Accelerate Operations revisan la actividad de su cuenta, consulte[Seguimiento de los cambios en sus cuentas de AMS Accelerate](#).

En los siguientes temas se explica por qué, cuándo y cómo AMS accede a su cuenta.

## Activadores de acceso a la cuenta de cliente de AMS

La actividad de acceso a la cuenta de los clientes de AMS depende de factores desencadenantes. Los factores desencadenantes actuales son los AWS tickets creados en nuestro sistema de gestión de problemas en respuesta a las alarmas y eventos de Amazon CloudWatch (CloudWatch), y los informes de incidentes o las solicitudes de servicio que envíes. Se pueden realizar varias llamadas de servicio y actividades a nivel de anfitrión para cada acceso.

La justificación del acceso, los activadores y el iniciador del disparador se muestran en la siguiente tabla.

Activadores de acceso

| Acceso | Initiator | Desencadenador |
|---|---|---|
| Aplicación de parches | AMS | Problema con el parche |
| Investigación de problemas internos | AMS | Problema problemático (un problema que se ha identificado como sistémico) |

| Acceso | Initiator | Desencadenador |
| --- | --- | --- |
| Investigación y solución de alertas | AMS | Elementos de trabajo operativos (SSM OpsItems) de AWS Systems Manager |
| Investigación y solución de incidentes | You | Caso de soporte entrante (una solicitud de servicio o incidente que envíes) |
| Cumplimiento de una solicitud de servicio entrante | You | |

## Funciones de IAM para el acceso a la cuenta de los clientes de AMS

Los operadores de AMS requieren las siguientes funciones para gestionar tu cuenta.

> **Note**
>
> Las funciones de acceso a AMS permiten a los operadores de AMS acceder a sus recursos para proporcionar las capacidades de AMS (consulteDescripción del servicio). La modificación de estas funciones puede inhibir nuestra capacidad de proporcionar estas capacidades. Si necesita modificar las funciones de acceso a AMS, consulte a su arquitecto de nube.

Funciones de IAM para el acceso de AMS a las cuentas de los clientes

| Nombre de función | Description (Descripción) |
| --- | --- |
| ams-access-admin | Este rol tiene acceso administrativo completo a su cuenta sin restricciones. Los servicios de AMS utilizan esta función con políticas de sesión restrictivas que limitan el acceso para implementar la infraestructura de AMS y administrar su cuenta. |
| ams-access-admin-operations | Esta función otorga a los operadores de AMS permisos administrativos para administrar su cuenta. Esta función no concede permisos de lectura, escritura o eliminación del contenido de los clientes en los |

| Nombre de función | Description (Descripción) |
| --- | --- |
| | AWS servicios que se utilizan habitualmente como almacenes de datos, como Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift y Amazon. ElastiCache Solo los operadores de AMS cualificados que tengan sólidos conocimientos y experiencia en la gestión de acceso pueden asumir esta función. Estos operadores sirven como punto de referencia para los problemas de administración de acceso y acceden a sus cuentas para solucionar los problemas de acceso de los operadores de AMS. |
| ams-access-management | Se implementa manualmente durante la incorporación. El sistema AMS Access requiere esta función para gestionarla `ams-access-roles` y `ams-access-managed-policies` apilarla. |
| ams-access-operations | Este rol tiene permisos para realizar tareas administrativas en sus cuentas. Este rol no tiene permisos de lectura, escritura o eliminación del contenido de los clientes en los AWS servicios que se utilizan habitualmente como almacenes de datos, como Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift y Amazon. ElastiCache Los permisos para realizar operaciones de AWS Identity and Access Management escritura también están excluidos de esta función. El personal de operaciones y los arquitectos de la nube de AMS Accelerate (CAs) pueden asumir esta función. |

| Nombre de función | Description (Descripción) |
| --- | --- |
| ams-access-read-only | Este rol tiene acceso de solo lectura a su cuenta. El personal de operaciones y los arquitectos de la nube de AMS Accelerate (CAs) pueden asumir esta función. Los permisos de lectura del contenido de los clientes en los AWS servicios que se utilizan habitualmente como almacenes de datos, como Amazon S3, Amazon RDS, DynamoDB o Amazon Redshift ElastiCache, y no tienen esta función. |
| ams-access-security-analyst | Esta función de seguridad de AMS tiene permisos en su cuenta de AMS para realizar una supervisión específica de las alertas de seguridad y gestionar los incidentes de seguridad. Solo unas pocas personas selectas de AMS Security pueden asumir esta función. |
| ams-access-security-analyst-de solo lectura | Esta función de seguridad de AMS se limita a los permisos de solo lectura en su cuenta de AMS para realizar una supervisión específica de las alertas de seguridad y gestionar los incidentes de seguridad. |

> **Note**
>
> Esta es la plantilla del rol. ams-access-management Es la pila que los arquitectos de nube (CAs) implementan manualmente en tu cuenta en el momento de la incorporación: management-role.yaml.
> Esta es la plantilla para los distintos roles de acceso para los distintos niveles de acceso:,,,: accelerate-roles.json. ams-access-read-only ams-access-operations ams-access-admin-operations ams-access-admin

## Cómo accede AMS a tu cuenta

Los operadores de AMS Accelerate pueden acceder a la consola y a las instancias de su cuenta en determinadas circunstancias.

Los operadores de AMS utilizan el servicio de acceso interno AMS Accelerate para acceder a sus cuentas de forma segura y auditada. Para acceder a sus instancias, los operadores de AMS utilizan el mismo servicio de acceso interno a AMS que el intermediario y, una vez concedido el acceso, los operadores de AMS Accelerate utilizan el administrador de sesiones SSM para acceder mediante credenciales de sesión. El acceso RDP para las instancias de Windows se proporciona mediante el establecimiento del reenvío de puertos a la instancia y la creación de un usuario local mediante SSM. Las credenciales del usuario local se utilizan para el acceso RDP y se eliminan al final de la sesión.

## Cómo y cuándo usar la cuenta de usuario root en AMS

El usuario raíz es el superusuario de su AWS cuenta. AMS monitorea el uso de root. Le recomendamos que utilice root solo para las pocas tareas que lo requieran, por ejemplo: cambiar la configuración de la cuenta, activar el acceso AWS Identity and Access Management (IAM) a la facturación y la gestión de costes, cambiar la contraseña raíz y habilitar la autenticación multifactor (MFA). Consulte las tareas que requieren credenciales de usuario raíz en la Guía del AWS Identity and Access Management usuario.

Rootee con AMS Accelerate:

AMS no le prohíbe usar su cuenta de usuario root. Sin embargo, AMS Operations and Security considera que su uso es una cuestión que debe investigarse y nos pondremos en contacto con su equipo de seguridad cada vez que lo utilice.

Le recomendamos que se ponga en contacto con su CSDM y su CA con veinticuatro horas de antelación para informarles sobre las tareas de acceso a la raíz que piensa realizar.

Respuesta de seguridad y operaciones de AMS al uso de root:

AMS recibe una alarma cuando se utiliza la cuenta de usuario raíz. Si el uso de las credenciales raíz no está programado, se ponen en contacto con el equipo de seguridad de AMS y con el equipo de su cuenta para comprobar si se trata de una actividad esperada. Si no es una actividad prevista, AMS trabaja con su equipo de seguridad para investigar el problema.

# Gestión de la seguridad en AMS Accelerate

AWS Managed Services utiliza varios controles para proteger sus activos de información y ayudarle a mantener segura su AWS infraestructura. AMS Accelerate mantiene una biblioteca de medidas correctivas Reglas de AWS Config y de medidas correctivas para garantizar que todas sus cuentas cumplan con los estándares del sector en materia de seguridad e integridad operativa. Reglas de AWS Config realiza un seguimiento continuo del cambio de configuración entre sus recursos registrados. Si un cambio infringe alguna de las condiciones de la regla, AMS informa de sus conclusiones y permite subsanar las infracciones de forma automática o previa solicitud, en función de la gravedad de la infracción. Reglas de AWS Config facilitar el cumplimiento de los estándares establecidos por: el Centro de Seguridad de Internet (CIS), el Marco de Seguridad en la Nube (CSF) del Instituto Nacional de Estándares y Tecnología (NIST), la Ley de Portabilidad y Responsabilidad de los Seguros de Salud (HIPAA) y el Estándar de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI).

Además, AMS utiliza Amazon GuardDuty para identificar actividades potencialmente no autorizadas o maliciosas en su AWS entorno. AMS monitorea los GuardDuty hallazgos las 24 horas del día, los 7 días AMS colabora con usted para comprender el impacto de los hallazgos e identificar las medidas correctivas basándose en las recomendaciones de las mejores prácticas. AMS también utiliza Amazon Macie para proteger sus datos confidenciales, como la información de salud personal (PHI), la información de identificación personal (PII) y los datos financieros.

> **Note**
>
> Amazon Macie es un servicio opcional y no está activado de forma predeterminada.

AMS Accelerate ofrece una gama de servicios operativos para ayudarlo a alcanzar la excelencia operativa en AWS. Para obtener más información sobre cómo AMS ayuda a sus equipos a alcanzar la excelencia operativa general Nube de AWS con las principales capacidades operativas de AMS, que incluyen el servicio de asistencia las 24 horas del día, los 7 días de la semana, la supervisión proactiva, la seguridad, la aplicación de parches, el registro y la copia de seguridad, consulte los diagramas de arquitectura de referencia de AMS.

Temas


- Utilice el documento SSM de Log4j para descubrir incidencias en Accelerate
- Supervisión de la seguridad de la infraestructura en AMS

- Protección de datos en Accelerate
- AWS Identity and Access Management en AMS Accelerate
- Respuesta a incidentes de seguridad en AMS
- Registro y supervisión de eventos de seguridad en Accelerate
- Cumplimiento de la configuración en Accelerate
- Respuesta a incidentes en Accelerate
- Resiliencia en Accelerate
- Control de seguridad para sistemas end-of-support operativos
- Mejores prácticas de seguridad en Accelerate
- Revisiones de seguridad de la solicitud de cambios
- Preguntas frecuentes sobre seguridad

# Utilice el documento SSM de Log4j para descubrir incidencias en Accelerate

El documento Log4j ( AWS Systems Manager documento SSM) le ayuda a buscar la biblioteca Log4j2 de Apache en las cargas de trabajo ingeridas. El documento de automatización proporciona un informe del ID de proceso de las aplicaciones Java en las que está activa la biblioteca Log4j2.

El informe incluye información sobre los archivos Java (archivos JAR), que se encuentran en el entorno especificado que contiene la clase. JndiLookup Se recomienda actualizar las bibliotecas descubiertas a la última versión disponible. Esta actualización mitiga la ejecución remota de código (RCE) identificada en el CVE-2021-44228. Descargue la última versión de la biblioteca Log4j de Apache. Para obtener más información, consulte Descargar Apache Log4j 2.

El documento se comparte con todas las regiones incorporadas a Accelerate,. Para acceder al documento, complete los siguientes pasos:

1. Abra la AWS Systems Manager consola en https://console.aws.amazon.com/systems-manager/.
2. En el panel de navegación, elija Documentos.
3. Selecciona Compartido conmigo.
4. En el cuadro de búsqueda, escribe AWSManagedServices-GatherLog4JInformation.
5. Utilice el control de velocidad para ejecutar el documento a escala.

El documento AWSManagedServices-GatherLog 4JInformation recopila los siguientes parámetros:

- InstanceId: (Obligatorio) ID de su instancia. EC2
- S3Bucket: (opcional) La URL o URI de S3 prefirmada de S3 (s3://BUCKET_NAME) en la que se van a cargar los resultados.
- AutomationAssumeRole: (Obligatorio) El ARN del rol que permite a la automatización realizar acciones en tu nombre.

Se recomienda ejecutar este documento mediante el control de velocidad. Puede configurar el parámetro de control de velocidad como el InstanceIdy asignarle una lista de instancias o aplicar una combinación de etiquetas y teclas para seleccionar todas las EC2 instancias que tengan una etiqueta determinada. AWS Managed Services también recomienda que proporcione un bucket de Amazon Simple Storage Service (Amazon S3) en el que cargar los resultados, de modo que pueda crear un informe a partir de los datos almacenados en S3. Para ver un ejemplo de cómo agregar los resultados en S3, consulte EC2 Instance Stack | Gather Log4j Information.

Si no puede actualizar el paquete, siga las pautas descritas en AWS Seguridad al utilizar los servicios de AWS seguridad para protegerse, detectar y responder a la vulnerabilidad de Log4j. Para mitigar las vulnerabilidades eliminando la funcionalidad de JndiLookup clase, ejecute el parche activo de Log4j en línea con sus aplicaciones Java. Para obtener más información sobre el hotpatch, consulte Hotpatch para Apache Log4j.

Si tienes dudas sobre el resultado de la automatización o sobre cómo proceder con otras mitigaciones, envía una solicitud de servicio.

## Supervisión de la seguridad de la infraestructura en AMS

Cuando se incorpora a AMS Accelerate e AWS implementa la siguiente infraestructura AWS Config básica y conjunto de reglas, AMS Accelerate utiliza estas reglas para supervisar sus cuentas.

- AWS Config función vinculada al servicio: AMS Accelerate despliega la función vinculada al servicio denominada AWSServiceRoleForConfig, que se utiliza AWS Config para consultar el estado de otros servicios. AWS El rol AWSServiceRoleForConfigvinculado al servicio confía en que el servicio asuma el rol. AWS Config La política de permisos del AWSServiceRoleForConfigrol contiene permisos de solo lectura y solo escritura para los recursos y permisos de solo lectura AWS Config para los recursos de otros servicios compatibles. AWS Config Si ya tiene un rol configurado con AWS Config Recorder, AMS Accelerate valida que el rol existente tenga una

política administrada de AWS Config adjunta. De lo contrario, AMS Accelerate reemplaza el rol por el rol vinculado al servicio. AWSServiceRoleForConfig

- AWS Config grabador y canal de entrega: AWS Config utiliza el grabador de configuración para detectar los cambios en las configuraciones de los recursos y capturarlos como elementos de configuración. AMS Accelerate implementa el grabador de configuración en todos los servicios Regiones de AWS, con un registro continuo de todos los recursos. AMS Accelerate también crea el canal de entrega de configuraciones, un bucket de Amazon S3, que se utiliza para registrar los cambios que se producen en AWS los recursos. El grabador de configuración actualiza los estados de configuración a través del canal de entrega. La grabadora de configuración y el canal de entrega son necesarios AWS Config para que funcionen. AMS Accelerate crea la grabadora en un todo Regiones de AWS y un canal de entrega en uno solo Región de AWS. Si ya tiene una grabadora y un canal de entrega en una Región de AWS, AMS Accelerate no elimina los AWS Config recursos existentes, sino que AMS Accelerate utiliza la grabadora y el canal de entrega existentes tras comprobar que están configurados correctamente. Para obtener más información sobre cómo reducir AWS Config los costes, consulteReduzca AWS Config los costos en Accelerate.
- AWS Config normas: AMS Accelerate mantiene una biblioteca de medidas correctivas Reglas de AWS Config y correctivas para ayudarle a cumplir con los estándares del sector en materia de seguridad e integridad operativa. Reglas de AWS Config realiza un seguimiento continuo de los cambios de configuración de sus recursos registrados. Si un cambio infringe alguna de las condiciones de la regla, AMS informa de sus conclusiones y permite subsanar las infracciones de forma automática o previa solicitud, en función de la gravedad de la infracción. Reglas de AWS Config facilitar el cumplimiento de los estándares establecidos por: el Centro de Seguridad de Internet (CIS), el Marco de Seguridad en la Nube (CSF) del Instituto Nacional de Estándares y Tecnología (NIST), la Ley de Portabilidad y Responsabilidad de los Seguros de Salud (HIPAA) y el Estándar de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI).
- AWS Config autorización del agregador: un agregador es un tipo de AWS Config recurso que recopila datos de AWS Config configuración y conformidad de varias cuentas y regiones. AMS Accelerate incorpora su cuenta a un agregador de configuraciones a partir del cual AMS Accelerate agrega la información de configuración de los recursos y los datos de cumplimiento de la configuración de su cuenta y genera el informe de cumplimiento. Si hay agregadores configurados en la cuenta propiedad de AMS, AMS Accelerate despliega un agregador adicional y el agregador existente no se modifica.

> **Note**
>
> El agregador Config no está configurado en sus cuentas; más bien, está configurado en cuentas propiedad de AMS y sus cuentas están incorporadas a él.

Para obtener más información, consulta: AWS Config

- AWS Config: ¿Qué es Config?
- Reglas de AWS Config: Evaluación de recursos con reglas
- Reglas de AWS Config: Verificación dinámica de la conformidad: Reglas de AWS Config — Verificación dinámica de la conformidad para los recursos en la nube
- AWS Config Agregador: agregación de datos multirregional y multicuenta

Para obtener información sobre los informes, consulte. AWS Config Informe de cumplimiento de controles

## Uso de funciones vinculadas a servicios para AMS Accelerate

AMS Accelerate utiliza roles AWS Identity and Access Management vinculados al servicio (IAM). Un rol vinculado a un servicio (SLR) es un tipo único de rol de IAM que está vinculado directamente a AMS Accelerate. AMS Accelerate predefine las funciones vinculadas al servicio e incluyen todos los permisos que el servicio necesita para llamar a otros servicios en su nombre. AWS

Un rol vinculado a un servicio facilita la configuración de AMS Accelerate, ya que no es necesario añadir manualmente los permisos necesarios. AMS Accelerate define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AMS Accelerate puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM.

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulte los AWS servicios que funcionan con IAM y busque los servicios con la opción Sí en la columna Funciones vinculadas a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

## Kit de herramientas de despliegue: función vinculada a los servicios para AMS Accelerate

AMS Accelerate utiliza el denominado rol vinculado a servicios (SLR) AWSServiceRoleForAWSManagedServicesDeploymentToolkit: este rol implementa la infraestructura de AMS Accelerate en las cuentas de los clientes.

> **Note**
>
> Esta política se actualizó recientemente; para obtener más información, consulte. Acelere las actualizaciones de las funciones vinculadas al servicio

Kit de herramientas de despliegue AMS Accelerate SLR

El rol AWSService RoleFor AWSManaged ServicesDeploymentToolkit vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `deploymenttoolkit.managedservices.amazonaws.com`

La política denominada AWSManagedServicesDeploymentToolkitPolicypermite a AMS Accelerate realizar acciones en los siguientes recursos:

- `arn:aws*:s3:::ams-cdktoolkit*`
- `arn:aws*:cloudformation:*:*:stack/ams-cdk-toolkit*`
- `arn:aws:ecr:*:*:repository/ams-cdktoolkit*`

Esta SLR concede a Amazon S3 permisos para crear y gestionar el depósito de despliegue que utiliza AMS para cargar recursos, como CloudFormation plantillas o paquetes de activos de Lambda, en la cuenta para las implementaciones de componentes. Esta SLR otorga CloudFormation permisos para implementar la CloudFormation pila que define los segmentos de implementación. Para obtener más información o descargar la política, consulte. AWSManagedServices_DeploymentToolkitPolicy

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un kit de herramientas de despliegue SLR para AMS Accelerate

No necesita crear manualmente un rol vinculado a servicios. Cuando se incorpora a AMS en la Consola de administración de AWS, la API o la AWS API AWS CLI, AMS Accelerate crea automáticamente la función vinculada al servicio.

> **Important**
>
> Esta función vinculada al servicio puede aparecer en su cuenta si utilizaba el servicio AMS Accelerate antes del 9 de junio de 2022, cuando comenzó a ofrecer funciones vinculadas al servicio y, posteriormente, AMS Accelerate creó la función en su cuenta. AWSService RoleFor AWSManaged ServicesDeploymentToolkit Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta de IAM.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando te incorporas a AMS, AMS Accelerate vuelve a crear el rol vinculado al servicio para ti.

Edición de un kit de herramientas de despliegue (SLR) para AMS Accelerate

AMS Accelerate no permite editar el rol vinculado al AWSService RoleFor AWSManaged ServicesDeploymentToolkit servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminar un kit de herramientas de despliegue (SLR) para AMS Accelerate

No es necesario eliminar el rol manualmente. AWSService RoleFor AWSManaged ServicesDeploymentToolkit Cuando te desconectas de AMS en la Consola de administración de AWS AWS CLI, la API o la AWS API, AMS Accelerate limpia los recursos y elimina automáticamente la función vinculada al servicio.

También puede utilizar la consola de IAM AWS CLI o la AWS API para eliminar manualmente el rol vinculado al servicio. Para ello, primero debe limpiar manualmente los recursos del rol vinculado al servicio para poder eliminarlo después manualmente.

> **Note**
>
> Si el servicio AMS Accelerate utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de AMS Accelerate utilizados por el rol AWSService RoleFor AWSManaged ServicesDeploymentToolkit vinculado al servicio

Elimine la `ams-cdk-toolkit` pila de todas las regiones en las que estaba integrada su cuenta en AMS (puede que primero tenga que vaciar manualmente los depósitos de S3).

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Usa la consola de IAM AWS CLI, la o la AWS API para eliminar el rol vinculado al servicio. AWSService RoleFor AWSManaged ServicesDeploymentToolkit Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

## El Detective controla la función vinculada al servicio para AMS Accelerate

AMS Accelerate usa el rol vinculado al servicio (SLR) denominado AWSServiceRoleForManagedServices_DetectiveControlsConfig: AWS Managed Services usa este rol vinculado al servicio para implementar el registrador de configuraciones, las reglas de configuración y los controles de S3 bucket detective.

La siguiente política administrada se adjunta a la AWSServiceRoleForManagedServices_DetectiveControlsConfigfunción vinculada al servicio: _. AWSManagedServices_DetectiveControlsConfig ServiceRolePolicy Para obtener actualizaciones de esta política, consulte Acelere las actualizaciones de las políticas AWS gestionadas.

Permisos para Detective Controls SLR para AMS Accelerate

El rol AWSServiceRoleForManagedServices_DetectiveControlsConfig vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `detectivecontrols.managedservices.amazonaws.com`

Esta función incluye la política `AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy` AWS

gestionada (consulte AWS política gestionada: _ AWSManagedServices_DetectiveControlsConfig ServiceRolePolicy El servicio utiliza la función para crear y configurar AMS Detective Controls en su cuenta, lo que requiere el despliegue de recursos como depósitos s3, reglas de configuración y un agregador). Debe configurar los permisos para permitir que una entidad de IAM (como un usuario, un grupo o un rol) cree, edite o elimine un rol vinculado a un servicio. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de AWS Identity and Access Management.

Creación de una cámara réflex de control de detectives para AMS Accelerate

No necesita crear manualmente un rol vinculado a servicios. Cuando te incorporas a AMS en la Consola de administración de AWS, la AWS CLI API o la AWS API, AMS Accelerate crea automáticamente la función vinculada al servicio.

> **Important**
>
> Esta función vinculada al servicio puede aparecer en su cuenta si utilizaba el servicio AMS Accelerate antes del 9 de junio de 2022, cuando comenzó a ofrecer funciones vinculadas al servicio y, posteriormente, AMS Accelerate creó la función en su cuenta. AWSServiceRoleForManagedServices_DetectiveControlsConfig Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta de IAM.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando te incorporas a AMS, AMS Accelerate vuelve a crear el rol vinculado al servicio para ti.

Edición de una cámara réflex de control de detectives para AMS Accelerate

AMS Accelerate no permite editar el rol vinculado al AWSServiceRoleForManagedServices_DetectiveControlsConfig servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminar una cámara réflex de control de detectives para AMS Accelerate

No es necesario eliminar el AWSServiceRoleForManagedServices_DetectiveControlsConfig rol manualmente. Cuando te desconectas de AMS en la Consola de administración de AWS AWS CLI,

la API o la AWS API, AMS Accelerate limpia los recursos y elimina automáticamente la función vinculada al servicio.

También puede utilizar la consola de IAM AWS CLI o la AWS API para eliminar manualmente el rol vinculado al servicio. Para ello, primero debe limpiar manualmente los recursos del rol vinculado al servicio para poder eliminarlo después manualmente.

> **Note**
>
> Si el servicio AMS Accelerate utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de AMS Accelerate utilizados por el rol AWSServiceRoleForManagedServices_DetectiveControlsConfig vinculado al servicio

Elimine `ams-detective-controls-config-recorder` `ams-detective-controls-config-rules-cdk` y `ams-detective-controls-infrastructure-cdk` acumule elementos de todas las regiones en las que estaba integrada su cuenta en AMS (puede que primero tenga que vaciar manualmente los depósitos de S3).

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Usa la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al servicio. AWSServiceRoleForManagedServices_DetectiveControlsConfig Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

## Amazon regula EventBridge la función vinculada al servicio para AMS Accelerate

AMS Accelerate utiliza el rol vinculado al servicio (SLR) denominado. AWSServiceRoleForManagedServices_Events Esta función confía en uno de los directores del servicio AWS Managed Services (events.managedservices.amazonaws.com) para que asuma la función por usted. El servicio usa el rol para crear una regla EventBridge gestionada por Amazon. Esta regla es la infraestructura necesaria en su cuenta de AWS para enviar la información sobre el cambio de estado de alarma de su cuenta a AWS Managed Services.

Permisos de EventBridge SLR para AMS Accelerate

El rol AWSServiceRoleForManagedServices_Events vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `events.managedservices.amazonaws.com`

Esta función incluye la política `AWSManagedServices_EventsServiceRolePolicy` AWS gestionada (consulteAWS política gestionada: AWSManagedServices_EventsServiceRolePolicy). El servicio utiliza la función para enviar información sobre los cambios en el estado de alarma de su cuenta a AMS. Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de AWS Identity and Access Management .

Puede descargar el JSON AWSManagedServices_EventsServiceRolePolicy en este ZIP: EventsServiceRolePolicy.zip.

Creación de una cámara EventBridge réflex para AMS Accelerate

No necesita crear manualmente un rol vinculado a servicios. Cuando te incorporas a AMS en la Consola de administración de AWS, la AWS CLI API o la AWS API, AMS Accelerate crea automáticamente la función vinculada al servicio.

> **Important**
>
> Esta función vinculada al servicio puede aparecer en su cuenta si utilizaba el servicio AMS Accelerate antes del 7 de febrero de 2023, cuando comenzó a ofrecer funciones vinculadas al servicio y, posteriormente, AMS Accelerate creó la función en su cuenta. AWSServiceRoleForManagedServices_Events Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta de IAM.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando te incorporas a AMS, AMS Accelerate vuelve a crear el rol vinculado al servicio para ti.

Edición de una cámara EventBridge réflex para AMS Accelerate

AMS Accelerate no permite editar el rol vinculado al AWSServiceRoleForManagedServices_Events servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminar una cámara EventBridge réflex para AMS Accelerate

No es necesario eliminar el AWSServiceRoleForManagedServices_Events rol manualmente. Cuando te desconectas de AMS en la Consola de administración de AWS AWS CLI, la API o la AWS API, AMS Accelerate limpia los recursos y elimina automáticamente la función vinculada al servicio.

También puede utilizar la consola de IAM AWS CLI o la AWS API para eliminar manualmente el rol vinculado al servicio. Para ello, primero debe limpiar manualmente los recursos del rol vinculado al servicio para poder eliminarlo después manualmente.

> **Note**
>
> Si el servicio AMS Accelerate utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de AMS Accelerate utilizados por el rol AWSServiceRoleForManagedServices_Events vinculado al servicio

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRoleForManagedServices_Events servicio. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

## Contacta con el rol vinculado al servicio para AMS Accelerate

AMS Accelerate utiliza la función vinculada al servicio (SLR) denominada AWSServiceRoleForManagedServices_Contacts: esta función facilita las notificaciones automáticas cuando se producen incidentes, ya que permite al servicio leer las etiquetas existentes del recurso afectado y recuperar el correo electrónico configurado del punto de contacto correspondiente.

Este es el único servicio que utiliza este rol vinculado al servicio.

Adjunta a la función AWSServiceRoleForManagedServices_Contactsvinculada al servicio se encuentra la siguiente política administrada:. AWSManagedServices_ContactsServiceRolePolicy Para obtener actualizaciones de esta política, consulte Acelere las actualizaciones de las políticas AWS gestionadas.

### Permisos para Contacts SLR para AMS Accelerate

El rol AWSServiceRoleForManagedServices_Contacts vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `contacts-service.managedservices.amazonaws.com`

Esta función incluye la política gestionada de `AWSManagedServices_ContactsServiceRolePolicy` AWS (consulteAWS política gestionada: AWSManagedServices_ContactsServiceRolePolicy). El servicio utiliza la función para leer las etiquetas de cualquier AWS recurso y encontrar el correo electrónico contenido en la etiqueta, del punto de contacto adecuado para cuando se produzcan incidentes. Esta función facilita las notificaciones automáticas cuando se producen incidentes, ya que permite a AMS leer esa etiqueta en un recurso afectado y recuperar el correo electrónico. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de AWS Identity and Access Management.

> **Important**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. AMS utiliza etiquetas para proporcionarle servicios de administración. Las etiquetas no se han diseñado para usarse con información privada o confidencial.

La política de permisos de roles denominada AWSManagedServices_ContactsServiceRolePolicy permite a AMS Accelerate realizar las siguientes acciones en los recursos especificados:

- Acción: permite que el servicio de contactos lea las etiquetas configuradas específicamente para contener el correo electrónico para que AMS envíe notificaciones de incidentes a cualquier recurso de AWS.

Puede descargar el JSON AWSManagedServices_ContactsServiceRolePolicy en este ZIP: ContactsServicePolicy.zip.

Creación de una cámara réflex de contactos para AMS Accelerate

No necesita crear manualmente un rol vinculado a servicios. Cuando te incorporas a AMS en la Consola de administración de AWS, la AWS CLI API o la AWS API, AMS Accelerate crea automáticamente la función vinculada al servicio.

> **Important**
>
> Esta función vinculada al servicio puede aparecer en su cuenta si utilizaba el servicio AMS Accelerate antes del 16 de febrero de 2023, cuando comenzó a ofrecer funciones vinculadas al servicio y, posteriormente, AMS Accelerate creó la función en su cuenta. AWSServiceRoleForManagedServices_Contacts Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta de IAM.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando te incorporas a AMS, AMS Accelerate vuelve a crear el rol vinculado al servicio para ti.

Edición de una cámara réflex de contactos para AMS Accelerate

AMS Accelerate no permite editar el rol vinculado al AWSServiceRoleForManagedServices_Contacts servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminar una cámara réflex de contactos para AMS Accelerate

No es necesario que elimines el AWSServiceRoleForManagedServices_Contacts rol manualmente. Cuando te desconectas de AMS en la Consola de administración de AWS AWS CLI, la API o la AWS API, AMS Accelerate limpia los recursos y elimina automáticamente la función vinculada al servicio.

También puede utilizar la consola de IAM AWS CLI o la AWS API para eliminar manualmente el rol vinculado al servicio. Para ello, primero debe limpiar manualmente los recursos del rol vinculado al servicio para poder eliminarlo después manualmente.

> **Note**
>
> Si el servicio AMS Accelerate utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de AMS Accelerate utilizados por el rol AWSServiceRoleForManagedServices_Contacts vinculado al servicio

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRoleForManagedServices_Contacts servicio. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

## Regiones compatibles con las funciones vinculadas al servicio de AMS Accelerate

AMS Accelerate admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio esté disponible. Para obtener más información, consulte Puntos de enlace y regiones de AWS.

## Acelere las actualizaciones de las funciones vinculadas al servicio

Consulte los detalles sobre las actualizaciones de las funciones vinculadas al servicio de Accelerate desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página AccelerateHistorial de documentos de la Guía del usuario de AMS Accelerate.

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Política actualizada: kit de herramientas de implementación | • Se agregaron estos nuevos permisos para el recurso`arn:aws:ecr:*:*:repository/ams-cdktoolkit*` :<br>`ecr:BatchGetRepositoryScanningConfiguration`<br>`ecr:PutImageScanningConfiguration` | 4 de abril de 2024 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Política actualizada: kit de herramientas de implementación | • Se agregaron estos nuevos permisos para el recurso `arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*` :<br>`cloudformation:DeleteChangeSet`<br>`cloudformation:DescribeStackEvents`<br>`cloudformation:GetTemplate`<br>`cloudformation:TagResource`<br>`cloudformation:UntagResource`<br>• Se agregaron estos nuevos permisos para el recurso `arn:aws:ecr:*:*:repository/ams-cdktoolkit*` :<br>`ecr:CreateRepository`<br>`ecr:DeleteLifecyclePolicy`<br>`ecr:DeleteRepository`<br>`ecr:DeleteRepositoryPolicy`<br>`ecr:DescribeRepositories`<br>`ecr:GetLifecyclePolicy`<br>`ecr:ListTagsForResource`<br>`ecr:PutImageTagMutability`<br>`ecr:PutLifecyclePolicy`<br>`ecr:SetRepositoryPolicy`<br>`ecr:TagResource`<br>`ecr:UntagResource`<br>• Además, algunas acciones existentes con caracteres comodín se redujeron a acciones individuales:<br>`- s3:DeleteObject*`<br>`+ s3:DeleteObject`<br>`+ s3:DeleteObjectTagging`<br>`+ s3:DeleteObjectVersion`<br>`+ s3:DeleteObjectVersionTagging`<br><br>`- s3:GetObject*`<br>`+ s3:GetObject`<br>`+ s3:GetObjectAcl`<br>`+ s3:GetObjectAttributes` | 9 de mayo de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| | <pre>+ s3:GetObjectLegalHold<br>+ s3:GetObjectRetention<br>+ s3:GetObjectTagging<br>+ s3:GetObjectVersion<br>+ s3:GetObjectVersionAcl<br>+ s3:GetObjectVersionAttributes<br>+ s3:GetObjectVersionForReplication<br>+ s3:GetObjectVersionTagging<br>+ s3:GetObjectVersionTorrent<br><br>- cloudformation:UpdateTermination*<br>+ cloudformation:UpdateTerminationProt<br>ection</pre> | |
| Política actualizada — Detective Controls | • Las CloudFormation acciones se han reducido aún más tras la confirmación con el equipo de seguridad y acceso<br>• Las acciones de Lambda se han eliminado de la política porque no afectan al embarque. onboarding/off | 10 de abril de 2023 |
| Política actualizada — Detective Controls | Se actualizó la política y se agregó la política de límites de permisos. | 21 de marzo de 2023 |
| Nueva función vinculada al servicio: Contacts SLR | Accelerate agregó un nuevo rol vinculado al servicio para el servicio de contactos.<br><br>Esta función facilita las notificaciones automáticas cuando se producen incidentes, ya que permite al servicio leer las etiquetas existentes del recurso afectado y recuperar el correo electrónico configurado del punto de contacto correspondiente. | 16 de febrero de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Nueva función vinculada al servicio: EventBridge | Accelerate agregó un nuevo rol vinculado a un servicio para una regla de Amazon EventBridge .<br><br>Esta función confía en uno de los directores del servicio AWS Managed Services (events.managedservices.amazonaws.com) para que asuma la función por usted. El servicio usa el rol para crear una regla EventBridge gestionada por Amazon. Esta regla es la infraestructura necesaria en su cuenta de AWS para enviar la información sobre el cambio de estado de alarma de su cuenta a AWS Managed Services. | 7 de febrero de 2023 |
| Función vinculada al servicio actualizada: kit de herramientas de implementación | Accelerate se actualiza AWSService RoleFor AWSManaged ServicesDeploymentToolkit con los nuevos permisos de S3.<br><br>Se agregaron los siguientes permisos nuevos:<br><br>`"s3:GetLifecycleConfiguration", "s3:GetBucketLogging", "s3:ListBucket", "s3:GetBucketVersioning", "s3:PutLifecycleConfiguration", "s3:GetBucketLocation", "s3:GetObject*"` | 30 de enero de 2023 |
| Accelerate comenzó a rastrear los cambios | Accelerate comenzó a realizar un seguimiento de los cambios en sus funciones vinculadas al servicio. | 30 de noviembre de 2022 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Nueva función vinculada al servicio: Detective Controls | Accelerate agregó una nueva función vinculada al servicio para implementar los controles de detección de Accelerate.<br><br>AWS Managed Services utiliza esta función vinculada a un servicio para implementar controles de registro de configuración, reglas de configuración y detección de cubos de S3. | 13 de octubre de 2022 |
| Nuevo rol vinculado a los servicios: kit de herramientas de implementación | Accelerate agregó una nueva función vinculada al servicio para implementar la infraestructura de Accelerate.<br><br>esta función implementa la infraestructura AMS Accelerate en las cuentas de los clientes. | 9 de junio de 2022 |

## AWS políticas gestionadas para AMS Accelerate

Una política AWS gestionada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

Para ver una tabla de cambios, consulteAcelere las actualizaciones de las políticas AWS gestionadas.

## AWS política gestionada: AWSManagedServices_AlarmManagerPermissionsBoundary

AWS Managed Services (AMS) usa la política `AWSManagedServices_AlarmManagerPermissionsBoundary` AWS administrada. Esta política AWS gestionada se utiliza en AWSManagedServices_AlarmManager _ ServiceRolePolicy para restringir los permisos de las funciones de IAM creadas por. AWSServiceRoleForManagedServices_AlarmManager

Esta política otorga a las funciones de IAM creadas como parte de ellas Cómo funciona Alarm Manager permisos para realizar operaciones como la evaluación de AWS Config, la configuración de AWS Config read to fetch Alarm Manager y la creación de las alarmas de Amazon CloudWatch necesarias.

La `AWSManagedServices_AlarmManagerPermissionsBoundary` política está asociada a la función vinculada al `AWSServiceRoleForManagedServices_DetectiveControlsConfig` servicio. Para ver las actualizaciones de este rol, consulte. Acelere las actualizaciones de las funciones vinculadas al servicio

Puede adjuntar esta política a sus identidades de IAM.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `AWS Config`— Permite permisos para evaluar las reglas de configuración y seleccionar la configuración de los recursos.
- `AWS AppConfig`— Permite permisos para recuperar la AlarmManager configuración.
- `Amazon S3`— Permite permisos para operar AlarmManager depósitos y objetos.
- `Amazon CloudWatch`— Permite permisos para leer y colocar las alarmas y métricas AlarmManager gestionadas.
- `AWS Resource Groups and Tags`— Permite permisos para leer las etiquetas de los recursos.
- `Amazon EC2`— Permite permisos para leer los EC2 recursos de Amazon.
- `Amazon Redshift`— Permite permisos para leer instancias y clústeres de Redshift.
- `Amazon FSx`— Permite permisos para describir los sistemas de archivos, los volúmenes y las etiquetas de recursos.

- `Amazon CloudWatch Synthetics`— Permite permisos para leer los recursos de Synthetics.
- `Amazon Elastic Kubernetes Service`— Permite permisos para describir el clúster de Amazon EKS.
- `Amazon ElastiCache`— Permite permisos para describir los recursos.

Puede descargar el archivo de la política en este ZIP: RecommendedPermissionBoundary.zip.

## AWS política gestionada: _ AWSManagedServices_DetectiveControlsConfig ServiceRolePolicy

AWS Managed Services (AMS) usa la política `AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy` AWS administrada. Esta política AWS gestionada está asociada a la función `AWSServiceRoleForManagedServices_DetectiveControlsConfig` vinculada al servicio (consulte). El Detective controla la función vinculada al servicio para AMS Accelerate Para ver las actualizaciones de la función vinculada al `AWSServiceRoleForManagedServices_DetectiveControlsConfig` servicio, consulte. Acelere las actualizaciones de las funciones vinculadas al servicio

La política permite al rol vinculado al servicio completar acciones en su lugar.

Puede adjuntar la ServiceRolePolicy política AWSManagedServices_DetectiveControlsConfig _ a sus entidades de IAM.

Para obtener más información, consulte Uso de funciones vinculadas a servicios para AMS Accelerate.

Detalles de los permisos

Esta política tiene los siguientes permisos para permitir a AWS Managed Services Detective Controls implementar y configurar todos los recursos necesarios.

- `CloudFormation`— Permite a AMS Detective Controls desplegar CloudFormation pilas con recursos como depósitos s3, reglas de configuración y grabador de configuración.
- `AWS Config`— Permite a AMS Detective Controls crear reglas de configuración de AMS, configurar un agregador y etiquetar recursos.
- `Amazon S3`— permite a AMS Detective Controls gestionar sus depósitos s3.

Puede descargar el archivo de política JSON en este ZIP: DetectiveControlsConfig_ ServiceRolePolicy .zip.

## AWS política gestionada: AWSManaged ServicesDeploymentToolkitPolicy

AWS Managed Services (AMS) usa la política `AWSManagedServicesDeploymentToolkitPolicy` AWS administrada. Esta política AWS gestionada está asociada a la función `AWSServiceRoleForAWSManagedServicesDeploymentToolkit` vinculada al servicio (consulte). Kit de herramientas de despliegue: función vinculada a los servicios para AMS Accelerate La política permite al rol vinculado al servicio completar acciones en su lugar. No puede adjuntar esta política a sus entidades de IAM. Para obtener más información, consulte Uso de funciones vinculadas a servicios para AMS Accelerate.

Para ver las actualizaciones de la función vinculada al `AWSServiceRoleForManagedServicesDeploymentToolkitPolicy` servicio, consulte. Acelere las actualizaciones de las funciones vinculadas al servicio

Detalles de los permisos

Esta política tiene los siguientes permisos para permitir a AWS Managed Services Detective Controls implementar y configurar todos los recursos necesarios.

- `CloudFormation`— Permite que AMS Deployment Toolkit despliegue pilas de CFN con los recursos de S3 que necesita el CDK.
- `Amazon S3`— permite a AMS Deployment Toolkit gestionar sus depósitos de S3.
- `Elastic Container Registry`— permite a AMS Deployment Toolkit gestionar su repositorio de ECR, que se utiliza para implementar los activos que necesitan las aplicaciones CDK de AMS.

Puede descargar el archivo de políticas JSON en este ZIP: .zip. AWSManaged ServicesDeploymentToolkitPolicy

## AWS política gestionada: AWSManagedServices_EventsServiceRolePolicy

AWS Managed Services (AMS) usa la política administrada de `AWSManagedServices_EventsServiceRolePolicy` AWS. Esta política AWS gestionada está asociada a la función vinculada al `AWSServiceRoleForManagedServices_Events`servicio. La política permite al rol vinculado al servicio completar acciones en su lugar. No puede adjuntar

esta política a sus entidades de IAM. Para obtener más información, consulte Uso de funciones vinculadas a servicios para AMS Accelerate.

Para ver las actualizaciones de la función vinculada al `AWSServiceRoleForManagedServices_Events` servicio, consulte. Acelere las actualizaciones de las funciones vinculadas al servicio

Detalles de los permisos

Esta política tiene los siguientes permisos para permitir EventBridge a Amazon enviar información sobre cambios de estado de alarma desde su cuenta a AWS Managed Services.

- `events`— Permite a Accelerate crear una regla EventBridge gestionada por Amazon. Esta regla es la infraestructura que necesita Cuenta de AWS para enviar información sobre los cambios de estado de alarma desde su cuenta a AWS Managed Services.

Puede descargar el archivo de política JSON en este ZIP: EventsServiceRolePolicy.zip.

## AWS política gestionada: AWSManagedServices_ContactsServiceRolePolicy

AWS Managed Services (AMS) usa la política administrada de `AWSManagedServices_ContactsServiceRolePolicy` AWS. Esta política AWS gestionada está asociada a la función `AWSServiceRoleForManagedServices_Contacts` vinculada al servicio (consulte). Creación de una cámara réflex de contactos para AMS Accelerate La política permite a AMS Contacts SLR analizar las etiquetas de sus recursos y sus valores en los recursos de AWS. No puede adjuntar esta política a sus entidades de IAM. Para obtener más información, consulte Uso de funciones vinculadas a servicios para AMS Accelerate.

> **Important**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. AMS utiliza etiquetas para proporcionarle servicios de administración. Las etiquetas no se han diseñado para usarse con información privada o confidencial.

Para obtener información actualizada sobre la función `AWSServiceRoleForManagedServices_Contacts` vinculada al servicio, consulte. Acelere las actualizaciones de las funciones vinculadas al servicio

Detalles de los permisos

Esta política tiene los siguientes permisos para permitir que la SLR de Contactos lea las etiquetas de los recursos para recuperar la información de contacto del recurso que haya configurado con antelación.

- `IAM`— Permite que el servicio de contactos consulte las etiquetas de los roles y usuarios de IAM.
- `Amazon EC2`— Permite que el servicio de contactos consulte las etiquetas de EC2 los recursos de Amazon.
- `Amazon S3`— Permite a Contacts Service ver las etiquetas de los buckets de Amazon S3. Esta acción utiliza una condición para garantizar que AMS acceda a sus etiquetas de bucket mediante el encabezado de autorización HTTP, el protocolo de firma SigV4 y el uso de HTTPS con TLS 1.2 o superior. Para obtener más información, consulte Métodos de autenticación y Claves de política específicas de autenticación de Amazon S3 Signature versión 4.
- `Tag`— Permite que el servicio de contactos consulte las etiquetas de otros AWS recursos.

- «iam: ListRoleTags «, «iam: ListUserTags «, «tag: GetResources «, «tag: «, GetTagKeys «tag: «, GetTagValues «ec2: «, DescribeTags «s3:» GetBucketTagging

Puede descargar el archivo de política JSON en este ZIP: .zip. ContactsServicePolicy

## Acelere las actualizaciones de las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS gestionadas de Accelerate desde que este servicio comenzó a realizar el seguimiento de estos cambios.

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Política actualizada: kit de herramientas de implementación | • Se agregaron estos nuevos permisos para el recurso`arn:aws:ecr:*:*:repository/ams-cdktoolkit*` :<br>`ecr:BatchGetRepositoryScanningConfiguration`<br>`ecr:PutImageScanningConfiguration` | 4 de abril de 2024 |
| Política actualizada: kit de | • Se agregaron estos nuevos permisos para el recurso`arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*` : | 9 de mayo de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| herramientas de implementación | <pre>cloudformation:DeleteChangeSet<br><br>cloudformation:DescribeStackEvents<br>cloudformation:GetTemplate<br>cloudformation:TagResource<br>cloudformation:UntagResource</pre> • Se agregaron estos nuevos permisos para el recurso`arn:aws:ecr:*:*:repository/ams-cdktoolkit*` : <pre>ecr:CreateRepository<br><br>ecr:DeleteLifecyclePolicy<br>ecr:DeleteRepository<br>ecr:DeleteRepositoryPolicy<br>ecr:DescribeRepositories<br>ecr:GetLifecyclePolicy<br>ecr:ListTagsForResource<br>ecr:PutImageTagMutability<br>ecr:PutLifecyclePolicy<br>ecr:SetRepositoryPolicy<br>ecr:TagResource<br>ecr:UntagResource</pre> • Además, algunas acciones existentes con caracteres comodín se redujeron a acciones individuales: <pre>- s3:DeleteObject*<br><br>+ s3:DeleteObject<br>+ s3:DeleteObjectTagging<br>+ s3:DeleteObjectVersion<br>+ s3:DeleteObjectVersionTagging<br><br>- s3:GetObject*<br>+ s3:GetObject<br>+ s3:GetObjectAcl<br>+ s3:GetObjectAttributes<br>+ s3:GetObjectLegalHold</pre> | |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| | <pre>+ s3:GetObjectRetention<br>+ s3:GetObjectTagging<br>+ s3:GetObjectVersion<br>+ s3:GetObjectVersionAcl<br>+ s3:GetObjectVersionAttributes<br>+ s3:GetObjectVersionForReplication<br>+ s3:GetObjectVersionTagging<br>+ s3:GetObjectVersionTorrent<br><br>- cloudformation:UpdateTermination*<br>+ cloudformation:UpdateTerminationProt<br>ection</pre> | |
| Política actualizada — Detective Controls | • Las CloudFormation acciones se han reducido aún más tras la confirmación con el equipo de seguridad y acceso<br>• Las acciones de Lambda se han eliminado de la política porque no afectan al embarque onboarding/off | 10 de abril de 2023 |
| Política actualizada — Detective Controls | La `ListAttachedRolePolicies` acción se elimina de la política. La acción tenía el recurso como comodín (*). Como «enumerar» es una acción no mutante, se le da acceso a todos los recursos y no se permite el comodín. | 28 de marzo de 2023 |
| Política actualizada — Detective Controls | Se actualizó la política y se agregó la política de límites de permisos. | 21 de marzo de 2023 |
| Nueva política: servicio de contactos | Accelerate agregó una nueva política para ver la información de contacto de su cuenta en las etiquetas de sus recursos.<br><br>Accelerate agregó una nueva política para leer las etiquetas de sus recursos, de modo que pueda recuperar con antelación la información de contacto del recurso que haya configurado. | 16 de febrero de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Nueva política: Events Service | Accelerate agregó una nueva política para enviar información sobre los cambios de estado de alarma de su cuenta a AWS Managed Services.<br><br>Otorga funciones de IAM creadas como parte de Cómo funciona Alarm Manager los permisos para crear una regla EventBridge gestionada por Amazon obligatoria. | 7 de febrero de 2023 |
| Política actualizada: kit de herramientas de implementación | Se agregaron permisos de S3 para facilitar la desvinculación de los clientes de Accelerate. | 30 de enero de 2023 |
| Nueva política — Detective Controls | Permite que el rol vinculado al servicio complete acciones para que usted despliegue los controles de Accelerate Detective. El Detective controla la función vinculada al servicio para AMS Accelerate | 19 de diciembre de 2022 |
| Nueva política: Alarm Manager | Accelerate agregó una nueva política para permitir permisos para realizar tareas de administración de alarmas.<br><br>Otorga funciones de IAM creadas como parte de Cómo funciona Alarm Manager los permisos para realizar operaciones como la evaluación de AWS Config, la configuración de AWS Config read to fetch alarm manager o la creación de las alarmas de Amazon CloudWatch necesarias. | 30 de noviembre de 2022 |
| Acelera y comienza a rastrear los cambios | Accelerate comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas. | 30 de noviembre de 2022 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Nueva política: kit de herramientas de implementación | Accelerate agregó esta política para las tareas de implementación.<br><br>Otorga al rol vinculado al servicio AWSServiceRoleForAWSManagedServicesDeploymentToolkitpermisos para acceder a los buckets y pilas de Amazon S3 relacionados con la implementación y actualizarlos. CloudFormation | 9 de junio de 2022 |

# Protección de datos en Accelerate

AMS Accelerate aprovecha las herramientas y procesos nativos GuardDuty, Servicios de AWS como Amazon, Amazon Macie (opcional) y otras herramientas y procesos internos patentados, para supervisar de forma continua sus cuentas gestionadas. Cuando se activa una alarma, AMS Accelerate asume la responsabilidad de la clasificación inicial y de la respuesta a la alarma. Los procesos de respuesta de AMS se basan en los estándares del NIST. AMS Accelerate pone a prueba periódicamente los procesos de respuesta mediante la simulación de respuesta a incidentes de seguridad para alinear su flujo de trabajo con los programas de respuesta de seguridad existentes para los clientes.

Cuando AMS Accelerate detecta una infracción o una amenaza inminente de infracción de sus políticas de AWS seguridad, Accelerate recopila información, incluidos los recursos afectados y cualquier cambio relacionado con la configuración. AMS Accelerate ofrece follow-the-sun asistencia las 24 horas del día, los 7 días de la semana, con operadores especializados que revisan e investigan activamente los paneles de control, las colas de incidentes y las solicitudes de servicio en todas sus cuentas gestionadas. Accelerate investiga los hallazgos con expertos en seguridad internos para analizar la actividad y notificárselo a través de los contactos de intensificación de la seguridad que figuran en su cuenta.

En función de los resultados, Accelerate interactúa con usted de forma proactiva. Si descubre que la actividad no está autorizada o es sospechosa, AMS trabaja con usted para investigar y solucionar o contener el problema. Existen determinados tipos de hallazgos GuardDuty que requieren que confirme el impacto antes de que Accelerate tome alguna medida. Por ejemplo, el tipo de GuardDuty búsqueda UnauthorizedAccess:IAMUser/ConsoleLoginindica que uno de sus usuarios ha iniciado sesión desde una ubicación inusual; AMS se lo notifica y le pide que revise el hallazgo para confirmar si este comportamiento es legítimo.

# Monitoriza con Amazon Macie

> **Important**
>
> AMS Accelerate no admite el monitoreo con Amazon Macie en la región de Asia Pacífico (Malasia).

AMS Accelerate apoya Amazon Macie, y es una buena práctica utilizarlo para detectar una lista amplia y completa de datos confidenciales, como información de salud personal (PHI), información de identificación personal (PII) y datos financieros.

Puede configurar Macie para que se ejecute periódicamente en cualquier bucket de Amazon S3. Esto automatiza la evaluación de los objetos nuevos o modificados dentro de un bucket a lo largo del tiempo. A medida que se generan problemas de seguridad, AMS se lo notifica y trabaja con usted para subsanarlos según sea necesario.

Para obtener más información, consulte Análisis de los hallazgos de Amazon Macie.

# Supervise con GuardDuty

GuardDuty es un servicio de supervisión continua de la seguridad que utiliza fuentes de información sobre amenazas, como listas de direcciones IP y dominios maliciosos, y aprendizaje automático para identificar actividades inesperadas, potencialmente no autorizadas y maliciosas en su AWS entorno. Esto puede incluir problemas como la escalada de privilegios, el uso de credenciales expuestas o la comunicación con direcciones IP o dominios maliciosos. GuardDuty monitorea el comportamiento de Cuenta de AWS acceso para detectar signos de peligro, como despliegues de infraestructura no autorizados o instancias implementadas en una AWS región que nunca has utilizado. GuardDuty también detecta llamadas inusuales a la API, como un cambio en la política de contraseñas para reducir la seguridad de la contraseña. Para obtener más información, consulte la Guía del usuario de GuardDuty .

Para ver y analizar sus GuardDuty hallazgos, complete los siguientes pasos:

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. Elija Hallazgos y, a continuación, seleccione un hallazgo específico para ver los detalles. Los detalles de cada hallazgo varían según el tipo de hallazgo, los recursos involucrados y la naturaleza de la actividad.

Para obtener más información sobre los campos de búsqueda disponibles, consulte los detalles de GuardDuty búsqueda.

## Utilice las reglas de GuardDuty supresión para filtrar los resultados

Una regla de supresión es un conjunto de criterios que consta de un atributo de filtro emparejado con un valor. Puede usar las reglas de supresión para filtrar los hallazgos de bajo valor sobre los que no tiene intención de actuar, como los resultados de falsos positivos o las actividades conocidas. Filtrar los resultados ayuda a reconocer con más facilidad las amenazas a la seguridad que podrían tener el mayor impacto en su entorno.

Para filtrar los hallazgos, las reglas de supresión archivan automáticamente los nuevos hallazgos que coinciden con los criterios especificados. Los resultados archivados no se envían a AWS Security Hub, Amazon S3 ni CloudTrail Events. Por lo tanto, los filtros de supresión reducen los datos inutilizables si se consumen los GuardDuty hallazgos a través de Security Hub o de una aplicación SIEM de terceros de alertas y emisión de tickets.

AMS tiene un conjunto definido de criterios para identificar las reglas de supresión para sus cuentas gestionadas. Cuando una cuenta gestionada cumple con este criterio, AMS aplica los filtros y le crea una solicitud de servicio (SR) en la que se detalla el filtro de supresión implementado.

Puede comunicarse con AMS a través de un SR para modificar o revertir los filtros de supresión.

### Vea los resultados archivados

GuardDuty sigue generando hallazgos incluso cuando esos hallazgos coinciden con sus reglas de supresión. Los hallazgos suprimidos se marcan como archivados. GuardDuty almacena los hallazgos archivados durante 90 días. Para ver las conclusiones archivadas durante esos 90 días en la GuardDuty consola, seleccione Archivado en la tabla de conclusiones. O bien, consulta los hallazgos archivados a través de la GuardDuty ListFindingsAPI con un valor de FindingCriteria de service.archived igual a true.

### Casos de uso comunes de las reglas de supresión

Los siguientes tipos de resultados tienen casos de uso comunes para la aplicación de reglas de supresión.

- Recon:EC2/Portscan: utilice una regla de supresión para archivar automáticamente los hallazgos cuando utilice un escáner de vulnerabilidades autorizado.

- UnauthorizedAccessRecon:EC2/PortscanSSHBrute: utilice una regla de supresión para archivar automáticamente los hallazgos cuando utilice un escáner de vulnerabilidades autorizado. — SEP----:EC2/ Force: utilice una regla de supresión para archivar automáticamente los hallazgos cuando estén dirigidos a instancias de bastión.
- Recon:EC2/ PortProbeUnprotectedPort: Utilice una regla de supresión para archivar automáticamente las conclusiones cuando se dirijan a instancias expuestas intencionadamente.

## Supervise con el firewall DNS Amazon Route 53 Resolver

Amazon Route 53 Resolver responde de forma recursiva a las consultas de DNS de AWS los recursos de registros públicos, los nombres de DNS específicos de Amazon VPC y las zonas alojadas privadas de Amazon Route 53, y está disponible de forma predeterminada en todos. VPCs Con DNS Firewall de Route 53 Resolver, puede filtrar y regular el tráfico DNS de salida para su virtual private cloud (VPC). Para ello, cree colecciones reutilizables de reglas de filtrado en grupos de reglas de DNS Firewall, asocie los grupos de reglas a su VPC y, a continuación, monitoree la actividad en los registros y métricas de DNS Firewall. En función de la actividad, puede ajustar el comportamiento de DNS Firewall según corresponda. Para obtener más información, consulte Uso del firewall de DNS para filtrar el tráfico DNS saliente.

Para ver y administrar la configuración del firewall DNS de Route 53 Resolver, utilice el siguiente procedimiento:

1. Inicie sesión en la consola de Amazon VPC Consola de administración de AWS y ábrala en. https://console.aws.amazon.com/vpc/
2. En Firewall de DNS, selecciona Grupos de reglas.
3. Revisa, edita o elimina la configuración existente o crea un grupo de reglas nuevo. Para obtener más información, consulte Cómo funciona el firewall DNS de Route 53 Resolver.

### Supervisión y seguridad del firewall DNS de Amazon Route 53 Resolver

El firewall DNS de Amazon Route 53 utiliza los conceptos de asociaciones de reglas, acción de reglas y prioridad de evaluación de reglas. Una lista de dominios es un conjunto reutilizable de especificaciones de dominio que se utiliza en una regla de DNS Firewall, dentro de un grupo de reglas. Al asociar un grupo de reglas a una VPC, DNS Firewall compara las consultas de DNS con las listas de dominios que se utilizan en las reglas. Si el Firewall de DNS encuentra una coincidencia, gestiona la consulta de DNS de acuerdo con la acción de la regla coincidente. Para obtener más

información sobre los grupos de reglas y las reglas, consulte Reglas y grupos de reglas del Firewall DNS.

Las listas de dominios se dividen en dos categorías principales:

- Listas de dominios gestionadas, que se AWS crean y mantienen para usted.
- Sus propias listas de dominios, que usted crea y mantiene.

Los grupos de reglas se evalúan en función de su índice de prioridad de asociación.

De forma predeterminada, AMS implementa una configuración de referencia que consta de la siguiente regla y grupo de reglas:

- Un grupo de reglas denominado`DefaultSecurityMonitoringRule`. El grupo de reglas tiene la prioridad de asociación más alta disponible en el momento de la creación para cada VPC existente en cada una de las VPC habilitadas. Región de AWS
- Una regla nombrada `DefaultSecurityMonitoringRule` con la prioridad 1 dentro del grupo de `DefaultSecurityMonitoringRule` reglas, mediante la lista de dominios `AWSManagedDomainsAggregateThreatList` gestionados con la acción ALERT.

Si tiene una configuración existente, la configuración básica se implementa con una prioridad inferior a la configuración existente. La configuración actual es la predeterminada. Utiliza la configuración básica de AMS como una configuración general si la configuración existente no proporciona instrucciones de mayor prioridad sobre cómo gestionar la resolución de consultas. Para modificar o eliminar la configuración básica, realice una de las siguientes acciones:

- Póngase en contacto con su administrador de prestación de servicios en la nube (CSDM) o con su arquitecto de nube (CA).
- Cree una solicitud de servicio.

## Cifrado de datos en AMS Accelerate

AMS Accelerate utiliza varios Servicios de AWS para el cifrado de datos.

Amazon Simple Storage Service ofrece varias opciones de cifrado de objetos que protegen los datos en tránsito y en reposo. El cifrado del lado del servidor cifra el objeto antes de guardarlo en discos de sus centros de datos y, a continuación, lo descifra al descargar los objetos. Siempre que autentique

su solicitud y tenga permiso de acceso, no existe diferencia alguna en la forma de obtener acceso a objetos cifrados o sin cifrar. Para obtener más información, consulte Protección de los datos en Amazon S3.

# AWS Identity and Access Management en AMS Accelerate

AWS Identity and Access Management es un servicio web que le ayuda a controlar de forma segura el acceso a AWS los recursos. Utilice IAM para controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos. Durante la incorporación de AMS Accelerate, usted es responsable de crear funciones de administrador de IAM multicuenta en cada una de sus cuentas gestionadas.

En AMS Accelerate, eres responsable de gestionar el acceso a tus recursos Cuentas de AWS y a los recursos subyacentes, como las soluciones de gestión de acceso, las políticas de acceso y los procesos relacionados. Esto significa que debe gestionar el ciclo de vida de los usuarios, los permisos en los servicios de directorio y el sistema de autenticación federada para acceder a la AWS consola o AWS APIs. Para ayudarlo a administrar su solución de acceso, AMS Accelerate implementa AWS Config reglas que detectan los errores de configuración más comunes de IAM y envía notificaciones de corrección. Para obtener más información, consulte Reglas administradas de AWS Config.

## Autenticación con identidades en AMS Accelerate

AMS usa funciones de IAM, que son un tipo de identidad de IAM. Una función de IAM es similar a la de un usuario, ya que es una identidad con políticas de permisos que determinan lo que la identidad puede y no puede hacer en ella. AWS Sin embargo, un rol no tiene credenciales asociadas y, en lugar de estar asociado exclusivamente a una persona, cualquier persona que lo necesite puede asumirlo. Un usuario de IAM puede asumir una función para disponer temporalmente de diferentes permisos para una tarea específica.

Los roles de acceso se controlan mediante la pertenencia a un grupo interno, que la Gerencia de Operaciones administra y revisa periódicamente. AMS utiliza las siguientes funciones de IAM.

> **Note**
>
> Las funciones de acceso de AMS permiten a los operadores de AMS acceder a sus recursos para proporcionar las capacidades de AMS (consulteDescripción del servicio). La modificación de estas funciones puede inhibir nuestra capacidad de proporcionar estas

capacidades. Si necesita modificar las funciones de acceso a AMS, consulte a su arquitecto de nube.

| Nombre del rol | Descripción |
| --- | --- |
| Utilizado por (entidad): solo AMS Access Service | |
| ams-access-management | Usted lo implementó manualmente durante la incorporación. AMS Access solo lo asume para implementar o actualizar las funciones de acceso. Permanece en tu cuenta después de la incorporación para futuras actualizaciones de las funciones de acceso. |
| Utilizado por (entidad): AMS Operations | |
| ams-access-admin-operations | Esta función tiene permisos administrativos para operar en las cuentas, pero no tiene permisos para leer, escribir o eliminar el contenido de los clientes en los AWS servicios que se utilizan habitualmente como almacenes de datos, como Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift y Amazon. ElastiCache Solo unas pocas personas selectas de AMS pueden asumir esta función. |
| ams-access-operations | Esta función de operaciones de AMS tiene permisos para realizar tareas administrativas en sus cuentas. Este rol no tiene permisos de lectura, escritura o eliminación del contenido de los clientes en los AWS servicios que se utilizan habitualmente como almacenes de datos, como Amazon Simple Storage Service, Amazon Relational Database Service, Amazon |

| Nombre del rol | Descripción |
| --- | --- |
| | DynamoDB, Amazon Redshift y Amazon. ElastiCache Los permisos para realizar operaciones de AWS Identity and Access Management escritura también están excluidos de esta función. |
| ams-access-read-only | Esta función de solo lectura de AMS se limita a los permisos de solo lectura de su cuenta de AMS. Esta función no concede permisos de lectura del contenido de los clientes en los AWS servicios que se utilizan habitualmente como almacenes de datos, como Amazon S3, Amazon RDS, DynamoDB o Amazon Redshift ElastiCache. |
| Utilizado por (entidad): AMS Operations y AMS Services | |
| ams_ssm_automation_role | Se supone que ejecuta los documentos de SSM Automation en AWS Systems Manager su cuenta. |
| ams_ssm_automation_role | |
| Usado por (entidad): AMS Security | |
| ams-access-security-analyst | Este rol de seguridad de AMS tiene permisos en su cuenta de AMS para supervisar específicamente las alertas de seguridad y gestionar los incidentes de seguridad. Solo unas pocas personas selectas de AMS Security pueden asumir esta función. Permisos de lectura del contenido de los clientes en los AWS servicios que se utilizan habitualmente como almacenes de datos, como Amazon S3, Amazon RDS, Amazon DynamoDB o Amazon ElastiCache Redshift, y que esta función no concede. |

| Nombre del rol | Descripción |
| --- | --- |
| ams-access-security-analyst-de solo lectura | Esta función de seguridad de AMS se limita a los permisos de solo lectura en su cuenta de AMS para realizar una supervisión específic a de las alertas de seguridad y gestionar los incidentes de seguridad. Permisos de lectura del contenido de los clientes en los AWS servicios que se utilizan habitualmente como almacenes de datos, como Amazon S3, Amazon RDS, Amazon DynamoDB o Amazon ElastiCache Redshift, y que esta función no concede. |
| Utilizado por (entidad): AWS Services | |
| ams-access-admin | Esta función de administrador de AMS tiene todos los permisos necesarios para operar en las cuentas sin restricciones. Solo los servicios internos de AMS (con una política de sesión limitada) pueden asumir la función de administr ador. |
| ams-opscenter-eventbridge-role | Amazon asume que EventBridge la creación forma parte del AWS Systems Manager OpsItems flujo de trabajo de Reglas de AWS Config remediación específico de AMS. |

| Nombre del rol | Descripción |
| --- | --- |
| AMSOSConfigurationCustomerInstanceRole | Esta función de IAM se aplica a sus EC2 instancias de Amazon cuando el servicio de configuración del sistema operativo AMS descubre que faltan las políticas de IAM requeridas. Permite que tus EC2 instancias de Amazon interactúen con AWS Systems Manager Amazon CloudWatch y EventBrid ge los servicios de Amazon. También incluye la política de administración personalizada de AMS para permitir el acceso RDP a sus instancias de Windows. |
| mc-patch-glue-service-rol | El flujo de trabajo de AWS Glue ETL lo asume para realizar la transformación de los datos y prepararlos para el generador de informes AMS Patch. |
| Utilizado por (entidad): AMS Service | |
| ams-alarm-manager- AWSManaged ServicesA larmManagerDe - <8-digit hash> | Asume la infraestructura del administrador de alarmas de AMS incluida en su cuenta de AMS para realizar Reglas de AWS Config la evaluación de una nueva AWS AppConfig implementación. |
| ams-alarm-manager- AWSManaged ServicesA larmManagerRe - <8-digit hash> | Lo asume la infraestructura de remediación del administrador de alarmas de AMS incluida en su cuenta de AMS para permitir la creación o eliminación de alarmas para su corrección. |
| ams-alarm-manager- SS- AWSManaged ServicesAlarmManager <8-digit hash> | Se asume AWS Systems Manager al invocar el servicio de reparación del administrador de alarmas de AMS en su cuenta de AMS. |

| Nombre del rol | Descripción |
| --- | --- |
| ams-alarm-manager- - AWSManaged ServicesAlarmManagerTr <8-digit hash> | Asume la infraestructura de gestión de alarmas de AMS incluida en su AWS cuenta para realizar una Reglas de AWS Config evaluación periódica de AMS. |
| ams-alarm-manager- AWSManaged ServicesA larmManagerVa - <8-digit hash> | Lo asume la infraestructura de gestión de alarmas de AMS incluida en su cuenta de AMS para garantizar que existan las alarmas necesarias en la AWS cuenta. |
| ams-backup-iam-role | Esta función se utiliza para ejecutarse AWS Backup en sus cuentas. |
| ams-monitoring- - AWSManaged ServicesL ogGroupLimitLamb <8-digit hash> | Lo asume la infraestructura de registro y monitoreo de AMS en su cuenta de AMS para evaluar el límite de grupos de Amazon CloudWatch Logs y compararlo con las cuotas de servicio. |
| ams-monitoring- AWSManaged Services RDSMonitoring RDSE- <8-digit hash> | Lo asume la infraestructura de registro y monitoreo de AMS en su cuenta de AMS para reenviar los eventos de Amazon RDS a Amazon CloudWatch Events. |
| ams-monitoring- - AWSManaged ServicesR edshiftMonitorin <8-digit hash> | Lo asume la infraestructura de registro y monitoreo de AMS en su cuenta de AMS para reenviar los eventos de Amazon Redshift (CreateCluster y DeleteCuster) a Amazon CloudWatch Events. |
| ams-monitoring-infrastruc- - AWSManaged ServicesMonito <8-digit hash> | La infraestructura de registro y monitoreo de AMS de su cuenta de AMS asume que publica mensajes en Amazon Simple Notification Service para validar que la cuenta informa de todos los datos necesarios. |

| Nombre del rol | Descripción |
| --- | --- |
| ams-opscenter-role | Lo utiliza el sistema de gestión de notificac iones de AMS de su cuenta de AMS para gestionar las alertas AWS Systems Manager OpsItems relacionadas con su cuenta. |
| ams-opsitem-autoexecution-role | El sistema de gestión de notificaciones de AMS lo utiliza para gestionar las correcciones automatizadas mediante documentos SSM para supervisar las alertas relacionadas con los recursos de su cuenta. |
| ams-patch-infrastructure-amspatchconfigrulero leC1- <8-digit hash> | Asumido AWS Config para evaluar los recursos de parches de AMS y detectar desviaciones en sus CloudFormation pilas. |
| ams-patch-infrastructure-amspatchcwruleopsite mams- <8-digit hash> | Asumido por Amazon EventBridge AWS Systems Manager OpsItems para crear errores de parcheo. |
| ams-patch-infrastructure-amspatchser vicebusamspat- <8-digit hash> | Amazon asume que envía un evento EventBrid ge al bus de eventos de AMS Patch Orchestra tor para recibir notificaciones de cambio de estado de AWS Systems Manager Maintenan ce Windows. |
| ams-patch-reporting-infra-amspatchreportingco nfig- <8-digit hash> | Asumido AWS Config para evaluar los recursos de informes de AMS Patch y detectar desviacio nes en sus pilas. CloudFormation |
| ams-resource-tagger- - AWSManaged ServicesResourceTagg <8-digit hash> | Asume la infraestructura de AMS Resource Tagger de su cuenta de AMS para realizar una Reglas de AWS Config evaluación en caso de una nueva AWS AppConfig implementación. |

| Nombre del rol | Descripción |
| --- | --- |
| ams-resource-tagger- - AWSManaged ServicesResourceTagg <8-digit hash> | Lo asume la infraestructura de AMS Resource Tagger de su cuenta de AMS para validar que existen las AWS etiquetas necesarias para los recursos gestionados. |
| ams-resource-tagger- - AWSManaged ServicesResourceTagg <8-digit hash> | Se supone que AWS Systems Manager para invocar el flujo de trabajo de corrección de AMS Resource Tagger en su cuenta de AMS. |
| ams-resource-tagger- - AWSManaged ServicesResourceTagg <8-digit hash> | Asume la infraestructura de remediación de AMS Resource Tagger de su cuenta de AMS para crear o eliminar AWS etiquetas para los recursos gestionados. |
| ams-resource-tagger- - AWSManaged ServicesResourceTagg <8-digit hash> | Lo asume la infraestructura de AMS Resource Tagger de su AWS cuenta para realizar una evaluación periódica de las reglas de AMS Config. |
| ams_os_configuration_event_rule_role- <AWS Region> | Amazon lo asume EventBridge para reenviar los eventos de su cuenta al servicio de configuración del sistema operativo AMS EventBus en la región correcta. |
| mc-patch-reporting-service | Asumido por el agregador de datos de parches y generador de informes AMS. |

**Note**

Esta es la plantilla para el ams-access-management rol. Es la pila que los arquitectos de nube (CAs) implementan manualmente en tu cuenta en el momento de la incorporación: management-role.yaml.
Esta es la plantilla para los distintos roles y niveles de acceso:,,,: accelerate-roles.yaml. ams-access-read-only ams-access-operations ams-access-admin-operations ams-access-admin

Para obtener más información sobre los identificadores AWS Cloud Development Kit (AWS CDK) (AWS CDK), incluidos los hashes, consulta Unique. IDs

Los servicios de funciones de AMS Accelerate asumen la ams-access-adminfunción de acceso programático a la cuenta, pero con una política de sesión definida para el servicio de funciones correspondiente (por ejemplo, parches, copias de seguridad, monitoreo, etc.).

AMS Accelerate sigue las mejores prácticas del sector para cumplir y mantener los requisitos de conformidad. El acceso de AMS Accelerate a su cuenta está registrado CloudTrail y también está disponible para su revisión mediante el seguimiento de cambios. Para obtener información sobre las consultas que puede utilizar para obtener esta información, consulteSeguimiento de los cambios en sus cuentas de AMS Accelerate.

## Administración de acceso mediante políticas

Varios equipos de soporte de AMS Accelerate, como ingenieros de operaciones, arquitectos de nube y gerentes de prestación de servicios en la nube (CSDMs), a veces necesitan acceder a sus cuentas para responder a las solicitudes de servicio e incidentes. Su acceso se rige por un servicio de acceso interno a AMS que impone controles, como la justificación empresarial, las solicitudes de servicio, las operaciones y los casos de soporte. El acceso predeterminado es de solo lectura y todos los accesos se rastrean y registran; consulte también. Seguimiento de los cambios en sus cuentas de AMS Accelerate

### Validación de los recursos de IAM

El sistema de acceso AMS Accelerate asume funciones en sus cuentas de forma periódica (al menos cada 24 horas) y valida que todos nuestros recursos de IAM sean los esperados.

Para proteger sus cuentas, AMS Accelerate cuenta con un sistema «canario» que monitorea y alerta sobre la presencia y el estado de las funciones de IAM, así como sobre las políticas asociadas a ellas, mencionadas anteriormente. Periódicamente, el canario asume esa ams-access-read-onlyfunción CloudFormation e inicia llamadas a la API de IAM contra tus cuentas. El canario evalúa el estado de las funciones de acceso de AMS Accelerate para asegurarse de que estén siempre intactas y. up-to-date Esta actividad crea CloudTrail registros en la cuenta.

El nombre de sesión AWS Security Token Service (AWS STS) del canario es AMS-Access-Roles-Auditor- {uuid4 ()} como se ve en y se producen las siguientes llamadas a la API: CloudTrail

- Llamadas a la API Cloud Formation: `describe_stacks()`

- Llamadas a la API de IAM:
  - `get_role()`
  - `list_attached_role_policies()`
  - `list_role_policies()`
  - `get_policy()`
  - `get_policy_version()`
  - `get_role_policy()`

# Respuesta a incidentes de seguridad en AMS

La seguridad es la principal prioridad de AWS Managed Services (AMS). AMS despliega recursos y controles en sus cuentas para administrarlas. AWS tiene un modelo de responsabilidad compartida: AWS gestiona la seguridad de la nube y usted es responsable de la seguridad en la nube. AMS protege sus datos y activos y ayuda a mantener su AWS infraestructura segura mediante el uso de controles de seguridad y una supervisión activa para detectar problemas de seguridad. Estas capacidades le ayudan a establecer una base de seguridad para las aplicaciones que se ejecutan en la AWS nube. AMS colabora con usted a través de la respuesta a incidentes de seguridad para evaluar el efecto y, luego, llevar a cabo la contención y las remediaciones en función de las recomendaciones de mejores prácticas.

Cuando se produce una desviación de la línea base, por ejemplo, debido a un error de configuración o a un cambio en factores externos, es necesario responder e investigar. Para hacerlo correctamente, debe comprender los conceptos básicos de la respuesta a incidentes de seguridad en su entorno AMS. También debe comprender los requisitos para preparar, formar y capacitar a los equipos de nube antes de que se produzcan problemas de seguridad. Es importante conocer los controles y las capacidades que puede utilizar, preparar planes de respuesta para los problemas de seguridad más comunes, como una cuenta de usuario comprometida o el uso indebido de cuentas privilegiadas, e identificar métodos de corrección que utilicen la automatización para mejorar la velocidad y la coherencia de la respuesta. Además, debe comprender sus requisitos normativos y de cumplimiento en lo que respecta a la creación de un programa de respuesta a incidentes de seguridad que cumpla con esos requisitos.

La respuesta a los incidentes de seguridad puede ser compleja, pero si se implementa un enfoque iterativo, se puede simplificar el proceso y permitir que el equipo de respuesta a incidentes mantenga satisfechos a las partes interesadas de los activos al proporcionar una detección y respuesta tempranas y continuas. En esta guía, le proporcionamos la metodología que utiliza AMS para la

respuesta a incidentes, la matriz de responsabilidad de AMS (RACI), cómo puede prepararse para un incidente de seguridad, cómo interactuar con AMS durante los incidentes de seguridad y algunos de los manuales de respuesta a incidentes que utiliza AMS.

## Cómo funciona la respuesta a incidentes de seguridad de AMS

AWS Managed Services se ajusta a la Guía de gestión de incidentes de seguridad informática NIST 800-61 para la respuesta a incidentes de seguridad. Al cumplir con este estándar del sector, ofrecemos un enfoque coherente para la gestión de eventos de seguridad y seguimos las mejores prácticas para proteger y responder a los incidentes de seguridad en la nube.

Ciclo vital de respuesta a incidentes

Cuando la detección identifica y genera una alerta de seguridad, o si solicita asistencia de seguridad, el equipo de operaciones de AWS Managed Services se asegura de que se lleva a cabo una investigación a tiempo, ejecuta automatizaciones para realizar la recopilación, clasificación y análisis de datos, le informa del análisis, lleva a cabo la investigación y cualquier actividad de contención y, a continuación, publica el análisis de los eventos.

Las actividades de recopilación, clasificación, análisis y contención de datos que se llevan a cabo durante la respuesta al incidente varían en función del tipo de incidente de seguridad que se investigue. Al final de este documento, encontrará ejemplos de flujos de trabajo de respuesta a incidentes de seguridad para escenarios seleccionados.

Durante los incidentes, AMS determina el curso de acción correcto de forma dinámica, lo que puede provocar que los pasos documentados se reordenen o se omitan según corresponda para garantizar que se obtenga el resultado correcto.

## Preparación

A medida que el panorama de amenazas evoluciona, AMS sigue ampliando sus capacidades de detección y respuesta. A medida que se añaden nuevas detecciones, AMS incorpora las alertas de estas nuevas detecciones a la plataforma de detección y respuesta. Los equipos de seguridad de AMS están capacitados para investigar y colaborar con usted durante todo el ciclo de vida de la respuesta a los incidentes de seguridad.

Debido a este enfoque de asociación, es importante que sus equipos de seguridad y aplicaciones estén preparados para colaborar con AMS para gestionar los eventos de seguridad a medida que se

produzcan. Esta documentación explica qué esperar durante un incidente de seguridad y le ayuda a prepararse para una respuesta rápida en caso de que se produzca un incidente de seguridad.

Esta documentación utiliza la definición 800-61 del NIST de un evento como cualquier suceso observable en un sistema o una red y un incidente como una infracción o amenaza inminente de violación de las políticas, las políticas de uso aceptable o las prácticas de seguridad estándar.

### Lista de verificación de preparación

Realice la siguiente lista de verificación con su administrador de entrega de soluciones en la nube (CSDM) de AMS y su arquitecto de nube (CA) de AMS:

- Comprenda qué cargas de trabajo se ejecutan en qué cuentas.
- Comprenda qué equipos internos son responsables de las distintas cargas de trabajo y etiquételos adecuadamente en las cargas de trabajo.
- Conserve internamente los datos de contacto de otros equipos que puedan ser necesarios durante la investigación de un incidente de seguridad y para tomar decisiones de contención.
- Confirma que los contactos de seguridad estén actualizados y se hayan agregado a todas las AWS cuentas gestionadas. Los contactos se administran por cuenta.
- Sepa cómo denunciar un incidente de seguridad a AMS y familiarícese con la gravedad y los tiempos de respuesta esperados.
- Asegúrese de que, cuando reciba las notificaciones de seguridad, se envíen a las personas y los sistemas adecuados, como los buscapersonas o el centro de operaciones de seguridad.
- Sepa qué fuentes de registro tiene a su disposición, dónde se almacenan en sus cuentas y quién tiene acceso a ellas.
- Aprenda a utilizar CloudWatch Insights para consultar los registros durante las investigaciones.
- Comprenda las opciones de contención disponibles por recurso (IAM, S3EC2, etc.) y las consecuencias en la disponibilidad de la carga de trabajo cuando se encuentra en situación de contención.

## Detect

Durante la administración de sus AWS cuentas, AMS supervisa las anomalías en el comportamiento de los usuarios, las actividades de las cuentas y los posibles eventos de seguridad mediante los datos recopilados de las fuentes y los controles de detección, incluidos, entre otros, Amazon,

GuardDuty VPC Flow Logs, CloudWatch Amazon Macie y los feeds internos de Threat Intelligence de AWS Config Amazon.

AMS utiliza AWS servicios nativos y otras tecnologías de detección para responder a los eventos de seguridad creados por:

- Config: tipos de búsqueda de conformidad
- GuardDuty Búsqueda de tipos
- Tipos de búsqueda de Macie
- Eventos del firewall DNS de Amazon Route 53 Resolver
- Eventos de seguridad de AMS (alarmas de vigilancia en la nube)

Se añaden nuevos hallazgos a medida que evolucionan los servicios, los productos y los ecosistemas de amenazas.

### Informe sobre los eventos de seguridad a AMS

Presente un incidente a través del portal o Soporte centro de soporte de AMS para notificar a AMS de un incidente de seguridad o solicitar una investigación.

## Análisis

Tras identificar e informar de un suceso de seguridad, el siguiente paso consiste en analizar si se trata de un falso positivo o de un incidente real. AMS utiliza técnicas automatizadas y de investigación manual para gestionar los eventos de seguridad. El análisis incluye la investigación de los registros de diferentes fuentes de detección, como los registros de tráfico de red, los registros del host, CloudTrail los eventos, los registros de AWS servicio, etc. El análisis también busca patrones que muestren un comportamiento anómalo por correlación.

Su colaboración es necesaria para comprender el contexto específico del entorno de la cuenta y establecer lo que es normal para su cuenta y sus cargas de trabajo. Esto ayuda a AMS a identificar una anomalía más rápido y a acelerar la respuesta a los incidentes.

### Gestione las comunicaciones de AMS sobre eventos de seguridad

AMS lo mantiene informado durante la investigación al contactar con sus contactos de seguridad mediante una denuncia de incidente. El administrador de prestación de servicios en la nube de AMS

(CSDM) y el arquitecto de la nube (CA) de AMS son los puntos de contacto a los que acudir para cualquier tipo de comunicación durante una investigación de seguridad activa.

La comunicación incluye la notificación automática cuando se genera una alerta de seguridad, la comunicación después del análisis del evento, el establecimiento de puentes de llamadas y la entrega continua de artefactos como archivos de registro, una instantánea de los recursos infectados y la obtención de los resultados de las investigaciones durante el evento de seguridad.

Los campos estándar incluidos en las notificaciones de alerta de seguridad de AMS se enumeran a continuación. Estos campos le proporcionan información para que pueda remitir los eventos a los equipos correspondientes de su organización para que los corrijan.

- Tipo de búsqueda
- Identificador de búsqueda (cuando proceda)
- Detectar la gravedad
- Descripción del hallazgo
- Buscando la fecha y hora de creación
- AWS ID de cuenta
- Región (si procede)
- AWS Recursos (IAMuser/role/policy, S3 EC2, EKS)

Se proporcionan campos adicionales según el tipo de hallazgo; por ejemplo, los hallazgos de EKS incluyen detalles del pod, el contenedor y el clúster.

## Contención

El enfoque de AMS en materia de contención consiste en asociarse con usted. Usted comprende el impacto en su empresa y en la carga de trabajo que pueden derivarse de las actividades de contención, como el aislamiento de la red, el desaprovisionamiento de usuarios o roles de IAM, la reconstrucción de instancias, etc.

Una parte esencial de la contención es la toma de decisiones. Por ejemplo, apague un sistema, aísle un recurso de la red o desactive el acceso o finalice las sesiones. Estas decisiones son más fáciles de tomar si existen estrategias y procedimientos predeterminados para contener el incidente. AMS proporciona la estrategia de contención y, a continuación, implementa la solución después de haber considerado el riesgo que implica la implementación de las acciones de contención.

Existen diferentes opciones de contención en función de los recursos que se analicen. AMS espera que se desplieguen varios tipos de contención simultáneamente durante la investigación de un incidente. Algunos de estos ejemplos incluyen:

- Aplique reglas de protección para bloquear el tráfico no autorizado (grupo de seguridad, NACL, reglas WAF, reglas SCP, denegar la inclusión en la lista, establecer una acción de firma en cuarentena o bloqueo)
- Aislamiento de recursos
- Aislamiento de red
- Inhabilitar los usuarios, las funciones y las políticas de IAM
- Modificar o reducir el privilegio de usuario y rol de IAM
- Terminación, suspensión o eliminación de recursos informáticos
- Restringir el acceso público desde el recurso afectado
- Claves de acceso, claves de API y contraseñas rotativas
- Eliminar las credenciales divulgadas y la información confidencial

AMS lo alienta a considerar el tipo de estrategias de contención para cada tipo de incidente grave que esté dentro de sus posibilidades de riesgo, con criterios claramente documentados que ayuden a la toma de decisiones en caso de que se produzca un incidente. Los criterios para determinar la estrategia adecuada incluyen:

- Posibles daños a los recursos
- Preservación de las pruebas
- Falta de disponibilidad del servicio (por ejemplo, conectividad de red, servicios prestados a terceros)
- Tiempo y recursos necesarios para implementar la estrategia
- Efectividad de la estrategia (por ejemplo, contención parcial, contención total)
- Permanencia de la solución (por ejemplo, decisiones entre puertas unidireccionales y puertas bidireccionales)
- Duración de la solución (por ejemplo, una solución alternativa de emergencia que se eliminará en cuatro horas, una solución temporal que se eliminará en dos semanas o una solución permanente).
- Aplique controles de seguridad que pueda activar para reducir el riesgo y disponer de tiempo para definir e implementar una contención más eficaz.

La velocidad de la contención es fundamental, por lo que AMS recomienda adoptar un enfoque gradual para lograr una contención eficiente y eficaz mediante la elaboración de estrategias a corto y largo plazo.

Utilice esta guía para considerar su estrategia de contención, que incluye diferentes técnicas según el tipo de recurso.

- Estrategia de contención
  - ¿Puede AMS identificar el alcance del incidente de seguridad?
    - En caso afirmativo, identifique todos los recursos (usuarios, sistemas, recursos).
    - En caso contrario, investigue en paralelo mientras ejecuta el siguiente paso en los recursos identificados.
  - ¿Se puede aislar el recurso?
    - En caso afirmativo, proceda a aislar los recursos afectados.
    - En caso contrario, colabore con los propietarios y administradores del sistema para determinar las medidas adicionales necesarias para contener el problema.
  - ¿Están todos los recursos afectados aislados de los no afectados?
    - En caso afirmativo, continúe con el siguiente paso.
    - Si no, continúe aislando los recursos afectados hasta que se logre contenerlos a corto plazo para evitar que el incidente se agrave aún más.
- Backup del sistema
  - ¿Se crearon copias de seguridad de los sistemas afectados para su posterior análisis?
  - ¿Están las copias forenses cifradas y almacenadas en una ubicación segura?
    - En caso afirmativo, continúe con el siguiente paso.
    - En caso contrario, cifre las imágenes forenses y almacénelas en una ubicación segura para evitar el uso accidental, los daños y las manipulaciones.

## Erradicación

Una vez contenido un incidente, puede ser necesario erradicarlo para eliminar por completo las fuentes de amenaza y proteger el sistema antes de pasar a la siguiente fase de recuperación. Las medidas de erradicación podrían incluir eliminar el malware y eliminar las cuentas de usuario comprometidas, así como identificar y mitigar todas las vulnerabilidades que se explotaron. Durante

la erradicación, es importante identificar todas las cuentas, los recursos y las instancias afectadas del entorno para poder solucionarlas.

Se recomienda que la erradicación y la recuperación se realicen de forma gradual, de modo que se prioricen las medidas de remediación. En el caso de los incidentes a gran escala, la recuperación puede llevar meses. La intención de las primeras fases debe ser aumentar la seguridad general con cambios de gran valor relativamente rápidos (días o semanas) para evitar futuros incidentes. Las fases posteriores deben centrarse en los cambios a largo plazo (por ejemplo, cambios en la infraestructura) y en el trabajo continuo para mantener la empresa lo más segura posible.

En el caso de algunos incidentes, la erradicación no es necesaria o se lleva a cabo durante la recuperación.

Considere lo siguiente:

- ¿Se puede cambiar la imagen del sistema y luego reforzarlo con parches u otras contramedidas para prevenir o reducir el riesgo de ataques?
- ¿Se ha eliminado todo el malware y otros artefactos que han dejado los atacantes y se han reforzado los sistemas afectados para evitar nuevos ataques?

## Recuperar

AMS colabora con usted para restablecer el funcionamiento normal de los sistemas, confirmar que funcionan con normalidad y (según proceda) corregir las vulnerabilidades para evitar incidentes similares.

Considere lo siguiente:

- ¿Están los sistemas afectados parcheados y reforzados contra el ataque reciente y los posibles ataques futuros?
- ¿Qué día y hora es posible restablecer la producción de los sistemas afectados?
- ¿Qué herramientas utilizará para probar, supervisar y comprobar que los sistemas que restaure para ponerlos en producción no son vulnerables a las técnicas de ataque iniciales?

## Informe posterior al incidente

Tras el suceso, AMS lleva a cabo un proceso de revisión de la investigación de todos los incidentes de seguridad. Además, AMS inicia un proceso de corrección de errores (COE) para abordar

los incidentes de seguridad causados por un error del sistema o de un procedimiento que, de forma plausible, tiene margen de mejora. AMS colabora con usted para mejorar continuamente la experiencia de investigación de seguridad. El proceso COE ayuda a AMS a identificar los factores que contribuyen a que los eventos afecten a los clientes y relaciona esas causas con las siguientes acciones, elementos que pueden evitar que se repitan eventos similares o ayuda a mitigar la duración o el nivel de impacto.

El proceso de revisión de la investigación de los incidentes de seguridad aborda los siguientes elementos para identificar las oportunidades de mejora:

- ¿Cuánto tiempo transcurrió desde el inicio del incidente hasta su descubrimiento, la evaluación inicial del impacto y cada etapa del proceso de gestión del incidente (por ejemplo, contención o recuperación)?
- ¿Cuánto tiempo tardó el equipo de respuesta a incidentes en responder al informe inicial del incidente?
- ¿Cuánto tiempo se tardó en realizar un análisis de impacto inicial?
- ¿Se pudo prevenir esto y cómo? ¿Existe alguna herramienta o proceso que pudiera haberlo evitado?
- ¿Podríamos haberlo detectado antes y cómo?
- ¿Qué pudo haber hecho que la investigación fuera más rápida?
- ¿Se siguieron los procedimientos de respuesta a incidentes documentados? ¿Fueron adecuados?
- ¿El intercambio de información con otras partes interesadas se realizó de manera oportuna? ¿Cómo podría mejorarse?
- ¿Fue eficaz la colaboración con otros equipos (de AWS seguridad, de cuentas, de AWS desarrollo y de seguridad del cliente)? Si no, ¿qué podría mejorarse?
- ¿Qué pasos de preparación faltaban que pudieran haber ayudado: matrices de escalamiento, RACI, modelos de responsabilidad compartida, etc.? ¿Es necesario actualizar algún Runbook?
- ¿Cuál fue la diferencia entre la evaluación de impacto inicial y la evaluación de impacto final? ¿Qué podemos hacer para mejorar la precisión de las evaluaciones en una fase temprana de la respuesta al incidente?
- ¿Cuáles son los elementos de acción que se derivan de las lecciones aprendidas?

## Guías de respuesta a incidentes de seguridad en AMS

Esta sección contiene dos manuales:

- Respuesta a la actividad del usuario root
- Respuesta a eventos de malware

## Respuesta a la actividad del usuario root

El usuario raíz es el superusuario de su AWS cuenta. Tenga en cuenta que AMS monitorea el uso de root. Se recomienda utilizar el usuario root solo para las pocas tareas que lo requieran, como cambiar la configuración de la cuenta, activar el acceso AWS Identity and Access Management (IAM) a la facturación y la gestión de costes, cambiar la contraseña root y activar la autenticación multifactor (MFA). Para obtener más información, consulte Tareas que requieren credenciales de usuario raíz.

Para obtener más información sobre cómo informar a AMS del uso raíz planificado, consulte Cuándo y cómo usar la cuenta raíz en AMS.

Cuando se detecta actividad por parte del usuario root (intentos fallidos de iniciar sesión que podrían indicar un ataque de fuerza bruta o actividad en la cuenta tras iniciar sesión correctamente), se genera un evento y se envía un incidente a tus contactos de seguridad definidos.

AWS Managed Services Operations investiga la actividad no planificada de los usuarios raíz, lleva a cabo la recopilación, clasificación y análisis de datos y realiza actividades de contención según sus instrucciones, seguidas de un análisis posterior al evento.

Si tiene el modelo operativo AMS Advanced, recibirá comunicaciones adicionales de los ingenieros de AMS CSDM y AMS Ops en las que se confirmará la actividad no planificada de los usuarios raíz debido a la responsabilidad de AMS de proteger las credenciales de los usuarios raíz. AMS investiga la actividad de los usuarios root hasta que se confirme el camino a seguir.

### Preparación

Informe a AMS de cualquier uso planificado del usuario root enviando una solicitud de servicio de AMS con los datos y las horas del evento planificado para evitar actividades innecesarias de respuesta a incidentes.

Póngase en contacto periódicamente GameDays con AMS para validar que los procesos de respuesta a incidentes de los clientes de AMS, las personas y los sistemas estén actualizados, y desarrolle la memoria muscular con las personas responsables para lograr una respuesta más rápida a los incidentes.

Fase A: Detectar

AMS supervisa la actividad raíz de las cuentas a través de fuentes de detección, incluida GuardDuty la supervisión de AMS.

Si tiene AMS Accelerate, el modelo operativo responde al incidente y solicita que se investigue la actividad inesperada del usuario root. Cuando esto ocurre, AMS Operations inicia el manual de cuentas comprometidas.

Si dispone de AMS Advanced, el modelo operativo responde al incidente o informa al CSDM de cualquier actividad planificada por parte de un usuario root para poner fin a una investigación en curso sobre una situación comprometida en la cuenta.

Fase B: analizar

AMS lleva a cabo una investigación exhaustiva de los eventos del usuario raíz cuando determina que la actividad no está autorizada. Utilizando tanto las automatizaciones como el equipo de respuesta de seguridad de AMS, los registros y los eventos se analizan para detectar anomalías y comportamientos inesperados en los usuarios root. Se proporcionan registros para ayudar a determinar si la actividad es desconocida, si se trata de un evento de un usuario raíz autorizado o si requiere una investigación más profunda.

Algunos ejemplos de la información proporcionada durante la investigación para respaldar las comprobaciones internas son:

- Información de la cuenta: ¿En qué cuenta se utilizó la cuenta raíz?
- Dirección de correo electrónico del usuario raíz: cada usuario raíz está asociado a una dirección de correo electrónico de su organización
- Detalles de autenticación: ¿desde dónde y cuándo accedió el usuario raíz a su entorno?
- Registros de actividad: ¿Qué hizo el usuario cuando inició sesión como root? Estos registros se presentan en forma de CloudWatch eventos. Comprender cómo leer estos registros ayuda en la investigación.

Se recomienda estar preparado para recibir la información de análisis y tener un plan sobre cómo llegar a los puntos de contacto autorizados para las cuentas de su organización. Como los usuarios raíz no se nombran como individuos, determinar quién tiene acceso a la dirección de correo electrónico raíz utilizada para la cuenta en su organización ayuda a dirigir rápidamente las preguntas internamente.

Fase C: Contener y erradicar

AMS colabora con sus equipos de seguridad para llevar a cabo la contención siguiendo las instrucciones de sus contactos autorizados de Customer Security. Las opciones de contención incluyen:

- Rotación de las credenciales y claves apropiadas.
- Finalizar las sesiones activas de las cuentas y los recursos.
- Erradicar los recursos creados.

Durante las actividades de contención, AMS trabaja en estrecha colaboración con su equipo de seguridad para garantizar que se minimice cualquier interrupción en sus cargas de trabajo y que las credenciales raíz estén debidamente protegidas.

Una vez completado el plan de contención, trabajará con el equipo de operaciones de AMS para tomar las medidas de recuperación necesarias.

Informe posterior al incidente

Según sea necesario, AMS inicia el proceso de revisión de la investigación para identificar las lecciones aprendidas. Como parte de completar un COE, AMS comunica cualquier hallazgo relevante a los clientes afectados para ayudarlos a mejorar su proceso de respuesta a los incidentes.

AMS documenta todos los detalles finales de la investigación, recopila las métricas adecuadas y, a continuación, informa del incidente a los equipos internos de AMS que necesiten información, incluidos el CSDM y la CA asignados.

## Respuesta a eventos de malware

Las EC2 instancias de Amazon se utilizan para alojar diversas cargas de trabajo, incluido software de terceros y software desarrollado a medida que implementan los equipos de aplicaciones de las organizaciones. AMS le ofrece y le anima a implementar sus cargas de trabajo en imágenes parcheadas y mantenidas de forma continua por AMS.

Durante el funcionamiento de las instancias, AMS monitorea las anomalías en el comportamiento o la actividad a través de una variedad de controles de detección de seguridad, incluidos Amazon GuardDuty, Network Traffic y los feeds internos de Inteligencia de Amenazas de Amazon.

AMS también monitorea los hallazgos de GuardDuty malware. Están disponibles tanto en AMS Advanced como en AMS Accelerate, si están activados. Consulta Protección contra malware en Amazon GuardDuty para obtener más información.

> **Note**
>
> Si has optado por Bring Your Own EPS, el proceso de respuesta a los incidentes es diferente al que se describe en esta página. Para obtener más información, consulte la documentación a la que se hace referencia.

Cuando se detecta malware, se crea un incidente y se le notifica del mismo. Esta notificación va seguida de cualquier actividad de reparación que se haya producido. AMS Operations investiga, recopila, clasifica y analiza los datos y, a continuación, lleva a cabo actividades de contención según sus instrucciones, seguidas de un análisis posterior al suceso.

Fase A: Detectar

AMS monitorea los eventos en las instancias con. GuardDuty AMS determina las actividades de enriquecimiento y clasificación adecuadas para ayudarle a tomar decisiones de contención o aceptación de riesgos en función del tipo de hallazgo o alerta.

La recopilación de datos se realiza en función del tipo de hallazgo. La recopilación de datos implica consultar múltiples fuentes de datos, tanto internas como externas, a la cuenta afectada para obtener una idea de la actividad observada o de las configuraciones preocupantes.

AMS correlaciona el hallazgo con cualquier otra alarma y alerta o telemetría de cualquier cuenta afectada o plataforma de inteligencia de amenazas de AMS.

Fase B: analizar

Una vez recopilados los datos, se analizan para identificar cualquier actividad o indicador preocupante. Durante esta fase de la investigación, AMS colabora con usted para integrar el conocimiento empresarial y el dominio de las instancias y las cargas de trabajo a fin de comprender qué se espera y qué es lo que está fuera de lo común.

Algunos ejemplos de la información proporcionada durante la investigación para respaldar las comprobaciones internas son:

- Información de la cuenta: ¿En qué cuenta se observó la actividad del malware?

- Detalles de la instancia: ¿Qué instancias están implicadas en los eventos de malware?
- Fecha y hora del evento: ¿Cuándo se activó la alerta?
- Información sobre la carga de trabajo: ¿Qué se está ejecutando en la instancia?
- Detalles sobre el malware, si corresponde: familias de malware e información de código abierto sobre el malware.
- Detalles sobre los usuarios o las funciones: ¿Qué usuarios o funciones se ven afectados por la actividad o participan en ella?
- Registros de actividad: ¿Qué actividades se registran en la instancia? Se presentan en forma de CloudWatch eventos y eventos del sistema de la instancia. Saber cómo leer estos registros le ayudará en la investigación
- Actividad de red: ¿Qué puntos finales se conectan a la instancia, a qué se conecta la instancia y cuál es el análisis del tráfico?

Se recomienda estar preparado para recibir información sobre la investigación y tener un plan sobre cómo contactar con los puntos de contacto adecuados para las cuentas, las instancias y las cargas de trabajo de la organización. Comprender la topología de la red y la conexión prevista puede ayudar a acelerar el análisis de impacto. El conocimiento de las pruebas de penetración planificadas en el entorno y de las implementaciones recientes realizadas por los propietarios de las aplicaciones también puede acelerar la investigación.

Si determina que la actividad está planificada y autorizada, el incidente se actualiza y la investigación finaliza. Si se confirma el compromiso, usted y AMS determinarán el plan de contención adecuado.

Fase C: Contener y erradicar

AMS colabora con usted para determinar las actividades de contención adecuadas en función de los datos recopilados y la información conocida. Las opciones de contención incluyen, pero no se limitan a:

- Preservar los datos mediante instantáneas
- Modificar las reglas de red para limitar el tráfico entrante o saliente de las instancias
- Modificar las políticas de usuarios y roles de SCP e IAM para limitar el acceso
- Finalización, suspensión o desactivación de instancias
- Finalizar cualquier conexión persistente
- Rotación de las credenciales y claves apropiadas

Si opta por realizar una actividad de erradicación contra la instancia, AMS lo ayudará a lograrlo. Las opciones incluyen, pero no se limitan a:

- Eliminar cualquier software no deseado
- Reconstruir la instancia a partir de una imagen limpia y completamente parcheada y volver a implementar las aplicaciones y la configuración
- Restauración de la instancia a partir de una copia de seguridad anterior
- Implementar aplicaciones y servicios en otra instancia de su cuenta que pueda ser adecuada para alojar las cargas de trabajo.

Es importante determinar cómo se distribuyó y ejecutó el malware en la instancia antes de restablecer el servicio para asegurarse de que se aplican todos los controles adicionales que impidan que el malware vuelva a aparecer en la instancia. AMS proporciona información o información adicional a sus socios o equipos forenses, según sea necesario, para respaldar la labor forense.

En este punto, trabajará con AMS Operations para las actividades de recuperación. AMS trabaja en estrecha colaboración con usted para minimizar las interrupciones en las cargas de trabajo y proteger las instancias.

Informe posterior al incidente

Según sea necesario, AMS inicia el proceso de revisión de la investigación para identificar las lecciones aprendidas. Como parte de completar un COE, AMS le comunica los hallazgos relevantes para ayudarlo a mejorar su proceso de respuesta a incidentes.

AMS documenta los detalles finales de la investigación, recopila las métricas adecuadas e informa del incidente a los equipos internos de AMS que requieren información, incluidos el CSDM y el CA asignados.

## Registro y supervisión de eventos de seguridad en Accelerate

Las cuentas inscritas en AMS Accelerate se configuran con un despliegue básico de CloudWatch eventos y alarmas que se ha optimizado para reducir el ruido e identificar los indicios de un incidente real. AMS Accelerate también se emplea GuardDuty para monitorear las cuentas. Para obtener más información, consulte Supervise con GuardDuty.

# Cumplimiento de la configuración en Accelerate

AMS Accelerate le ayuda a configurar sus recursos con altos estándares de seguridad e integridad operativa, y a cumplir con los siguientes estándares del sector:

- Centro de Seguridad de Internet (CIS)
- Marco de seguridad en la nube (CSF) del Instituto Nacional de Estándares y Tecnología (NIST)
- Ley de Portabilidad y Responsabilidad de Seguros Médicos de EE. UU (Health Insurance Portability and Accountability Act, HIPAA).
- Estándar de seguridad de datos (DSS) de la industria de tarjetas de pago (PCI)

Para ello, implementamos todo nuestro conjunto de AWS Config reglas de cumplimiento en su cuenta, consulte. Biblioteca de reglas AMS Config Una AWS Config regla representa las configuraciones deseadas para un recurso y se evalúa en función de los cambios de configuración en la configuración de AWS los recursos. Cualquier cambio de configuración desencadena un gran número de reglas para comprobar su conformidad. Por ejemplo, supongamos que crea un bucket de Amazon S3 y lo configura para que sea legible públicamente, infringiendo los estándares del NIST. La bucket-public-read-prohibited regla ams-nist-cis-s 3 detecta la infracción y etiqueta el bucket de S3 como no compatible en el informe de configuración. Como esta regla pertenece a la categoría de corrección automática de incidentes, crea inmediatamente un informe de incidentes que le avisa del problema. Otras infracciones más graves de las reglas pueden provocar que AMS solucione el problema automáticamente. Consulte Respuestas a las infracciones en Accelerate.

> **Important**
>
> Si quiere que hagamos más, por ejemplo, si quiere que AMS corrija una infracción en su nombre, independientemente de su categoría, envíe una solicitud de servicio en la que pida a AMS que corrija los recursos no conformes por usted. En la solicitud de servicio, incluya un comentario como «Como parte de la corrección de la regla de configuración de AMS, corrija los recursos *RESOURCE_ARNS_OR_IDs* no conformes y configure la regla de la cuenta» y *CONFIG_RULE_NAME* añada los datos necesarios para subsanar la infracción.
> Si quiere que hagamos menos, por ejemplo, si no quiere que tomemos medidas en relación con un segmento de S3 concreto que, por diseño, requiere acceso público, puede crear excepciones, consulte. Crear excepciones a las reglas en Accelerate

# Biblioteca de reglas AMS Config

Accelerate despliega una biblioteca de reglas de configuración de AMS para proteger su cuenta. Estas reglas de configuración comienzan con `ams-`. Puede ver las reglas de su cuenta y su estado de conformidad desde la AWS Config consola, la AWS CLI o la AWS Config API. Para obtener información general sobre el uso AWS Config, consulte ViewingConfiguration Cumplimiento.

> **Note**
>
> Regiones de AWS En el caso de las regiones con suscripción voluntaria y de gov cloud, solo implementamos un subconjunto de las reglas de configuración debido a las restricciones regionales. Comprueba la disponibilidad de las reglas en las regiones consultando el enlace asociado al identificador en la tabla de reglas de configuración de AMS Accelerate.
> No puede eliminar ninguna de las reglas de configuración de AMS implementadas.

## Tabla de reglas

Descargar como ams_config_rules.zip.

Reglas de configuración de AMS

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-guardduty-habilitado-centralizado | GuardDuty | Periódico | Remediar | CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (2) (iv), 164.312 (e) (2) (ii); PCI: 2.2, 3.4, 8.2.1; |
| ams-nist-cis-vpc-flow-logs-enabled | VPC | Periódico | Remediar | CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.PT-1; HIPAA: 164.308 (a) (3) (ii) (A), 164.312 (b); PCI: 2.2, 10.1, 10.3.2, 10.3.3, 10.3.4, 10.3.4, 10.3.5, 10.3.6; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-eks-secrets-encrypted | EKS | Periódico | Incidente | CIS: NA; NIST-CSF: NA; HIPAA: NA; PCI: NA; |
| ams-eks-endpoint-no-acceso público | EKS | Periódico | Incidente | CIS: NA; NIST-CSF: NA; HIPAA: NA; PCI: NA; |
| ams-nist-cis-vpc-default-security-group-closed | VPC | Config changes | Incidente | CIS: CIS.11, CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164.312 (e) (1); PCI: 1.2,1.3,2.1,2.2,1.2.1,1.3.1,1.3.1,1.3.2,2.2.2; |
| ams-nist-cis-iam-política de contraseñas | IAM | Periódico | Incidente | CIS: NA; NIST-CSF: PR.AC-1, PR.AC-4; HIPAA: 164,308 (a) (3) (i) ,164,308 (a) (3) (ii) (A) ,164,308 (a) (3) (ii) (B) ,164,308 (a) (4) (i) ,164,308 (a) (4) (ii) (A) ,164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1); PCI: 7.1.2, 7.1.3, 7.2.1, 7.2.2; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-iam-root-access-key-check | IAM | Periódico | Incidente | CIS: CIS.16, CIS.4; NIST-CSF: PR.AC-1, PR.AC-4, PR.PT-3; HIPAA: 164,308 (a) (3) (i) ,164,308 (a) (ii) (A) ,164,308 (a) (3) (ii) (B) ,164,308 (a) (a), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1); PCI: 2.2,7.1.2,7.1.3,7.2.1.7.2.2; |
| ams-nist-cis-iam-user-mfa-enabled | IAM | Periódico | Incidente | CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-4; HIPAA: 164,308 (a) (3) (i) ,164,308 (a) (3) (ii) (A) ,164,308 (a) (3) (ii) (B) ,164,308 (a) (4) (i) ,164,308 (a) ,164,308 (a) ,164,308 (a) ,164,308 (a), (4) (ii) (A) 64.308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1); PCI: 2.2,7.1.2,7.1.3, 7.2.1; |
| ams-nist-cis-restricted-ssh | Grupos de seguridad | Config changes | Incidente | CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-4; HIPAA: 164,308 (a) (3) (i) ,164,308 (a) (4) (ii) (A) ,164,308 (a) (4) (ii) (B) ,164,308 (a) (4) (ii) (C) ,164.312 (a) (1); PCI: 2.2, 7.2, 8.1, 8.1.4; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-restricted-puertos comunes | Grupos de seguridad | Config changes | Incidente | CIS: CIS.11, CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164,308 (a) (3) (i) ,164.308 (a) (3) (ii) (B) ,164.308 (a) (4) (i) ,164.308 (a) (4) (ii)) (A), 164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1.2,1.3,2 ,2,1.3.2,1.3.2,2.2.2; |
| ams-nist-cis-s3 account-level-public-access - bloques | S3 | Config changes | Incidente | CIS: CIS.9, CIS.12, CIS.14; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (a) (4) (ii) (A) ,164.308 (a) (4) (ii), 164.308 (a) (4) (ii), 164,308 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1.2,1.2.1 ,1.3.1,1.3.2,1.3.4, 1.3.6, 2.2, 2.2.2; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-s3- bucket-public-read-prohibited | S3 | Config changes | Incidente | CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (a) (4) (ii) (A) ,164.308 (a) (4) (ii), 164.308 (a) (4) (ii), 164,308 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1.2,1.3,2.2,1.2.1,1.3.1,1.3 .2,1.3.4, .3.6, 2.2.2; |
| ams-nist-cis-s3- bucket-public-write-prohibited | S3 | Config changes | Incidente | CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (a) (4) (ii) (A) ,164.308 (a) (4) (ii), 164.308 (a) (4) (ii), 164,308 (a) (4) (ii) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1.2,1.3,2.2,1.2.1,1.3.1,1.3 .2,1.3.4, .3.6, 2.2.2; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-sbucket-server-side-encryptionHabilitado para 3 | S3 | Config changes | Incidente | CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (2) (iv), 164.312 (c) (2), 164.312 (e) (2) (ii); PCI: 2.2, 3.4, 10.5, 8.2.1; |
| ams-nist-cis-securityhub-habilitado | Centro de seguridad | Periódico | Incidente | CIS: CIS.3, CIS.4, CIS.6, CIS.12, CIS.16, CIS.19; NIST-CSF: PR.DS-5, PR.PT-1; HIPAA: 164.312 (b); PCI: NA; |
| ams-nist-cis-ecinstance-managed-by-systems2-administrador | EC2 | Config changes | Informe | CIS: CIS.2, CIS.5; NIST-CSF: ID.AM-2, PR.IP-1; HIPAA: 164.308 (a) (5) (ii) (B); PCI: 2.4; |
| ams-nist-cis-cloudtrail-habilitado | CloudTrail | Periódico | Informe | CIS: CIS.16, CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.MA-2, PR.PT-1; HIPAA: 164.308 (a) (3) (ii) (A), 164.308 (a) (5) (ii) (C), 164.312 (b); PCI: 10.1,10.2.1,10.2.2 ,102.3, 10,4, 102,5, 10,2, 102,7, 103,1,103,2,10,3, 10,3, 103,4, 103,5, 103,6; |
| ams-nist-cis-access-teclas giradas | IAM | Periódico | Informe | CIS: CIS.16; NIST-CSF: PR.AC-1; HIPAA: 164.308 (a) (4) (ii) (B); PCI: 2.2; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-acm-certificate-expiration-check | Certificate Manager | Config changes | Informe | CIS: CIS.13, CIS.14; NIST-CSF: PR.AC-5, PR.PT-4; HIPAA: NA; PCI: 4.1; |
| ams-nist-cis-alb-comprobar http-to-https-redirection | ALB | Periódico | Informe | CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (1), 164.312 (e) (2) (i), 164.312 (e) (2) (ii); PCI: 2.3, 4.1, 8.2.1; |
| ams-nist-cis-api- encriptado gw-cache-enabled-and | API Gateway | Config changes | Informe | CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4; |
| ams-nist-cis-api-gw-execution-logging-enabled | API Gateway | Config changes | Informe | CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.PT-1; HIPAA: 164.312 (b); PCI: 10.1, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.5.4; |
| ams-nist-autoscaling-group-elb-healthcheck-required | ELB | Config changes | Informe | CIS: NA; NIST-CSF: PR.PT-1, PR.PT-5; HIPAA: 164.312 (b); PCI: 2.2; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-cloud-trail-encryption-enabled | CloudTrail | Periódico | Informe | CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (2) (iv), 164.312 (e) (2) (ii); PCI: 2.2, 3.4, 10.5; |
| ams-nist-cis-cloud- -habilitado trail-log-file-validation | CloudTrail | Periódico | Informe | CIS: CIS.6; NIST-CSF: PR.DS-6; HIPAA: 164.312 (c) (1), 164.312 (c) (2); PCI: 2.2, 10.5, 11.5, 10.5.2, 10.5.5; |
| ams-nist-cis-cloudtrail-Compatible con eventos de datos s3 | CloudTrail | Periódico | Informe | CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.PT-1; HIPAA: 164.308 (a) (3) (ii) (A), 164.312 (b); PCI: 2.2,10.1,10.2.1,10.2.2,10.2.3,10.2.5, 10.3.1, 10.3.2, 10.3.2, 10.3.3, 10.3.4, 10.3.5 10.3.6; |
| ams-nist-cis-cloudwatch-alarm-action-check | CloudWatch | Config changes | Informe | CIS: CIS.13, CIS.14; NIST-CSF: NA; HIPAA: 164.312 (a) (2) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4; |
| ams-nist-cis-cloudwatch-log-group-encrypted | CloudWatch | Periódico | Informe | CIS: CIS.13, CIS.14; NIST-CSF: NA; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-codebuild-project-envvar-awscred-check | CodeBuild | Config changes | Informe | CIS: CIS.18; NIST-CSF: PR.DS-5; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C), 164.312 (a) (1); PCI: 8.2.1; |
| ams-nist-cis-codebuild-comprobar project-source-repo-url | CodeBuild | Config changes | Informe | CIS: CIS.18; NIST-CSF: PR.DS-5; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C), 164.312 (a) (1); PCI: 8.2.1; |
| ams-nist-cis-db-instance-backup-enabled | RDS | Config changes | Informe | CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i), 164.308 (a) (7) (ii) (A) ,164.308 (a) (7) (ii) (B); PCI: NA; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-dms-replication-not-public | DMS | Periódico | Informe | CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (a) (4) (ii) (A) ,164.308 (a) (4) (ii), 164.308 (a) (4) (ii), 164,308 (a) (4) (ii) (C) ,164.312 (a) (1), 164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4, 1.3.6, 2.2.2; |
| ams-nist-dynamodb-autoscaling-habilitado | DynamoDB | Periódico | Informe | CIS: NA; NIST-CSF: ID.BE-5, PR.DS-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i), 164.308 (a) (7) (ii) (C); PCI: NA; |
| ams-nist-cis-dynamodbCompatible con -PIRT | DynamoDB | Periódico | Informe | CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i), 164.308 (a) (7) (ii) (A) ,164.308 (a) (7) (ii) (B); PCI: NA; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-dynamodb-throughput-control de límites | DynamoDB | Periódico | Informe | CIS: NA; NIST-CSF: NA; HIPAA: 164.312 (b); PCI: NA; |
| ams-nist-ebs-optimized-instancia | EBS | Config changes | Informe | CIS: NA; NIST-CSF: NA; HIPAA: 164.308 (a) (7) (i); PCI: NA; |
| ams-nist-cis-ebs-snapshot-public-restorable-check | EBS | Periódico | Informe | CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (a) (4) (ii) (A) ,164.308 (a) (4) (ii), 164.308 (a) (4) (ii), 164,308 (a) (4) (ii) (C) ,164.312 (a) (1), 164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4, 1.3.6, 2.2.2; |
| ams-nist-ec2- instance-detailed-monitoring-enabled | EC2 | Config changes | Informe | CIS: NA; NIST-CSF: DE.AE-1, PR.PT-1; HIPAA: 164.312 (b); PCI: NA; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-ec2- instance-no-public-ip | EC2 | Config changes | Informe | CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164,308 (a) (3) (i) ,164,308 (a) (4) (ii) (A) ,164,308 (a) (4) (ii) (C) ,164.312 (a) (1), 164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4, 1.3.6, 2.2.2; |
| ams-nist-cis-ecmanagedinstance-association-compliance-statusVerificación 2 | EC2 | Config changes | Informe | CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C) ,164.312 (a) (a) (1), 164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4, 1.3.6, 2.2.2; |
| ams-nist-cis-ecmanagedinstance-patch-compliance-statusVerificación 2 | EC2 | Config changes | Informe | CIS: CIS.2, CIS.5; NIST-CSF: ID.AM-2, PR.IP-1; HIPAA: 164.308 (a) (5) (ii) (B); PCI: 6.2; |
| ams-nist-cis-ecInstancia de 2 paradas | EC2 | Periódico | Informe | CIS: CIS.2; NIST-CSF: ID.AM-2, PR.IP-1; HIPAA: NA; PCI: NA; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-ec2- volume-in use-check | EC2 | Config changes | Informe | CIS: CIS.2; NIST-CSF: PR.IP-1; HIPAA: NA; PCI: NA; |
| ams-nist-cis-efs-cheque cifrado | EFS | Periódico | Informe | CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4, 8.2.1; |
| ams-nist-cis-eip-adjunto | EC2 | Config changes | Informe | CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4, 8.2.1; |
| ams-nist-cis-elasticache-comprobar redis-cluster-automatic-backup | ElastiCache | Periódico | Informe | CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i), 164.308 (a) (7) (ii) (A), 164.308 (a) (7) (ii) (B); PCI: NA; |
| ams-nist-cis-opensearch-encrypted-at-rest | OpenSearch | Periódico | Informe | CIS: CIS.14, CIS.13; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4, 8.2.1; |
| ams-nist-cis-opensearch-in-vpc-only | OpenSearch | Periódico | Informe | CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4, 8.2.1; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-elb-acm-certificate-required | Certificate Manager | Config changes | Informe | CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A) ,164.308 (a), 164.308 (a) (4) (ii), 164,308 (a), 164,308 (a) (4) (ii) (C) 64.312 (a) (1), 164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4, 1.3.6, 2.2.2; |
| ams-nist-elb-deletion-protección habilitada | ELB | Config changes | Informe | CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312 (a) (2) (2) (iv), 164.312 (e) (1), 164.312 (e) (2), 164.312 (e) (2) (ii); PCI: 4.1, 8.2.1; |
| ams-nist-cis-elb-Habilitado para el registro | ELB | Config changes | Informe | CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.PT-1; HIPAA: 164.312 (b); PCI: 10.1, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.5.4; |
| ams-nist-cis-emr-Compatible con Kerberos | EMR | Periódico | Informe | CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.PT-1; HIPAA: 164.312 (b); PCI: 10.1, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.5.4; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-emr-master-no-public-ip | EMR | Periódico | Informe | CIS: CIS.14, CIS.16; NIST-CSF: PR.AC-1, PR.AC-4, PR.AC-6; HIPAA: 164,308 (a) (3) (i) ,164,308 (a) (ii) (A) ,164,308 (a) (3) (ii) (B) ,164,308 (a) (a) (4) (ii) (A), 164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1); PCI: 7.2.1; |
| ams-nist-cis-encrypted-volúmenes | EBS | Config changes | Informe | CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C) ,164.312 (a) (a) (1), 164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4, 1.3.6, 2.2.2; |
| ams-nist-cis-guardduty-non-archived-findings | GuardDuty | Periódico | Informe | CIS: CIS.12, CIS.13, CIS.16, CIS.19, CIS.3, CIS.4, CIS.6, CIS.8; NIST-CSF: DE.AE-2, DE.AE-3, DE.CM-4, DE.DP-5, ID.RA-1, ID.RA-3, PR.DS-5, PR.PT-1; HIPAA: 164.308 (a) (5) (ii) (C), 164,308 (a) (6) (ii), 164,312 (b); PCI: 6.1, 11.4, 5.1.2; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-iam-group-has-users-check | IAM | Config changes | Informe | CIS: NA; NIST-CSF: PR.AC-4, PR.AC-1; HIPAA: 164,308 (a) (3) (i) ,164,308 (a) (3) (ii) (A) ,164,308 (a) (3) (ii) (B) ,164,308 (a) (4) (i) ,164,308 (a) (4) (ii) (A) ,164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1); PCI: 7.1.2, 7.1.3, 7.2.1, 7.2.2; |
| ams-nist-cis-iam- policy-no-statements-with -acceso de administrador | IAM | Config changes | Informe | CIS: CIS.16; NIST-CSF: PR.AC-6, PR.AC-7; HIPAA: 164.308 (a) (4) (ii) (B), 164.308 (a) (5) (ii) (D), 164.312 (d); PCI: 8.2.3, 8.2.4, 8.2.5; |
| ams-nist-cis-iam-user-group-membership-check | IAM | Config changes | Informe | CIS: CIS.16, CIS.4; NIST-CSF: PR.AC-1, PR.AC-4, PR.PT-3; HIPAA: 164,308 (a) (3) (i) ,164,308 (a) (4) (ii) (A) ,164,308 (a) (4) (ii) (B) ,164,308 (a) (4) (ii) (C) ,164.312 (a) (1), 164.312 (a) (2) (i); PCI: 2.2,7.1.2,7.2.1,8.1.1; |
| ams-nist-cis-iam-user-no-policies-check | IAM | Config changes | Informe | CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-7; HIPAA: 164.308 (a) (4) (ii) (B), 164.312 (d); PCI: 8.3; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-iam-user-unused-credentials-check | IAM | Periódico | Informe | CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-4, PR.PT-3; HIPAA: 164,308 (a) (3) (i) ,164,308 (a) (ii) (A) ,164,308 (a) (3) (ii) (B) ,164,308 (a) (a) (4) (ii) (A), 164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1); PCI: 2.2,7.1.2,7.1.3.7.2.1.7.2.2; |
| ams-nist-cis-ec2- instances-in-vpc | EC2 | Config changes | Informe | CIS: CIS.11, CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164,308 (a) (3) (i) ,164.308 (a) (3) (ii) (B) ,164.308 (a) (4) (i) ,164.308 (a) (4) (ii)) (A), 164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1.2,1.3,2 ,2,1.3.2,1.3.2,2.2.2; |
| ams-nist-cis-internet-gateway-authorized-vpc-only | Puerta de enlace de Internet | Periódico | Informe | CIS: CIS.9, CIS.12; NIST-CSF: NA; HIPAA: NA; PCI: NA; |
| ams-nist-cis-kms- -eliminación cmk-not-scheduled-for | KMS | Periódico | Informe | CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: NA; PCI: 3.5, 3.6; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-lambda-concurrency-comprobar | Lambda | Config changes | Informe | CIS: NA; NIST-CSF: NA; HIPAA: 164.312 (b); PCI: NA; |
| ams-nist-lambda-dlq-comprobar | Lambda | Config changes | Informe | CIS: NA; NIST-CSF: NA; HIPAA: 164.312 (b); PCI: NA; |
| ams-nist-cis-lambda-function-public-access-prohibited | Lambda | Config changes | Informe | CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A) ,164.308 (a), 164.308 (a) (4) (ii), 164,308 (a), 164,308 (a) (4) (ii) (C) 64.312 (a) (1), 164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.2,1.3.4, 2.2.2; |
| ams-nist-cis-lambda-interior-vpc | Lambda | Config changes | Informe | CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C) ,164.312 (a) (a) (1), 164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4, 2.2.2; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-mfa- enabled-for-iam-console-acceso | IAM | Periódico | Informe | CIS: CIS.16; NIST-CSF: PR.AC-7; HIPAA: 164.312 (d); PCI: 2.2, 8.3; |
| ams-nist-cis-multi-region-cloudtrail-enabled | CloudTrail | Periódico | Informe | CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.MA-2, PR.PT-1; HIPAA: 164.308 (a) (3) (ii) (A), 164.312 (b); PCI: 2.2,10.1,10.2.1,10 .2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.710. 3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6; |
| ams-nist-rds-enhanced-habilitado para monitoreo | RDS | Config changes | Informe | CIS: NA; NIST-CSF: PR.PT-1; HIPAA: 164.312 (b); PCI: NA; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-rds-instance-public-access-check | RDS | Config changes | Informe | CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (a) (4) (ii) (A) ,164.308 (a) (4) (ii), 164.308 (a) (4) (ii), 164,308 (a) (4) (ii) (C) ,164.312 (a) (1), 164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4, 1.3.6, 2.2.2; |
| ams-nist-rds-multi-az-soporte | RDS | Config changes | Informe | CIS: NA; NIST-CSF: ID.BE-5, PR.DS-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i), 164.308 (a) (7) (ii) (C); PCI: NA; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-rds-snapshots-public-prohibited | RDS | Config changes | Informe | CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (a) (4) (ii) (A) ,164.308 (a) (4) (ii), 164.308 (a) (4) (ii), 164,308 (a) (4) (ii) (C) ,164.312 (a) (1), 164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4, 1.3.6, 2.2.2; |
| ams-nist-cis-rds-cifrado en almacenamiento | RDS | Config changes | Informe | CIS: CIS.13, CIS.5, CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-1, PR.PT-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (b), 164.312 (e) (2) (ii); PCI: 3.4, 10.1, 10.2.1, 10.2.2, 10.2.2.10.3 2,4, 102,5, 103,3,1, 10,3, 10,3, 103,4,103,5, 103,6, 8,21; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-redshift-cluster-configuration-check | RedShift | Config changes | Informe | CIS: CIS.6, CIS.13, CIS.5; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-1, PR.PT-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (b), 164.312 (e) (2) (ii); PCI: 3.4, 8.2.1, 10.2.1, 10.2.1, 10.2.10.10.10.10 2.3, 10.2.4, 10.2.5, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6; |
| ams-nist-cis-redshift-cluster-public-access-check | RedShift | Config changes | Informe | CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (a) (4) (ii) (A) ,164.308 (a) (4) (ii), 164.308 (a) (4) (ii), 164,308 (a) (4) (ii) (C) ,164.312 (a) (1), 164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4, 1.3.6, 2.2.2; |
| ams-nist-cis-redshift-require-tls-ssl | RedShift | Periódico | Informe | CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (1), 164.312 (e) (2) (i), 164.312 (e) (2) (ii); PCI: 2.3, 4.1; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-root-account-hardware-mfa-enabled | IAM | Periódico | Informe | CIS: CIS.16, CIS.4; NIST-CSF: PR.AC-7; HIPAA: 164.312 (d); PCI: 2.2, 8.3; |
| ams-nist-cis-root-account-mfa-enabled | IAM | Periódico | Informe | CIS: CIS.16, CIS.4; NIST-CSF: PR.AC-7 ; HIPAA: 164.312 (d); PCI: 2.2, 8.3; |
| ams-nist-cis-s3- bucket-default-lock-enabled | S3 | Config changes | Informe | CIS: CIS.14, CIS.13; NIST-CSF: ID.BE-5, PR.PT-5, RC.RP-1; HIPAA: NA; PCI: NA; |
| ams-nist-cis-s3- bucket-logging-enabled | S3 | Config changes | Informe | CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.PT-1; HIPAA: 164.308 (a) (3) (ii) (A), 164.312 (b); PCI: 2.2,10.1,10.2.1,10.2.2,10.2.3,10.2.4,10.2.5, 10.2.5,10.2.7, 10.3.1, 3.10.2.2, 10.3.10.3.4, 10.3.5, 10.3.6; |
| ams-nist-cis-s3- bucket-replication-enabled | S3 | Config changes | Informe | CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i), 164.308 (a) (7) (ii) (A) ,164.308 (a) (7) (ii) (B); PCI: 2.2, 10.5.3; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-s3- bucket-ssl-requests-only | S3 | Config changes | Informe | CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312 (a) (2) (2) (iv), 164.312 (c) (2), 164.312 (e) (2) (i), 164.312 (e), 164.312 (e) (2) (ii); PCI: 2.2, 4.1, 8.2.1; |
| ams-nist-cis-s3- bucket-versioning-enabled | S3 | Periódico | Informe | CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.DS-6, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164,308 (a) (7) (i) ,164,308 (a) (7) (ii) (A) ,164,308 (a) (7) (ii) (B) ,164.312 (c) (1), 164,312 (c) (2); PCI: 10.5.3; |
| ams-nist-cis-sagemaker-endpoint-configuration-kms-key - configurado | SageMaker | Periódico | Informe | CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4, 8.2.1; |
| ams-nist-cis-sagemaker--configurado notebook-instance-kms-key | SageMaker | Periódico | Informe | CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4, 8.2.1; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-sagemaker- -acceso notebook-no-direct-internet | SageMaker | Periódico | Informe | CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A) ,164.308 (a), 164.308 (a) (4) (ii), 164,308 (a), 164,308 (a) (4) (ii) (C) 64.312 (a) (1), 164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4, 1.3.6, 2.2.2; |
| ams-nist-cis-secretsmanager-rotation-enabled-check | Secrets Manager | Config changes | Informe | CIS: CIS.16; NIST-CSF: PR.AC-1; HIPAA: 164.308 (a) (4) (ii) (B); PCI: NA; |
| ams-nist-cis-secretsmanager-scheduled-rotation-success-check | Secrets Manager | Config changes | Informe | CIS: CIS.16; NIST-CSF: PR.AC-1; HIPAA: 164.308 (a) (4) (ii) (B); PCI: NA; |
| ams-nist-cis-sns-kms cifrados | SNS | Config changes | Informe | CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (2) (iv), 164.312 (e) (2) (ii); PCI: 8.2.1; |

| Nombre de la regla | Servicio | Desencadenador | Acción | Marcos |
|---|---|---|---|---|
| ams-nist-cis-vpc- -puertos autorizados sg-open-only-to | VPC | Config changes | Informe | CIS: CIS.11, CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.1,1.3.2,2.2.2; |
| ams-nist-vpc-vpn-2 túneles hacia arriba | VPC | Config changes | Informe | CIS: NA; NIST-CSF: ID.BE-5, PR.DS-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i); PCI: NA; |
| ams-cis-ec2-ebs-encryption-by-default | EC2 | Periódico | Informe | CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (2) (iv), 164.312 (e) (2) (ii); PCI: 2.2, 3.4, 8.2.1; |
| ams-cis-rds-snapshot-encriptado | RDS | Config changes | Informe | CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4, 8.2.1; |
| ams-cis-redshift-cluster-comprobación de la configuración de mantenimiento | RedShift | Config changes | Informe | CIS: CIS.5; NIST-CSF: PR.DS-4, PR.IP-1, PR.IP-4; HIPAA: 164.308 (a) (5) (ii) (A), 164.308 (a) (7) (ii) (A); PCI: 6.2; |

# Respuestas a las infracciones en Accelerate

Todas las infracciones de las reglas de Config aparecen en el informe de configuración. Se trata de una respuesta universal. Según la categoría de remediación (gravedad) de la regla, AMS podría tomar medidas adicionales, que se resumen en la siguiente tabla. Para obtener más información sobre cómo personalizar el código de acción para determinadas reglas, consulteRespuestas a los hallazgos personalizados.

Acciones de remediación

| Código de acción | Acciones de AMS |
| --- | --- |
| Informe | 1. Agregar al informe de configuración |
| Incidente | 1. Agregar al informe de configuración<br>2. Informe automático de incidentes en Accelerate |
| Remediar | 1. Agregar al informe de configuración<br>2. Informe automático de incidentes en Accelerate<br>3. Corrección automática en Accelerate |

¿Solicitar ayuda adicional

> **Note**
>
> AMS puede subsanar cualquier infracción por usted, independientemente de su categoría de remediación. Para solicitar ayuda, envíe una solicitud de servicio e indique qué recursos desea que AMS corrija con un comentario como: «Como parte de la corrección de la regla de configuración de AMS, corrija el *RESOURCE_ARNS_OR_IDs* recurso ARNs/IDs>, la regla de configuración de la cuenta que no cumple los requisitos» y añada las entradas necesarias para subsanar la infracción. *CONFIG_RULE_NAME*

AMS Accelerate cuenta con una biblioteca de documentos y manuales de AWS Systems Manager automatización para ayudar a corregir los recursos no conformes.

## Agregar al informe de configuración

AMS genera un informe de configuración que rastrea el estado de cumplimiento de todas las reglas y recursos de su cuenta. Puede solicitar el informe a su CSDM. También puede revisar el estado de conformidad desde la consola de AWS Config, la AWS CLI o la API de AWS Config. Su informe de configuración incluye:

- Los principales recursos de su entorno, que no cumplen con las normas, para descubrir posibles amenazas y errores de configuración
- Cumplimiento de los recursos y las reglas de configuración a lo largo del tiempo
- Config las descripciones de las reglas, la severidad de las reglas y los pasos de corrección recomendados para corregir los recursos no conformes

Cuando un recurso pasa a un estado no compatible, el estado del recurso (y el estado de la regla) pasa a ser No compatible en tu informe de configuración. Si la regla pertenece a la categoría de corrección Config Report Only, de forma predeterminada, AMS no realiza ninguna otra acción. Siempre puede crear una solicitud de servicio para solicitar ayuda o remediación adicional a AMS.

Para obtener más información, consulte AWS Config Reporting.

## Informe automático de incidentes en Accelerate

En el caso de infracciones moderadamente graves de las normas, AMS crea automáticamente un informe de incidentes para notificarle que un recurso ha dejado de cumplir las normas y le pregunta qué medidas le gustaría llevar a cabo. Dispones de las siguientes opciones a la hora de responder a un incidente:

- Solicite que AMS corrija los recursos no conformes enumerados en el incidente. A continuación, intentamos subsanar el recurso que no cumple con las normas y se lo notificamos una vez que se haya resuelto el incidente subyacente.
- Puede resolver el problema de forma manual en la consola o mediante su sistema de despliegue automatizado (por ejemplo, mediante las actualizaciones de plantillas de CI/CD Pipeline). A continuación, puede resolver el incidente. El recurso no conforme se vuelve a evaluar según el cronograma de la regla y, si el recurso se evalúa como no conforme, se crea un nuevo informe de incidente.
- Puede optar por no resolver el recurso no conforme y simplemente resolver el incidente. Si actualiza la configuración del recurso más adelante, AWS Config activará una reevaluación y se le volverá a alertar para evaluar la no conformidad de ese recurso.

### Corrección automática en Accelerate

Las reglas más críticas pertenecen a la categoría Auto Remediate. El incumplimiento de estas normas puede afectar gravemente a la seguridad y la disponibilidad de sus cuentas. Cuando un recurso infringe una de estas reglas:

1. AMS le notifica automáticamente con un informe de incidente.
2. AMS inicia una reparación automática utilizando nuestros documentos SSM automatizados.
3. AMS actualiza el informe de incidentes con el éxito o el fracaso de la remediación automática.
4. Si la solución automática no funciona, un ingeniero de AMS investiga el problema.

## Crear excepciones a las reglas en Accelerate

La función Reglas de AWS Config de excepción de recursos le permite suprimir la notificación de recursos específicos que no cumplen con las normas para una regla específica.

> **Note**
>
> Los recursos exentos siguen apareciendo como No conformes en la consola de AWS Config Service. Los recursos exentos aparecen con una marca especial en Config Reports (Resource_Exception:TRUE). CSDMs Puedes filtrar esos recursos según esa columna al generar informes.

Si tienes recursos que sabes que no cumplen con los requisitos, puedes eliminar un recurso específico para una regla de configuración específica en sus informes de configuración. Para ello:

Envía una solicitud de servicio a Accelerate relacionada con tu cuenta, junto con una lista de las reglas de configuración y los recursos que quieres eximir del informe. Debe proporcionar una justificación empresarial explícita (por ejemplo, no es necesario que lo *`resource_name_1`* denuncie y no *`resource_name_2`* tenga copias de seguridad porque no queremos que se haga una copia de seguridad). Para obtener ayuda para enviar una solicitud de servicio de Accelerate, consulteCrear una solicitud de servicio en Accelerate.

Pegue en la solicitud las siguientes entradas (para cada recurso añada un bloque independiente con todos los campos obligatorios, como se muestra) y, a continuación, envíelas:

```
[
```

```
    {
        "resource_name": "resource_name_1",
        "config_rule_name": "config_rule_name_1",
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    },
    {
        "resource_name": "resource_name_2",
        "config_rule_name": "config_rule_name_2",
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    }
]
```

## Reduzca AWS Config los costos en Accelerate

Puede reducir los costes de AWS Config si utiliza la opción de registrar periódicamente el tipo de `AWS::EC2::Instance` recurso. El registro periódico captura los últimos cambios de configuración de sus recursos una vez cada 24 horas, lo que reduce la cantidad de cambios realizados. Cuando está habilitada, AWS Config solo registra la configuración más reciente de un recurso al final de un período de 24 horas. Esto le permite adaptar los datos de configuración a casos de uso específicos de planificación operativa, cumplimiento y auditoría que no requieren una supervisión continua. Este cambio solo se recomienda si tiene aplicaciones que dependen de arquitecturas efímeras, lo que significa que aumenta o reduce constantemente el número de instancias.

Para optar por el registro periódico para este tipo de `AWS::EC2::Instance` recurso, póngase en contacto con su equipo de entrega de AMS.

## Respuestas a los hallazgos personalizados

Puede elegir cómo quiere que AMS Accelerate responda a algunos hallazgos (reglas de Config no compatibles). Puede configurar AMS para que responda a las constataciones, corrigiéndolas, pidiéndole su aprobación para subsanarlas o simplemente informándole en su próxima revisión empresarial mensual (MBR). Puede cambiar las respuestas predeterminadas de las reglas de AMS Accelerate Config. Para ver las reglas, vaya a Configuración y cumplimiento > Tabla de reglas o descargue la tabla de reglas como un archivo ZIP ams_config_rules.zip.

Cambiar las respuestas predeterminadas te ayuda a aumentar el estado de seguridad y conformidad de tu cuenta, ya que permite corregir más errores. Al corregir más hallazgos, habrá menos casos que deban esperar a ser revisados y aprobados manualmente. La amplia biblioteca de manuales de

corrección de AMS corrige constantemente los recursos que no cumplen con las normas y solo nos pondremos en contacto con usted cuando sea necesario.

Las respuestas personalizadas solo se utilizan con recursos nuevos o con los recursos existentes con eventos nuevos. Por ejemplo, un recurso que dejó de ser compatible tras un cambio. Esto se debe a que los recursos más antiguos suelen requerir una inspección más profunda antes de corregirlos y es más fácil aplicar la corrección de los recursos a medida que se crean o se modifican. Para solicitar que se corrija el hallazgo de cualquier recurso en cualquier momento, envíe una solicitud de servicio.

## Solicitar un cambio en las respuestas predeterminadas

Cloud Architects (CAs) trabajará con usted durante la incorporación para recopilar sus preferencias. CAsa continuación, configure la configuración inicial en los sistemas AMS internos. Una vez incorporado, cree una solicitud de servicio para solicitar actualizaciones de sus configuraciones. Puede solicitar actualizaciones de configuración tantas veces como sea necesario. Tenga en cuenta que Operations solo actualiza las configuraciones de la cuenta en la que se creó la solicitud de servicio. Si necesita actualizar varias cuentas al mismo tiempo, póngase en contacto con su arquitecto de nube. Su CA le pedirá que añada una solicitud de servicio a sus preferencias con fines de auditoría.

## Cambiar las respuestas predeterminadas para sus hallazgos y cuentas

Siempre necesitas una preferencia de respuesta para cada cuenta y hallazgo. AMS proporciona una respuesta predeterminada (consulte Cumplimiento de la configuración), por lo que esta configuración es opcional. Puede cambiar las respuestas predeterminadas de cada búsqueda por las siguientes opciones:

- Corregir: AMS corrige el hallazgo de forma manual o automática. AMS revisa la corrección y le avisa si falla.
- Solicitud de aprobación: AMS crea un caso saliente para notificarle el hallazgo. Utilice esta opción cuando desee revisar la constatación antes de aprobar su corrección o eximirla. A continuación, AMS ejecuta la acción que prefiera.
- Sin acción (solo informe): AMS no toma ninguna medida para corregir o agravar el hallazgo. Es posible que los resultados sigan apareciendo en la consola y que los informes se presenten durante ese tiempo. MBRs

> **Note**
>
> No puede cambiar la configuración de las reglas que AMS debe corregir. Por ejemplo, habilitar Amazon GuardDuty y VPC Flow Logs.

### Cambiar las respuestas predeterminadas por recursos

Puedes configurar aún más la respuesta a recursos específicos mediante etiquetas. Puedes usar tus etiquetas preexistentes o etiquetar recursos con Resource Tagger. Para obtener más información, consulteAcelere el etiquetador de recursos). La configuración de los recursos con etiquetas tiene prioridad sobre la acción predeterminada para la búsqueda. Cuando un recurso tiene varias etiquetas con diferentes configuraciones asociadas, AMS no puede ejecutar correcciones personalizadas. En su lugar, AMS le envía una solicitud de servicio saliente para informarle de la situación. Por ejemplo, para la búsqueda bucket-server-side-encryptionhabilitada para S3, puede:

- Cambie la respuesta para «remediar» los depósitos S3 no cifrados con el par clave-valor de la etiqueta «Regulated: True»
- Cambie la respuesta a «sin acción» cuando los buckets S3 no cifrados tengan las etiquetas «Regulado: falso», y
- Cambie la respuesta predeterminada de los buckets S3 no cifrados a «solicitar aprobación». Esto se aplica a todos los cubos de S3 que no tengan las etiquetas «Regulado: verdadero» o «Regulado: falso»

También puedes añadir la entrada necesaria para ejecutar una respuesta de búsqueda personalizada. Por ejemplo, para las correcciones que requieren una clave de cifrado, puede proporcionar su clave IDs a AMS. Puede cambiar los parámetros de entrada de los manuales de corrección, pero AMS no admite la integración con los manuales de ejecución personalizados. Para obtener una descripción de los manuales de corrección de AMS en el Config Report, consulte. AWS Config Informe de cumplimiento de controles

## Respuesta a incidentes en Accelerate

Al recibir una alerta, el equipo de AMS utiliza soluciones automatizadas y manuales para que los recursos vuelvan a estar en buen estado. Si la remediación no funciona, AMS inicia el proceso de gestión de incidentes para colaborar con su equipo. Puede cambiar las líneas base actualizando la configuración predeterminada en un archivo de configuración.

## Respuesta a incidentes e incorporación en AMS Accelerate

Durante la incorporación, AMS Accelerate suprime la creación automática de incidentes para sus recursos actuales que no cumplen con las normas; en su lugar, su administrador de prestación de servicios en la nube (CSDM) le proporciona un informe que contiene todas las normas y recursos de incumplimiento para que los revise. Una vez que haya identificado las reglas que desea que AMS corrija, cree una solicitud de servicio en la consola Soporte central en la que se indiquen dichas reglas y recursos. La siguiente plantilla de solicitud de servicio es un ejemplo de una solicitud de un cliente a AMS para corregir manualmente los recursos no conformes. Si AMS tiene más preguntas, colaboramos con usted en la solicitud de servicio para recopilar la información requerida.

```
Hello,
Please remediate the following resources for the Config Rule "ENCRYPTED_VOLUMES".
Resource List:
    "Vol-12345678"
    "Vol-87654312"
Thank you
```

Una vez finalizado el proceso de incorporación, AMS Accelerate crea automáticamente un incidente para cada recurso que no cumpla con las normas marcadas como incidente automático.

# Resiliencia en Accelerate

La infraestructura AWS global se basa en zonas de disponibilidad Regiones de AWS y en ellas. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y operar aplicaciones y bases de datos que conmuten automáticamente entre zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, son más tolerantes a errores y son más escalables que las infraestructuras tradicionales de centros de datos de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura AWS global.

Para obtener información sobre la gestión de la continuidad de AMS Accelerate, consulteGestión de la continuidad en AMS Accelerate.

# Control de seguridad para sistemas end-of-support operativos

Los sistemas operativos que estén fuera del período de soporte general de la EOS o del fabricante end-of-support del sistema operativo y que no reciban actualizaciones de seguridad corren un mayor riesgo de seguridad.

AWS ofrece algunos servicios para ayudar a gestionar el sistema operativo end-of-support. Para obtener información acerca de Windows end-of-support, consulte Programa de End-of-Support migración para Windows Server.

> **Note**
>
> Encontrará información adicional sobre este tema accediendo a los informes de AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact. Para acceder a AWS Artifact, puede ponerse en contacto con su CSDM para obtener instrucciones o ir a Introducción a AWS Artifact. Esta información no se incluye en esta guía del usuario porque contiene contenido de seguridad confidencial.

# Mejores prácticas de seguridad en Accelerate

AMS Accelerate utiliza paquetes de conformidad, que proporcionan un marco de cumplimiento de uso general diseñado para permitirle crear controles de seguridad, operativos o de optimización de costes mediante acciones gestionadas o personalizadas Reglas de AWS Config y correctivas. AWS Config Para obtener información sobre cómo configurar mejor estos paquetes de conformidad, consulte las mejores prácticas operativas para el CSF AWS Config del NIST y las mejores prácticas operativas para el CIS Top 20.

# Revisiones de seguridad de la solicitud de cambios

El proceso de revisión de las solicitudes de cambio de AWS Managed Services garantiza que AMS lleve a cabo una revisión de seguridad de los cambios solicitados a medida que se implementan en su nombre en su cuenta.

Estándares técnicos de AMS Acceleratedefina los criterios de seguridad, las configuraciones y los procesos mínimos para establecer la seguridad básica de sus cuentas. Cuando AMS implementa los cambios solicitados, seguimos estos estándares.

AMS evalúa todas las solicitudes de cambio en función de las normas técnicas de AMS. Cualquier cambio que pueda reducir el nivel de seguridad de tu cuenta al apartarse de los estándares técnicos pasa por un proceso de revisión de seguridad. Durante este proceso, AMS resalta el riesgo relevante y el responsable de la aprobación de riesgos lo revisa y aprueba para lograr un equilibrio entre las necesidades empresariales y de seguridad.

## Proceso de gestión de riesgos de seguridad del cliente

El proceso de gestión de riesgos para la seguridad del cliente (CSRM) de AMS Accelerate ayuda a identificar y comunicar claramente los riesgos a los propietarios adecuados. Este proceso minimiza los riesgos de seguridad en su entorno y reduce la sobrecarga operativa continua en caso de identificar los riesgos.

De forma predeterminada, cuando alguien de su organización solicita que AMS implemente un cambio en su entorno gestionado, AMS revisa el cambio para determinar si la solicitud no cumple los estándares técnicos, lo que podría alterar la postura de seguridad de su cuenta. Si existe un riesgo de seguridad alto o muy alto, el personal de seguridad autorizado acepta o rechaza la revisión del cambio. Los cambios solicitados también se evalúan para determinar si tienen efectos adversos en la capacidad de AMS para gestionar la cuenta. Si la revisión detecta posibles impactos adversos, AMS requerirá revisiones y aprobaciones adicionales.

### Riesgo: aceptación, validez y revisión

Las aceptaciones de riesgos son válidas durante un año a partir de la fecha de aprobación. Si al cabo de un año vuelve a surgir un escenario de riesgo previamente aceptado, la aceptación del riesgo debe revisarse y volver a aprobarse antes de poder aplicarse. Esta revisión anual garantiza que las decisiones sobre riesgos se mantengan alineadas con las normas técnicas actuales, los requisitos reglamentarios y la evolución del perfil de riesgo de su organización.

### Exclusión

Puede excluirse del flujo de trabajo basado en la aprobación en el proceso de CSRM en caso de riesgos altos o muy altos. Para cambiar la opción de CSRM para cuentas específicas, de la CSRM estándar a la de solo notificación, colabore con sus gerentes de prestación de servicios en la nube para crear una aceptación única del riesgo. Si opta por la opción de solo notificación, AMS implementará los cambios solicitados independientemente de la categoría de riesgo. AMS envía una notificación de riesgo a los responsables de la aprobación de riesgos autorizados en lugar de solicitar la aprobación antes de la implementación del cambio.

Hable con sus arquitectos de nube o gerentes de prestación de servicios en la nube para obtener más información sobre el proceso de CSRM de AMS, cómo cambiar la opción de CSRM predeterminada al incorporar nuevas cuentas de AMS o cómo actualizar las cuentas existentes.

> **Note**
>
> AMS recomienda encarecidamente que utilice la opción predeterminada de CSRM estándar en todas sus cuentas.

## Estándares técnicos de AMS Accelerate

Las siguientes son las categorías de estándares técnicos de Accelerate:

| ID | Categoría |
|---|---|
| AMS-STD-X002 | AWS Identity and Access Management |
| AMS-STD-X003 | Seguridad de la red |
| AMS-STD-X004 | Pruebas de penetración |
| AMS-STD-X005 | Amazon GuardDuty |
| AMS-STD-X007 | Registro |

## Controles estándar en AMS Accelerate

Los siguientes son los controles estándar de AMS:

AMS-STD-X002 - (IAM) AWS Identity and Access Management

| ID | Norma técnica |
|---|---|
| 1.0 | Duración del tiempo de espera |
| 1.1 | El tiempo de espera predeterminado de un usuario federado es de una hora y puede aumentarse hasta cuatro horas. |

| ID | Norma técnica |
| --- | --- |
| 1.2 | El tiempo de espera de la sesión RDP para Microsoft Windows Server está establecido en 15 minutos y se puede extender según el caso de uso. |
| 2.0 | AWS Uso de la cuenta raíz |
| 2.1 | Si se utiliza una cuenta raíz por cualquier motivo, Amazon GuardDuty debe estar configurado para generar los resultados pertinentes. |
| 2.2 | No se deben crear claves de acceso para la cuenta raíz. |
| 3.0 | Creación y modificación de usuarios |
| 3.1 | Se pueden crear IAM users/roles con acceso programático y permisos de solo lectura sin ninguna política de tiempo limitado. Sin embargo, no se permite el permiso para permitir la lectura de objetos (por ejemplo, S3:GetObject) en todos los depósitos de Amazon Simple Storage Service de la cuenta. |
| 3.1.1 | Se pueden crear usuarios humanos de IAM para el acceso a la consola y con permisos de solo lectura con la política de límite de tiempo (hasta 180 días), mientras que la política removal/renewal/extension de límite de tiempo determinado generará la notificación de riesgo. Sin embargo, no se permite el permiso para leer objetos (por ejemplo, S3:GetObject) en todos los depósitos de S3 de la cuenta. |

| ID | Norma técnica |
| --- | --- |
| 3.2 | No se deben crear usuarios y roles de IAM para el acceso programático y de consola con permisos que modifiquen la infraestructura (escritura y administración de permisos) en la cuenta del cliente sin una aceptación arriesgada. Existen excepciones para los permisos de escritura a nivel de objeto de S3, que se permiten sin riesgo de aceptación siempre que los segmentos específicos estén dentro del ámbito de aplicación y las operaciones de etiquetado en etiquetas no relacionadas con AMS. |
| 3.3 | En los servidores Microsoft Windows, solo se debe crear una cuenta de servicio gestionada por grupos de Microsoft (gMSA). |
| 4.0 | Políticas, acciones y APIs |
| 4.4 | Una política no debe proporcionar acceso al administrador con una declaración equivalente a «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*» sin riesgo de aceptación. |
| 4.6 | No se deben permitir las llamadas a la API contra las políticas clave de KMS para las claves de infraestructura de AMS en las políticas de IAM del cliente. |
| 4.8 | No se deben permitir acciones que cambien los registros DNS de la infraestructura de AMS en Amazon Route 53. |

| ID | Norma técnica |
| --- | --- |
| 4.9 | Los usuarios humanos de IAM con acceso a la consola creados después de seguir el debido proceso no deben tener ninguna política asociada directamente, excepto la política de confianza, el rol y la política de tiempo limitado. |
| 4.10 | Se pueden crear perfiles de instancias de Amazon EC2 con acceso de lectura a un secreto o espacio de nombres específico AWS Secrets Manager dentro de la misma cuenta. |
| 4.12 | La política de IAM no debe incluir ninguna acción que incluya la acción Permitir registros (DeleteLogGroup y registros) DeleteLogStream en cualquier grupo de CloudWatch registros de AMS Amazon. |
| 4.13 | No se deben permitir los permisos para crear claves multirregionales. |
| 4.14 | El acceso a los ARN de los buckets de S3 que aún no se han creado en las cuentas de los clientes se puede proporcionar restringiendo el acceso a los buckets a las cuentas de los clientes especificando el número de cuenta mediante la clave de condición S3 específica del servicio s3:. ResourceAccount |
| 4.15.1 | Puede ver, crear, enumerar y eliminar el acceso a su panel de control personalizado de S3 Storage Lens. |
| 4.16 | Se pueden conceder todos los permisos relacionados con SQL Workbench roles/users para trabajar en las bases de datos de Amazon Redshift. |

| ID | Norma técnica |
| --- | --- |
| 4.17 | Se puede conceder cualquier AWS CloudShel l permiso a los roles de los clientes como alternativa a la CLI. |
| 4.18 | Una función de IAM con el AWS servicio como principio de confianza también debe estar en línea con los estándares técnicos de la IAM. |
| 4.19 | Los roles vinculados a servicios (SLRs) no están sujetos a los estándares técnicos de AMS IAM, ya que los crea y mantiene el equipo de servicio de IAM. |
| 4.20 | La política de IAM no debería permitir la lectura de objetos (por ejemplo, S3:GetObject) en todos los depósitos de S3 de la cuenta. |
| 4.21 | Todos los permisos de IAM para el tipo de recurso «savingsplan» se pueden conceder a los clientes. |
| 4.22 | El ingeniero de AMS no puede copiar ni mover los datos de los clientes (archivos, objetos S3, bases de datos, etc.) manualmente en ninguno de los servicios de almacenamiento de datos como Amazon S3, Amazon Relational Database Service, Amazon DynamoDB, etc., ni en el sistema de archivos del sistema operativo . |
| 6.0 | Políticas de cuentas cruzadas |
| 6.1 | Se pueden configurar las funciones de IAM y las políticas de confianza entre las cuentas de AMS que pertenecen al mismo cliente según los registros de los clientes. |

| ID | Norma técnica |
| --- | --- |
| 6.2 | Las políticas de confianza de los roles de IAM entre cuentas AMS y no AMS deben configura rse únicamente si la cuenta ajena a AMS pertenece al mismo cliente de AMS (confirma ndo que están bajo la misma AWS Organizat ions cuenta o haciendo coincidir el dominio de correo electrónico con el nombre de la empresa del cliente). |
| 6.3 | Las políticas de confianza de las funciones de IAM entre las cuentas de AMS y las cuentas de terceros no deben configurarse sin correr el riesgo de aceptarlas. |
| 6.4 | Se pueden configurar políticas multicuentas para acceder a cualquier cuenta de AMS CMKs del mismo cliente gestionada por un cliente. |
| 6.5 | Se pueden configurar políticas multicuenta para acceder a cualquier clave de KMS de una cuenta que no sea de AMS mediante una cuenta de AMS. |
| 6.6 | No se deben permitir las políticas multicuen ta para acceder a cualquier clave de KMS de una cuenta de AMS por parte de una cuenta de terceros sin una aceptación arriesgada. |
| 6.6.1 | Las políticas multicuentas para acceder a cualquier clave de KMS de una cuenta de AMS desde una cuenta que no sea de AMS solo se pueden configurar si la cuenta que no es de AMS es propiedad del mismo cliente de AMS. |

| ID | Norma técnica |
| --- | --- |
| 6.7 | Se pueden configurar políticas multicuenta para acceder a cualquier dato o recurso del bucket de S3 donde se puedan almacenar datos (como Amazon RDS, Amazon DynamoDB o Amazon Redshift) entre cuentas de AMS del mismo cliente. |
| 6.8 | Se pueden configurar políticas multicuenta para acceder a cualquier dato o recurso del bucket de S3 donde se puedan almacenar datos (como Amazon RDS, Amazon DynamoDB o Amazon Redshift) en una cuenta que no sea de AMS desde una cuenta de AMS con acceso de solo lectura. |
| 6.9 | Las políticas multicuenta para acceder a cualquier dato o recurso del bucket de S3 donde se puedan almacenar datos (como Amazon RDS, Amazon DynamoDB o Amazon Redshift) con permisos de escritura de AMS a una cuenta que no sea de AMS (o de una cuenta que no sea de AMS a AMS) solo deben configurarse si la cuenta que no es de AMS es propiedad del mismo cliente de AMS (confirma ndo que está en la misma cuenta o haciendo coincidir el dominio de correo electrónico con AWS Organizations el nombre de la empresa del cliente). |

| ID | Norma técnica |
| --- | --- |
| 6,10 | Se pueden configurar políticas multicuenta para acceder a cualquier dato o recurso del bucket de S3 donde se puedan almacenar datos (como Amazon RDS, Amazon DynamoDB o Amazon Redshift) en una cuenta de terceros desde una cuenta de AMS con acceso de solo lectura. |
| 6.11 | Las políticas multicuenta para acceder a cualquier dato o recurso del bucket de S3 donde se puedan almacenar datos (como Amazon RDS, Amazon DynamoDB o Amazon Redshift) en una cuenta de terceros desde una cuenta de AMS con acceso de escritura no deben configurarse sin riesgo de aceptación. |
| 6.12 | Las políticas multicuentas de cuentas de terceros para acceder a un bucket de S3 de un cliente de AMS o a los recursos en los que se puedan almacenar datos (como Amazon RDS, Amazon DynamoDB o Amazon Redshift) no deben configurarse sin una aceptación arriesgada. |
| 7.0 | User Groups (Grupos de usuarios) |
| 7.1 | Se permiten los grupos de IAM con permisos de solo lectura y no mutativos. |
| 8.0 | Políticas basadas en recursos |
| 8.4 | Los recursos de la infraestructura de AMS deben protegerse de la administración por parte de identidades no autorizadas mediante la incorporación de políticas basadas en los recursos. |

| ID | Norma técnica |
| --- | --- |
| 8.2 | Los recursos del cliente deben configurarse con políticas basadas en los recursos con privilegios mínimos, a menos que el cliente especifique explícitamente una política diferente. |

AMS-STD-X003: Seguridad de red

El siguiente es el control estándar para el X003: Seguridad de red:

| ID | Norma técnica |
| --- | --- |
| | Redes |
| 1.0 | Reservado para el control futuro |
| 2.0 | Se permite la IP elástica en las instancias EC2 |
| 3.0 | Se debe utilizar el plano de control AMS y, por extensión, en el plano de datos, el TLS 1.2+. |
| 5.0 | Un grupo de seguridad no debe tener una fuente como 0.0.0.0/0 en la regla de entrada si no está conectado a un balanceador de cargas según la versión 9.0 |
| 6.0 | El depósito o los objetos de S3 no deben hacerse públicos sin riesgo de ser aceptados. |
| 7.0 | No se debe permitir el acceso a la administración de servidores en los puertos SSH/22 o SSH/2222 (no SFTP/2222), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/5900-5901 TS/CITRIX/1494 o 1604, LDAP/389 o 636 y RPC/135, NETBIOS/137-139 desde |

| ID | Norma técnica |
| --- | --- |
| | fuera de la VPC a través de grupos de seguridad. |
| 8.0 | No se debe permitir el acceso a la administr ación de bases de datos en los puertos (MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433) o en un puerto personalizado desde un puerto público que no esté enrutado a una VPC a través de DX, VPC-peer o una VPN a través de un grupo de seguridad. IPs |
| 8.1 | Cualquier recurso en el que se puedan almacenar los datos de los clientes no debe exponerse directamente a la Internet pública. |
| 9.0 | El acceso directo a las aplicaciones a través de los puertos HTTP/80, HTTPS/8443 y HTTPS/443 desde Internet solo está permitido a los balanceadores de carga, pero no a ningún recurso informático directamente, como instancias EC2, contenedores, etc. ECS/EKS/F argate |
| 10.0 | Se puede permitir el acceso de las aplicaciones a través de los puertos HTTP/80 y HTTPS/443 desde el rango de IP privadas del cliente. |
| 11.0 | No se debe permitir ningún cambio en los grupos de seguridad que controlan el acceso a la infraestructura de AMS sin asumir riesgos. |
| 12.0 | AMS Security hará referencia a los estándares cada vez que se solicite la incorporación de un grupo de seguridad a una instancia. |

| ID | Norma técnica |
| --- | --- |
| 14.0 | La asociación entre cuentas de zonas alojadas privadas VPCs desde una cuenta de AMS a una cuenta que no es de AMS (o que no es de AMS a una cuenta de AMS) solo debe configurarse si la cuenta que no es de AMS es propiedad del mismo cliente de AMS (confirma ndo que están bajo la misma cuenta de la organización de AWS o haciendo coincidir el dominio de correo electrónico con el nombre de la empresa del cliente) mediante herramientas internas. |
| 15.0 | Se pueden permitir las conexiones de emparejamiento de VPC entre cuentas que pertenecen al mismo cliente. |
| 16.0 | La base de AMS se AMIs puede compartir con cuentas ajenas a AMS siempre que ambas cuentas sean propiedad del mismo cliente (confirmando que están bajo la misma AWS Organizations cuenta o haciendo coincidir el dominio de correo electrónico con el nombre de la empresa del cliente) mediante herramientas internas. |
| 17.0 | El puerto FTP 21 no debe configurarse en ninguno de los grupos de seguridad sin una aceptación del riesgo. |
| 18.0 | Se permite la conectividad de red entre cuentas a través de Transit Gateway siempre que todas las cuentas sean propiedad del cliente. |
| 19.0 | No está permitido convertir una subred privada en pública |

| ID | Norma técnica |
| --- | --- |
| 20.0 | No se deben permitir las conexiones de emparejamiento de VPC con cuentas de terceros (que no sean propiedad del cliente). |
| 21.0 | No se debe permitir la conexión de Transit Gateway a una cuenta de terceros (que no sea propiedad del cliente). |
| 22.0 | El tráfico de red necesario para que AMS preste los servicios a los clientes no debe bloquearse en el punto de salida de la red del cliente. |
| 23.0 | La solicitud ICMP entrante a Amazon EC2 desde el cliente infra requerirá una notificación de riesgo. |
| 24,0 | Se permiten las solicitudes entrantes del público IPs enrutadas a Amazon VPC a través de DX, VPC-peer o VPN a través de un grupo de seguridad. |
| 25.0 | Las solicitudes entrantes del público que IPs no se enruten a Amazon VPC a través de DX, VPC-peer o VPN a través de un grupo de seguridad requerirían una aceptación de riesgo. |
| 26,0 | Se permiten solicitudes ICMP salientes desde Amazon EC2 a cualquier destino. |
| 27.0 | Uso compartido de grupos de seguridad |
| 27.1 | Si un grupo de seguridad cumple con este estándar de seguridad, se puede compartir entre cuentas VPCs de la misma cuenta y entre cuentas de la misma organización. |

| ID | Norma técnica |
| --- | --- |
| 27.2 | Si un grupo de seguridad no cumple con este estándar y anteriormente se requería la aceptación del riesgo para este grupo de seguridad, no se permite el uso de la función de uso compartido de grupos de seguridad entre la misma cuenta o entre cuentas de la misma organización sin la aceptación del riesgo para esa nueva VPC o cuenta. VPCs |

AMS-STD-X004: Pruebas de penetración

El siguiente es el control estándar para el X004: Pruebas de penetración

1. AMS no admite la infraestructura de pentest. Es responsabilidad del cliente. Por ejemplo, Kali no es una distribución de Linux compatible con AMS.
2. Los clientes deben cumplir con las pruebas de penetración.
3. En caso de que el cliente desee realizar pruebas de penetración de la infraestructura en las cuentas, se debe avisar previamente a AMS con 24 horas de antelación.
4. AMS proporcionará al cliente una infraestructura de pentesting según los requisitos del cliente que se especifiquen explícitamente en la solicitud de cambio o servicio presentada por el cliente.
5. La gestión de la identidad de la infraestructura de pentesting del cliente es responsabilidad del cliente.

AMS-STD-X005 - GuardDuty

El siguiente es el control estándar para el X005 - GuardDuty

1. GuardDuty debe estar activado en todas las cuentas de los clientes en todo momento.
2. GuardDuty las alertas deben almacenarse en la misma cuenta o en cualquier otra cuenta gestionada por la misma organización.
3. No se GuardDuty debe utilizar la función de lista de IP confiables de. En su lugar, se puede utilizar el archivado automático como alternativa, lo que resulta útil para fines de auditoría.

## AMS-STD-X007: Registro

El siguiente es el control estándar para el X007: Registro

| ID | Norma técnica |
|---|---|
| 1.0 | Tipos de registro |
| 1.1 | Registros del sistema operativo: todos los hosts deben registrar como mínimo los eventos de autenticación del host, los eventos de acceso para todos los usos de privilegios elevados y los eventos de acceso para todos los cambios en la configuración de acceso y privilegios, tanto si se realizan correctamente como si no. |
| 1.2 | AWS CloudTrail: el registro CloudTrail de eventos de administración debe estar habilitad o y configurado para enviar los registros a un bucket de S3. |
| 1.3 | Registros de flujo de VPC: todos los registros de tráfico de red deben registrarse mediante registros de flujo de VPC. |
| 1.4 | Registro de acceso al servidor Amazon S3: los buckets S3 obligatorios por AMS que almacenan registros deben tener habilitado el registro de acceso al servidor. |
| 1.5 | AWS Config Instantáneas: AWS Config deben registrar los cambios de configuración de todos los recursos compatibles en todas las regiones y entregar los archivos de instantáneas de configuración a los depósitos de S3 al menos una vez al día. |
| 1.7 | Registros de aplicaciones: los clientes pueden habilitar el inicio de sesión en sus aplicaciones |

| ID | Norma técnica |
| --- | --- |
| | y almacenarlos en un grupo de CloudWatch registros o en un depósito de S3. |
| 1.8 | Registro a nivel de objeto de S3: los clientes pueden habilitar el registro a nivel de objeto en sus depósitos de S3. |
| 1.9 | Registro de servicios: los clientes pueden habilitar y reenviar los registros de los servicios de SSPS como cualquier otro servicio principal. |
| 1.10 | Registros de Elastic Classic/Application Load Balancer/Network Load Balancing (Load Balancer): las entradas de los registros de acceso y errores deben almacenarse en los buckets S3 gestionados por AMS 2.0. |
| 2.0 | Control de acceso |
| 2.3 | Los depósitos S3 exigidos por AMS que almacenan registros no deben permitir el uso de cuentas de terceros como norma en las políticas de los depósitos. |
| 2.4 | Los registros de CloudWatch los grupos de registros de Logs no se deben eliminar sin la aprobación explícita del contacto de seguridad autorizado por el cliente. |
| 3.0 | Retención de registros |
| 3.1 | Los grupos de CloudWatch registros exigidos por AMS deben tener un período de retención mínimo de 90 días en los registros. |

| ID | Norma técnica |
| --- | --- |
| 3.2 | Los depósitos S3 exigidos por AMS que almacenan los registros deben tener un período de retención mínimo de 18 meses. |
| 3.3 | AWS Backup las instantáneas deberían estar disponibles con una retención mínima de 31 días en los recursos compatibles. |
| 4.0 | Cifrado |
| 4.1 | El cifrado debe estar habilitado en todos los depósitos de S3 que necesiten los equipos de AMS que almacenen los registros. |
| 4.2 | Cualquier reenvío de registros desde las cuentas de los clientes a cualquier otra cuenta debe estar cifrado. |
| 5.0 | Integridad |
| 5.1 | El mecanismo de integridad del archivo de registro debe estar activado. Eso significa configurar la «validación del archivo de registro» en las AWS CloudTrail rutas requeridas por los equipos de AMS. |
| 6.0 | Reenvío de registros |
| 6.1 | Cualquier registro se puede reenviar de una cuenta de AMS a otra cuenta de AMS del mismo cliente. |

| ID | Norma técnica |
| --- | --- |
| 6.2 | Cualquier registro puede reenviarse de AMS a una cuenta ajena a una cuenta ajena a AMS únicamente si la cuenta que no es de AMS pertenece al mismo cliente de AMS (confirma ndo que tiene la misma AWS Organizations cuenta o haciendo coincidir el dominio del correo electrónico con el nombre de la empresa del cliente y la cuenta vinculada al PAGADOR) mediante herramientas internas. |

## Cambios que introduzcan riesgos de seguridad altos o muy altos en su entorno

Los siguientes cambios introducen un riesgo de seguridad alto o muy alto en su entorno:

AWS Identity and Access Management

- High_risk-IAM-001: Cree claves de acceso para la cuenta raíz
- High_risk-IAM-002: modificación de la política de SCP para permitir un acceso adicional
- High_risk-IAM-003: modificación de la política de SCP que podría dañar la infraestructura de AMS
- High_Risk-IAM-004: Creación de una cuenta de cliente role/user con permisos variables en la infraestructura (escritura, gestión de permisos o etiquetado)
- High_Risk-IAM-005: IAM aplica políticas de confianza entre las cuentas AMS y las cuentas de terceros (que no son propiedad del cliente)
- High_risk-IAM-006: políticas multicuenta para acceder a cualquier clave de KMS desde una cuenta de AMS (desde una cuenta de terceros)
- High_risk-IAM-007: políticas multicuenta de cuentas de terceros para acceder a un bucket de S3 de un cliente de AMS o a recursos donde se puedan almacenar datos (como Amazon RDS, Amazon DynamoDB o Amazon Redshift)
- High_Risk-IAM-008: asigne los permisos de IAM a cualquier infraestructura que modifique el permiso de la cuenta del cliente
- High_risk-IAM-009: Permite publicar y leer todos los depósitos de S3 de la cuenta

Seguridad de la red

- High_RISK-NET-001: Abra los puertos de administración del sistema operativo SSH/22 o SSH/2222 (no SFTP/2222), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/ 5900-5901 TS/ CITRIX/1494 o 1604, LDAP/389 o 636 y NETBIOS/137-139 desde Internet
- High_risk-net-002: Abra los puertos de administración de bases de datos MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433 o cualquier puerto de administración de clientes desde Internet
- High_risk-net-003: abra los puertos de aplicaciones HTTP/80, HTTPS/8443 y HTTPS/443 directamente en cualquier recurso informático. Por ejemplo, instancias, contenedores, etc. desde Internet EC2 ECS/EKS/Fargate
- High_Risk-Net-004: cualquier cambio en los grupos de seguridad que controlan el acceso a la infraestructura AMS
- High_risk-net-006: interconexión de VPC con la cuenta de terceros (que no es propiedad del cliente)
- High_risk-net-007: Se ha añadido el firewall del cliente como punto de salida para todo el tráfico de AMS
- High_risk-net-008: No se permite adjuntar archivos adjuntos a Transit Gateway a la cuenta de terceros
- High_Risk-S3-001: Aprovisiona o habilita el acceso público en el bucket S3

Registro

- CloudTrailHigh_risk-log-001: Desactivar.
- High_risk-log-002: deshabilita los registros de flujo de la VPC.
- High_risk-log-003: Se reenvían los registros mediante cualquier método (notificación de eventos S3, extracción mediante un agente SIEM, inserción mediante un agente SIEM, etc.) desde una cuenta gestionada por AMS a una cuenta de terceros (que no es propiedad del cliente)
- High_risk-log-004: Utilice un registro que no sea de AMS para CloudTrail

Misceláneo

- High_risk-enc-001: deshabilita el cifrado en cualquier recurso si está activado

# Preguntas frecuentes sobre seguridad

AMS proporciona follow-the-sun asistencia las 24 horas, los 7 días de la semana, los 365 días del año a través de centros Los ingenieros de operaciones especializados de AMS supervisan activamente los cuadros de mando y las colas de incidentes. Por lo general, AMS gestiona sus cuentas mediante la automatización. En raras circunstancias que requieran experiencia específica en resolución de problemas o implementación, un ingeniero de operaciones de AMS podría acceder a sus AWS cuentas.

Las siguientes son preguntas frecuentes sobre las mejores prácticas de seguridad, los controles, los modelos de acceso y los mecanismos de auditoría que AMS Accelerate utiliza cuando un ingeniero de operaciones o un sistema de automatización de AMS accede a sus cuentas.

## ¿Cuándo acceden los ingenieros de operaciones de AMS a mis entornos?

Los ingenieros de operaciones de AMS no tienen acceso permanente a sus cuentas o instancias. El acceso a las cuentas de los clientes se concede a los operadores de AMS solo en casos de uso empresarial justificables, como alertas, incidentes, solicitudes de cambio, etc. El acceso se documenta en AWS CloudTrail los registros.

Para obtener información sobre la justificación del acceso, los activadores y los iniciadores de los activadores, consulteActivadores de acceso a la cuenta de cliente de AMS.

## ¿Qué funciones asumen los ingenieros de operaciones de AMS cuando acceden a mis cuentas?

En los raros casos (aproximadamente un 5%) que requieren la intervención humana en su entorno, los ingenieros de operaciones de AMS inician sesión en su cuenta con un rol de acceso predeterminado de solo lectura. El rol predeterminado no tiene acceso a ningún contenido que se almacene habitualmente en almacenes de datos, como Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift y Amazon. ElastiCache

Para obtener una lista de las funciones que los ingenieros de operaciones y sistemas de AMS necesitan para prestar servicios en su cuenta, consulte. Funciones de IAM para el acceso a la cuenta de los clientes de AMS

## ¿Cómo accede un ingeniero de operaciones de AMS a mi cuenta?

Para acceder a las cuentas de los clientes, los ingenieros de operaciones de AMS utilizan un servicio de acceso AWS interno a AMS. Este servicio interno solo está disponible a través de un canal privado y seguro para que el acceso a sus cuentas sea seguro y esté auditado.

1. Los ingenieros de operaciones de AMS utilizan la autenticación interna del servicio de acceso AMS junto con una autenticación de dos factores. Además, el ingeniero de operaciones debe proporcionar una justificación empresarial (ticket de incidente o identificador de solicitud de servicio) en la que se describa la necesidad de acceder a su AWS cuenta.
2. En función de la autorización del ingeniero de operaciones, el servicio de acceso a AMS proporciona al ingeniero la función adecuada (lecturaonly/Operator/Admin) y la URL de inicio de sesión en la AWS consola. El acceso a su cuenta es de corta duración y tiene un límite de tiempo.
3. Para acceder a las instancias de Amazon EC2, los ingenieros de operaciones de AMS utilizan el mismo servicio de acceso interno a AMS que el intermediario. Una vez concedido el acceso, los ingenieros de operaciones de AMS suelen acceder AWS Systems Manager Session Manager a las instancias con credenciales de sesión de corta duración.

   Para proporcionar acceso RDP a las instancias de Windows, el ingeniero de operaciones utiliza Amazon EC2 Systems Manager para crear un usuario local en la instancia y establecer el reenvío de puertos a la instancia. El ingeniero de operaciones utiliza las credenciales de usuario local para el acceso RDP a la instancia. Las credenciales del usuario local se eliminan al final de la sesión.

El siguiente diagrama describe el proceso utilizado por los ingenieros de operaciones de AMS para acceder a su cuenta:

## ¿Cómo hago un seguimiento de los cambios realizados por AMS en mis AWS cuentas gestionadas por AMS?

Acceso a la cuenta

Para ayudarlo a realizar un seguimiento de los cambios realizados por la automatización o por el equipo de operaciones de AMS Accelerate, AMS proporciona la interfaz SQL de registros de cambios

en la consola de Amazon Athena y los registros de AMS Accelerate. Estos recursos proporcionan la siguiente información:

- Quién accedió a tu cuenta.
- Cuándo se accedió a la cuenta.
- Qué privilegios se utilizaron para acceder a su cuenta.
- Qué cambios realizó AMS Accelerate en su cuenta.
- Por qué se realizaron los cambios en su cuenta.

Configuración de recursos

Consulte CloudTrail los registros para realizar un seguimiento de las configuraciones de sus AWS recursos durante los últimos 90 días. Si su configuración tiene más de 90 días, acceda a los registros en Amazon S3.

Registros de instancias

El Amazon CloudWatch Agent recopila los registros del sistema operativo. Consulte los CloudWatch registros para ver los registros de inicio de sesión y otros registros de acciones compatibles con su sistema operativo.

Para obtener más información, consulte Seguimiento de los cambios en sus cuentas de AMS Accelerate.

## ¿Cuáles son los controles de proceso para que el ingeniero de operaciones de AMS acceda a mi cuenta?

Antes de unirse a AMS, los ingenieros de operaciones pasan por una verificación de antecedentes penales. Como los ingenieros de AMS administran la infraestructura de los clientes, también tienen una verificación de antecedentes anual obligatoria. Si un ingeniero no pasa la verificación de antecedentes, se revoca el acceso.

Todos los ingenieros de operaciones de AMS deben completar una formación obligatoria en materia de seguridad, como la seguridad de la infraestructura, la seguridad de los datos y la respuesta a incidentes antes de que se les conceda acceso a los recursos.

## ¿Cómo se gestiona el acceso privilegiado?

Un subconjunto de usuarios debe completar una formación adicional y mantener los derechos de acceso privilegiados para un acceso elevado. El acceso y el uso se inspeccionan y auditan. AMS limita el acceso privilegiado a circunstancias excepcionales o cuando el acceso con privilegios mínimos no puede satisfacer su solicitud. El acceso privilegiado también tiene un límite de tiempo.

## ¿Los ingenieros de operaciones de AMS utilizan MFA?

Sí. Todos los usuarios deben usar MFA y Proof of Presence para prestarle servicios.

## ¿Qué ocurre con su acceso cuando un empleado de AMS deja la organización o cambia de puesto?

El acceso a las cuentas y los recursos de los clientes se proporciona mediante la pertenencia a grupos internos. La membresía se basa en criterios estrictos, como el puesto de trabajo específico, el responsable jerárquico y la situación laboral en AMS. Si la familia laboral de un ingeniero de operaciones cambia o su seudónimo está deshabilitado, se revoca el acceso.

## ¿Qué controles de acceso regulan el acceso de los ingenieros de operaciones de AMS a mis cuentas?

Existen varios niveles de controles técnicos para hacer cumplir los principios de «necesidad de información» y «privilegio mínimo» para el acceso a su entorno. La siguiente es una lista de los controles de acceso:

- Todos los ingenieros de operaciones deben formar parte de un AWS grupo interno específico para acceder a las cuentas y los recursos de los clientes. La pertenencia a un grupo se basa estrictamente en la necesidad de conocimiento y se automatiza con criterios predefinidos.
- AMS practica el acceso «no persistente» a su entorno. Esto significa que las operaciones de AMS acceden a sus AWS cuentas «just-in-time» con credenciales de corta duración. El acceso a sus cuentas solo se proporciona después de que se haya presentado y revisado una justificación interna del caso empresarial (solicitud de servicio, incidente, solicitud de gestión de cambios, etc.).
- AMS sigue el principio del mínimo privilegio. Por lo tanto, los ingenieros de operaciones autorizados asumen el acceso de solo lectura de forma predeterminada. Los ingenieros solo utilizan el acceso de escritura cuando es necesario realizar cambios en el entorno debido a un incidente o a una solicitud de cambio.

- AMS utiliza AWS Identity and Access Management funciones estándar y fácilmente identificables que utilizan el prefijo «ams» para supervisar y gestionar sus cuentas. Todos los accesos están registrados AWS CloudTrail para que puedas auditarlos.
- AMS utiliza herramientas de back-end automatizadas para detectar los cambios no autorizados en su cuenta durante la fase de validación de la información del cliente tras la ejecución de los cambios.

## ¿Cómo monitorea AMS el acceso de los usuarios root?

El acceso root siempre activa el proceso de respuesta a los incidentes. AMS usa la GuardDuty detección de Amazon para monitorear la actividad de los usuarios root. Si GuardDuty genera una alerta, AMS crea un evento para una investigación más profunda. AMS le notifica si se detecta una actividad inesperada en la cuenta raíz y el equipo de seguridad de AMS inicia una investigación.

## ¿Cómo responde AMS a los incidentes de seguridad?

AMS investiga los eventos de seguridad que se generan a partir de servicios de detección como Amazon o Amazon GuardDuty Macie y a partir de problemas de seguridad informados por los clientes. AMS colabora con su equipo de respuesta de seguridad para ejecutar el proceso de respuesta a incidentes de seguridad (SIR). El proceso SIR de AMS se basa en el marco de la guía de gestión de incidentes de seguridad informática de la NIST SP 800-61 Rev. 2, y proporciona una respuesta de seguridad 24 horas al día, 7 días a la semana, 365 días al año. follow-the-sun AMS trabaja con usted para analizar y contener rápidamente los incidentes de seguridad.

## ¿A qué marcos y certificaciones estándares del sector se adhiere AMS?

Al igual que otros AWS servicios, AWS Managed Services cuenta con la certificación OSPAR, HIPAA, HITRUST, GDPR, SOC*, ISO*, FedRAMP (Medium/High), IRAP y PCI. Para obtener más información sobre las certificaciones, los reglamentos y los marcos de conformidad de los clientes a los que AWS se ajusta, consulte AWS Compliance.

Barandillas de seguridad

AWS Managed Services utiliza varios controles para proteger sus activos de información y ayudarle a mantener segura su AWS infraestructura. AMS Accelerate mantiene una biblioteca de AWS Config normas y medidas correctivas para ayudarle a garantizar que sus cuentas cumplen con los estándares del sector en materia de seguridad e integridad operativa. AWS Config las reglas

realizan un seguimiento continuo de los cambios en la configuración de los recursos registrados. Si un cambio infringe las condiciones de una regla, AMS le informará de sus conclusiones. Puede subsanar las infracciones automáticamente o mediante solicitud, en función de la gravedad de la infracción.

AMS utiliza AWS Config reglas para ayudar a cumplir los requisitos de las siguientes normas:

- Center for Internet Security (CIS)
- Marco de seguridad en la nube (CSF) del Instituto Nacional de Estándares y Tecnología (NIST)
- Ley de Portabilidad y Responsabilidad de Seguros Médicos de EE. UU (Health Insurance Portability and Accountability Act, HIPAA).
- Estándar de seguridad de datos (DSS) de la industria de tarjetas de pago (PCI)

Para obtener más información, consulte Gestión de la seguridad en AMS Accelerate

## ¿Cómo puedo acceder a los informes más recientes sobre la certificación, los marcos y el cumplimiento de la seguridad? AWS

Puede encontrar los informes de seguridad y conformidad actuales de AWS los servicios mediante los siguientes métodos:

- Puede utilizarlos AWS Artifactpara descargar el informe más reciente sobre la seguridad, la disponibilidad y la confidencialidad de un AWS servicio.
- Para obtener una lista de la mayoría de AWS los servicios, incluidos AWS Managed Services, que cumplen con los marcos de conformidad globales, consultehttps://aws.amazon.com/compliance/services-in-scope/. Por ejemplo, seleccione PCI y busque AWS Managed Services.

  Puede buscar «AMS» para encontrar artefactos de seguridad específicos de AMS en una AWS cuenta gestionada por AMS. AWS Managed Services está dentro del ámbito de aplicación del SOC 3.
- El informe AWS SOC 2 (System and Organizations Controls) se publica en el AWS Artifact repositorio. Este informe evalúa los AWS controles que cumplen los criterios de seguridad, disponibilidad y confidencialidad establecidos en la sección 100 del TSP del Instituto Estadounidense de Contadores Públicos Certificados (AICPA), titulada «Criterios de servicios de confianza».

## ¿Comparte AMS diagramas de arquitectura de referencia sobre los distintos aspectos de las funciones de AMS?

Para ver la arquitectura de referencia de AMS, descargue el PDF AWS Managed Services for Proactive Monitoring.

## ¿Cómo controla AMS quién accede a mis cuentas y qué necesita la empresa para acceder a ellas?

Para garantizar la continuidad del servicio y la seguridad de sus cuentas, AMS accede a su cuenta o a sus instancias únicamente en respuesta a problemas proactivos de salud o mantenimiento, eventos relacionados con el estado o la seguridad, actividades planificadas o solicitudes de los clientes. El acceso a sus cuentas está autorizado mediante los procesos de AMS, tal como se describe en el modelo de acceso de AMS Accelerate. Estos flujos de autorización contienen barreras de protección para evitar el acceso inadvertido o inapropiado. Como parte del flujo de acceso, AMS suministra el sistema de autorización para una necesidad empresarial. Esta necesidad empresarial puede ser un elemento de trabajo asociado a su cuenta, como un caso que haya abierto en AMS. O bien, la necesidad empresarial puede ser un flujo de trabajo autorizado, como la solución de parches. Todos los accesos requieren una justificación que los sistemas AMS internos validen, verifiquen y autoricen en tiempo real y se basen en normas empresariales para adaptar las solicitudes de acceso a las necesidades de la empresa.

Los ingenieros de operaciones de AMS no disponen de una forma de acceder a tus cuentas sin requisitos empresariales válidos. Todos los accesos a las cuentas y las necesidades empresariales asociadas se registran en las AWS CloudTrail entradas de sus AWS cuentas. Esto proporciona una transparencia total y la oportunidad de realizar su propia auditoría e inspección. Además de su inspección, AMS tiene inspecciones automatizadas y realiza inspecciones manuales, según sea necesario, de las solicitudes de acceso, y audita las herramientas y el acceso humano para revisar los accesos anómalos.

## ¿Los ingenieros de AMS tienen acceso a mis datos almacenados en un servicio de almacenamiento de AWS datos, como Amazon S3, Amazon RDS, DynamoDB y Amazon Redshift?

Los ingenieros de AMS no tienen acceso al contenido de los clientes almacenado en AWS los servicios que se utilizan habitualmente para el almacenamiento de datos. El acceso a los datos

AWS APIs utilizados para leer, escribir, modificar o eliminar datos en estos servicios está restringido por una política explícita de denegación de IAM asociada a las funciones de IAM utilizadas para el acceso de los ingenieros de AMS. Además, las barandillas internas y las automatizaciones de AMS impiden que los ingenieros de operaciones de AMS eliminen o modifiquen las condiciones de denegación.

## ¿Los ingenieros de AMS tienen acceso a los datos de los clientes almacenados en Amazon EBS, Amazon EFS y Amazon FSx?

Los ingenieros de AMS pueden iniciar sesión en las instancias de Amazon EC2 como administradores. El acceso de administrador es necesario para solucionar algunos casos, entre los que se incluyen, entre otros, los problemas del sistema operativo (SO) y los errores de los parches. Los ingenieros de AMS suelen acceder al volumen del sistema para solucionar los problemas detectados. Sin embargo, el acceso de los ingenieros de AMS no está limitado ni restringido al volumen del sistema.

## ¿Cómo se restringe o controla el acceso a los puestos de automatización que tienen altos privilegios en mis entornos?

El `ams-access-admin` rol lo utiliza exclusivamente AMS Automation. Estas automatizaciones implementan, administran y mantienen los recursos necesarios que AMS utiliza para implementarlos en sus entornos para la recopilación de datos de telemetría, estado y seguridad a fin de realizar funciones operativas. Los ingenieros de AMS no pueden asumir funciones de automatización y están restringidos por la asignación de funciones en los sistemas internos. En tiempo de ejecución, AMS aplica de forma dinámica una política de sesión con privilegios mínimos restringida a cada automatización. Esta política de sesión limita la capacidad y los permisos de la automatización.

## ¿Cómo implementa AMS el principio del mínimo privilegio tal como se propugna en el AWS Well-Architected Framework para las funciones de automatización?

En tiempo de ejecución, AMS aplica una política de sesión limitada y con privilegios mínimos a cada automatización. Esta política de sesión restringida limita la capacidad y los permisos de la automatización. Las políticas de sesión que tienen permisos para crear recursos de IAM también tienen el requisito de adjuntar un límite de permisos. Este límite de permisos reduce el riesgo de escalada de privilegios. Cada equipo incorpora una política de sesión que solo utiliza ese equipo.

## ¿Qué sistemas de registro y supervisión se utilizan para detectar intentos de acceso no autorizados o actividades sospechosas relacionadas con funciones de automatización?

AWS mantiene repositorios centralizados que proporcionan una funcionalidad básica de archivo de registros para uso interno de los equipos de AWS servicio. Estos registros se almacenan en Amazon S3 para ofrecer una alta escalabilidad, durabilidad y disponibilidad. AWS Luego, los equipos de servicio pueden recopilar, archivar y ver los registros de servicio en un servicio de registro central.

Los hosts de producción AWS se implementan mediante imágenes de referencia maestras. Las imágenes de referencia están equipadas con un conjunto estándar de configuraciones y funciones que incluyen el registro y la supervisión por motivos de seguridad. Los equipos de AWS seguridad almacenan estos registros y pueden acceder a ellos para analizar la causa raíz en caso de que se sospeche que se ha producido un incidente de seguridad.

Los registros de un anfitrión determinado están disponibles para el equipo propietario de ese anfitrión. Los equipos pueden buscar en sus registros un análisis operativo y de seguridad.

## ¿Cómo se gestionan los incidentes o brechas de seguridad relacionados con la infraestructura de automatización y qué protocolos ayudan a responder y mitigar con rapidez?

AWS Los planes de contingencia y los manuales de respuesta a incidentes han definido y probado herramientas y procesos para detectar, mitigar, investigar y evaluar los incidentes de seguridad. Estos planes y manuales incluyen directrices para responder a posibles violaciones de datos de conformidad con los requisitos contractuales y reglamentarios.

## ¿Se realizan periódicamente evaluaciones de seguridad, análisis de vulnerabilidades y pruebas de penetración en la infraestructura de automatización?

AWS El departamento de seguridad realiza análisis de vulnerabilidades periódicos en los sistemas operativos, las aplicaciones web y las bases de datos del AWS entorno host mediante una variedad de herramientas. AWS Los equipos de seguridad también se suscriben a las fuentes de noticias para detectar las posibles averías de los proveedores y supervisan de forma proactiva los sitios web de los proveedores y otros medios relevantes para detectar nuevos parches.

## ¿Cómo se restringe el acceso a la infraestructura de automatización únicamente al personal autorizado?

El acceso a AWS los sistemas se asigna en función del mínimo privilegio y lo aprueba una persona autorizada. Las funciones y áreas de responsabilidad (por ejemplo, la solicitud y aprobación del acceso, la solicitud y aprobación de la gestión de cambios, el desarrollo, las pruebas y el despliegue, etc.) están segregados entre diferentes personas para reducir la modificación no autorizada o involuntaria o el uso indebido de los sistemas. AWS No se permiten cuentas grupales o compartidas dentro de los límites del sistema.

## ¿Qué medidas se implementan para mantener los estándares de seguridad y evitar el acceso no autorizado o las filtraciones de datos en el proceso de automatización?

El propietario o administrador correspondiente aprueba el acceso a los recursos, incluidos los servicios, los hosts, los dispositivos de red y los grupos de Windows y UNIX, mediante el sistema de administración de permisos AWS patentado. El registro de la herramienta de administración de permisos captura las solicitudes de cambios de acceso. Los cambios en las funciones de trabajo revocan automáticamente el acceso del empleado a los recursos. Se debe solicitar y aprobar el acceso continuo de ese empleado.

AWS requiere una autenticación de dos factores a través de un canal criptográfico aprobado para la autenticación en la AWS red interna desde ubicaciones remotas. Los dispositivos de firewall restringen el acceso al entorno informático, refuerzan los límites de los clústeres informáticos y restringen el acceso a las redes de producción.

Los procesos se implementan para proteger la información y las herramientas de auditoría contra el acceso, la modificación y la eliminación no autorizados. Los registros de auditoría contienen un conjunto de elementos de datos para respaldar los requisitos de análisis necesarios. Además, los registros de auditoría están disponibles para que los usuarios autorizados los inspeccionen o analicen cuando lo soliciten y en respuesta a eventos relacionados con la seguridad o que afecten a la empresa.

Los derechos de acceso de los usuarios a los AWS sistemas (por ejemplo, la red, las aplicaciones, las herramientas, etc.) se revocan en un plazo de 24 horas a partir de la finalización o desactivación. Las cuentas de usuario inactivas se desactivan y and/or se eliminan al menos cada 90 días.

## ¿Están activadas la detección o el monitoreo de anomalías para el acceso o el registro de auditoría para detectar el aumento de privilegios o el uso indebido del acceso a fin de alertar proactivamente al equipo de AMS?

Los hosts de producción AWS están equipados con un sistema de registro por motivos de seguridad. Este servicio registra las acciones humanas en los hosts, incluidos los inicios de sesión, los intentos de inicio de sesión fallidos y los cierres de sesión. Los equipos de AWS seguridad almacenan estos registros y pueden acceder a ellos para analizar la causa raíz en caso de que se sospeche que se ha producido un incidente de seguridad. Los registros de un anfitrión determinado también están disponibles para el equipo propietario de ese anfitrión. Los equipos de servicio disponen de una herramienta preliminar de análisis de registros que les permite buscar en sus registros un análisis operativo y de seguridad. Los procesos se implementan para ayudar a proteger los registros y las herramientas de auditoría contra el acceso, la modificación y la eliminación no autorizados. El equipo AWS de seguridad realiza un análisis de los registros para identificar los eventos en función de los parámetros de gestión de riesgos definidos.

## ¿Qué tipos de datos de clientes se extraen de las cuentas gestionadas por AMS y cómo se utilizan y almacenan?

AMS no accede a su contenido ni lo utiliza para ningún propósito. AMS define el contenido del cliente como el software (incluidas las imágenes de las máquinas), los datos, el texto, el audio, el vídeo o las imágenes que un cliente o cualquier usuario final transfiere AWS para su procesamiento, almacenamiento o alojamiento Servicios de AWS en relación con la cuenta de un cliente, y cualquier resultado computacional que un cliente o su usuario final obtenga de lo anterior mediante el uso que haga de Servicios de AWSél.

# Supervisión y gestión de eventos en AMS Accelerate

El sistema de monitoreo AMS Accelerate monitorea sus AWS recursos para detectar fallas, degradación del rendimiento y problemas de seguridad.

Como cuenta gestionada, AMS Accelerate configura e implementa alarmas para AWS los recursos aplicables, supervisa estos recursos y realiza las correcciones necesarias.

El sistema de monitoreo AMS Accelerate se basa en herramientas internas, como Resource Tagger y Alarm Manager Servicios de AWS, y aprovecha, como AWS AppConfigAmazon CloudWatch (CloudWatch), Amazon EventBridge (anteriormente conocido como CloudWatch), Amazon GuardDuty, Amazon Macie y. AWS Health

AMS Accelerate ofrece una gama de servicios operativos para ayudarlo a alcanzar la excelencia operativa en. AWS Para comprender rápidamente cómo AMS ayuda a sus equipos a alcanzar la excelencia operativa general Nube de AWS con algunas de nuestras capacidades operativas clave, como el servicio de asistencia las 24 horas del día, los 7 días de la semana, la supervisión proactiva, la seguridad, la aplicación de parches, el registro y la copia de seguridad, consulte los diagramas de arquitectura de referencia de AMS.

Temas


- ¿Qué es la supervisión?
- Cómo funciona la supervisión
- Alertas del monitoreo de referencia en AMS
- Notificaciones de incidentes compatibles con las aplicaciones en AMS
- Acelere el administrador de alarmas
- Remediación automática de alertas por parte de AMS
- Uso de Amazon EventBridge Managed Rules en AMS
- Remediador de confianza en AMS


Para obtener información sobre la supervisión de Amazon EKS, consulte Supervisión y gestión de incidentes para Amazon EKS en AMS Accelerate

## ¿Qué es la supervisión?

La monitorización de AMS Accelerate ofrece las siguientes ventajas:

- Una configuración predeterminada que crea, administra e implementa políticas en su cuenta gestionada para todos los AWS recursos o los compatibles que seleccione.
- Una base de monitoreo para que tengas un nivel de protección predeterminado, incluso si no configuras ningún otro monitoreo para tus cuentas administradas. Para obtener más información, consulte Alertas del monitoreo de referencia en AMS.
- La capacidad de personalizar las alarmas de recursos de referencia para que se ajusten a sus requisitos.
- Cuando es posible, AMS Operations corrige automáticamente las alertas para evitar o reducir el impacto en sus aplicaciones. Por ejemplo, si utilizas una EC2 instancia de Amazon independiente y no pasa la comprobación de estado del sistema, AMS intentará recuperar la instancia deteniéndola y reiniciándola. Para obtener más información, consulte Remediación automática de alertas por parte de AMS .
- Visibilidad de las alertas activas y previamente resueltas mediante. OpsCenter Por ejemplo, si tienes un uso elevado e inesperado de la CPU en una EC2 instancia de Amazon, puedes solicitar acceso a la AWS Systems Manager consola (que incluye el acceso a la OpsCenter consola) y verla OpsItem directamente en la OpsCenter consola.
- Investigando las alertas para determinar las acciones adecuadas. Para obtener más información, consulte Gestión de incidentes en AMS Accelerate.
- Las alertas se generan en función de la configuración de su cuenta y de AWS los servicios compatibles. La configuración de supervisión de una cuenta hace referencia a todos los parámetros de recursos de la cuenta que crean una alerta. La configuración de supervisión de una cuenta incluye las definiciones de CloudWatch alarma y los elementos EventBridge (antes denominados CloudWatch eventos) que generan la alerta (alarma o evento). Para obtener más información sobre los parámetros de los recursos, consulteAlertas del monitoreo de referencia en AMS.
- Notificación de fallos inminentes, continuos, inminentes o potenciales, de una degradación del rendimiento o de problemas de seguridad generados por la supervisión básica configurada en una cuenta (conocida como alerta). Entre los ejemplos de alertas se incluyen una CloudWatch alarma, un evento o un hallazgo de un AWS servicio, como GuardDuty o. AWS Health

## Cómo funciona la supervisión

Consulte los siguientes gráficos sobre la arquitectura de supervisión en AWS Managed Services (AMS).

El siguiente diagrama muestra la arquitectura de monitoreo AMS Accelerate.

Una vez que se etiquetan los recursos en función de la política definida mediante el etiquetador de recursos y se implementan las definiciones de alarmas, en la siguiente lista se describen los procesos de supervisión del AMS.

- Generación: en el momento de la incorporación de la cuenta, AMS configura la supervisión de referencia (una combinación de alarmas CloudWatch (CW) y reglas de eventos de CW) para todos los recursos creados en una cuenta gestionada. La configuración de supervisión básica genera una alerta cuando se activa una alarma de CW o se genera un evento de CW.
- Agregación: todas las alertas generadas por sus recursos se envían al sistema de monitoreo de AMS, dirigiéndolas a un tema de SNS de la cuenta. También puede configurar la forma en que AMS agrupa las alertas de Amazon EC2. AMS agrupa todas las alertas relacionadas con la misma instancia de EC2 en un solo incidente o crea un incidente por alerta, según sus preferencias. Puede cambiar esta configuración en cualquier momento trabajando con su administrador de prestación de servicios en la nube o con un arquitecto de nube.
- Procesamiento: AMS analiza las alertas y las procesa en función de su potencial de impacto. Las alertas se procesan como se describe a continuación.
  - Alertas con un impacto conocido en los clientes: conducen a la creación de un nuevo informe de incidentes y AMS sigue el proceso de gestión de incidentes.

    Ejemplo de alerta: una instancia de Amazon EC2 no supera una comprobación de estado del sistema, AMS intenta recuperar la instancia deteniéndola y reiniciándola.
  - Alertas con un impacto incierto en los clientes: en el caso de este tipo de alertas, AMS envía un informe del incidente y, en muchos casos, le pide que verifique el impacto antes de que AMS tome medidas. Sin embargo, si se aprueban las comprobaciones relacionadas con la infraestructura, AMS no le enviará ningún informe del incidente.

    Por ejemplo: una alerta de un uso superior al 85% de la CPU durante más de 10 minutos en una instancia de Amazon EC2 no se puede clasificar inmediatamente como incidente, ya que este comportamiento podría esperarse en función del uso. En este ejemplo, AMS Automation realiza comprobaciones relacionadas con la infraestructura del recurso. Si se aprueban esas comprobaciones, AMS no envía ninguna notificación de alerta, incluso si el uso de la CPU supera el 99%. Si Automation detecta que las comprobaciones relacionadas con la infraestructura están fallando en el recurso, AMS envía una notificación de alerta y comprueba si es necesaria una mitigación. Las notificaciones de alerta se analizan en detalle en esta sección.

AMS ofrece opciones de mitigación en la notificación. Cuando respondes a la notificación confirmando que la alerta es un incidente, AMS crea un nuevo informe de incidente y comienza el proceso de gestión de incidentes de AMS. Las notificaciones de servicio que reciben una respuesta que indica que «no afecta al cliente» o que no reciben respuesta alguna durante tres días se marcan como resueltas y la alerta correspondiente se marca como resuelta.

- Alertas sin impacto en el cliente: si, tras una evaluación, AMS determina que la alerta no afecta al cliente, se cierra.

  Por ejemplo, AWS Health notifica que una instancia EC2 necesita ser reemplazada, pero esa instancia ha sido cancelada desde entonces.

## Notificaciones agrupadas de instancias EC2

Puede configurar la supervisión de AMS para agrupar las alertas de la misma instancia de EC2 en un solo incidente. Su administrador de prestación de servicios en la nube o su arquitecto de nube pueden configurarlo por usted. Hay cuatro parámetros que puede configurar para cada cuenta administrada por AMS.

1. Alcance: elija entre toda la cuenta o basado en etiquetas.
   - Para especificar una configuración que se aplique a todas las instancias de EC2 de esa cuenta, elija scope = account-wide.
   - Para especificar una configuración que se aplique únicamente a las instancias EC2 de esa cuenta con una etiqueta específica, elija scope = tag-based.
2. Regla de agrupación: elija una clásica o una instancia.
   - Para configurar la agrupación a nivel de instancia para todos los recursos de tu cuenta, elige ámbito = toda la cuenta y regla de agrupación = instancia.
   - Para configurar recursos específicos de tu cuenta para que usen la agrupación a nivel de instancia, etiqueta esas instancias y, a continuación, elige ámbito = basado en etiquetas y regla de agrupación = nivel de instancia.
   - Para no usar la agrupación de instancias para las alertas de tu cuenta, elige la regla de agrupación = clásica.
3. Opción de participación: elige no incluir ninguna, solo informar o elegir la opción predeterminada.
   - Para que AMS no cree incidentes ni ejecute automatizaciones para las alarmas desde esos recursos mientras la configuración esté activa, no elija ninguna.

- Para que AMS no cree incidentes ni ejecute automatizaciones para las alarmas desde esos recursos mientras la configuración esté activa, ni ejecute la reparación automática de los documentos de Systems Manager, sino que incluya registros de estos eventos en los informes, elija solo informar. Esto puede resultar útil si desea reducir el volumen de casos de asistencia ante incidentes con los que interactúa y si algunos incidentes procedentes de algunos recursos no requieren atención inmediata, por ejemplo, los que se producen en una cuenta ajena a la producción.
- Para que AMS procese sus alertas, ejecute automatizaciones y cree casos de incidentes cuando sea necesario, elija la opción predeterminada.

4. Resolver después: elija entre 24 horas, 48 horas o 72 horas. Por último, configure cuándo se cierran automáticamente los casos de incidentes. Si el tiempo transcurrido desde la correspondencia del último caso alcanza el valor de resolución posterior configurado, el incidente se cierra.

### Notificación de alerta

Como parte del procesamiento de alertas, en función del análisis de impacto, AWS Managed Services (AMS) crea un incidente e inicia el proceso de administración de incidentes para su corrección, cuando se puede determinar el impacto. Si no se puede determinar el impacto, AMS envía una notificación de alerta a la dirección de correo electrónico asociada a su cuenta mediante una notificación de servicio. En algunos casos, esta notificación de alerta no se envía. Por ejemplo, si las comprobaciones relacionadas con la infraestructura superan una alerta de uso elevado de la CPU, no se te enviará ninguna notificación de alerta. Para obtener más información, consulte el diagrama sobre la arquitectura de supervisión de AMS para ver el proceso de gestión de alertas en. Cómo funciona la supervisión

## Notificación de alertas basada en etiquetas

Usa etiquetas para enviar notificaciones de alerta para tus recursos a diferentes direcciones de correo electrónico. Se recomienda utilizar notificaciones de alerta basadas en etiquetas, ya que las notificaciones que se envían a una sola dirección de correo electrónico pueden causar confusión cuando varios equipos de desarrolladores utilizan la misma cuenta. Las notificaciones de alertas basadas en etiquetas no se ven afectadas por la Notificaciones agrupadas de instancias EC2 configuración que elijas.

Con las notificaciones de alerta basadas en etiquetas, puedes:

- Enviar alertas a una dirección de correo electrónico específica: etiquete los recursos que tengan alertas que deban enviarse a una dirección de correo electrónico específica con la`key = OwnerTeamEmail`,`value = EMAIL_ADDRESS`.
- Enviar alertas a varias direcciones de correo electrónico: para usar varias direcciones de correo electrónico, especifique una lista de valores separados por comas. Por ejemplo, `key = OwnerTeamEmail`, `value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, ...`. El número total de caracteres del campo de valor no puede superar los 260.
- Use una clave de etiqueta personalizada: para usar una clave de etiqueta personalizada, proporcione el nombre de la clave de etiqueta personalizada a su CSDM en un correo electrónico en el que dé su consentimiento explícito para activar las notificaciones automáticas para la comunicación basada en etiquetas. Se recomienda utilizar la misma estrategia de etiquetado para las etiquetas de contacto en todas las instancias y recursos.

> **Note**
>
> El valor clave `OwnerTeamEmail` no tiene por qué estar en camel Case. Sin embargo, las etiquetas distinguen mayúsculas de minúsculas y se recomienda utilizar el formato recomendado.
> La dirección de correo electrónico debe especificarse en su totalidad, con el signo «at» (@) para separar la parte local del dominio. Ejemplos de direcciones de correo electrónico no válidas: `Team.AppATabc.xyz` o`john.doe`. Para obtener información general sobre tu estrategia de etiquetado, consulta los recursos de etiquetado AWS. No añadas información de identificación personal (PII) en tus etiquetas. Usa listas de distribución o alias siempre que sea posible.
> La notificación de alertas basada en etiquetas es compatible con los recursos de los siguientes servicios de Amazon: EC2, Elastic Block Store (EBS), Elastic Load Balancing (ELB), Application Load Balancer (ALB), Network Load Balancer, Relational Database Service (RDS), Elastic File System (EFS) OpenSearch y VPN. FSx Site-to-Site

## Alertas del monitoreo de referencia en AMS

Obtenga información sobre los valores predeterminados de monitorización de AMS Accelerate. Para obtener más información, consulte Supervisión y gestión de eventos en AMS Accelerate.

La siguiente tabla muestra lo que se monitorea y los umbrales de alerta predeterminados. Puede cambiar los umbrales de alerta con un documento de configuración personalizado o enviar una solicitud de servicio. Para obtener instrucciones sobre cómo cambiar la configuración de alarma personalizada, consulte. Cambiar la configuración de alarmas de Accelerate Para recibir notificaciones cuando las alarmas superen su umbral, además del proceso de alerta estándar de AMS, puede sobrescribir las configuraciones de alarma. Para obtener instrucciones, consulte Acelere el administrador de alarmas.

Amazon CloudWatch ofrece una mayor retención de las métricas. Para obtener más información, consulte CloudWatch Límites.

> **Note**
>
> AMS Accelerate calibra su monitorización de referencia de forma periódica. Las cuentas nuevas siempre se incorporan con la supervisión de referencia más reciente y en la tabla se describe la supervisión de referencia de las cuentas recién incorporadas. AMS Accelerate actualiza periódicamente la supervisión básica de las cuentas existentes, por lo que es posible que se produzca un retraso antes de que se apliquen las actualizaciones.

Alertas del monitoreo de referencia

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| En el caso de las alertas destacadas (*), AMS evalúa el impacto de forma proactiva y las corrige siempre que es posible; si no es posible remediarlas, AMS crea un incidente. Si la automatiz ación no corrige el problema, AMS le informa del caso del incidente y contrata a un ingeniero de AMS. Además, si opta por el tema de las Direct-Customer-Alerts redes sociales, estas alertas se enviarán directamente a su correo electrónico. | | |
| Instancia de Application Load Balancer | ApplicationLoadBalancerErro rCount<br><br>(HTTPCode_ELB_5xx_ COUNT/RequestCount) *100<br><br>suma > 15% durante 1 minuto, 5 veces consecutivas. | Recuento de errores LoadBalancer HTTP: 5XX en la aplicación<br><br>CloudWatch alarma por un número excesivo de códigos de respuesta HTTP 5XX |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| | | generados por el Loadbalancer. |
| Instancia de Application Load Balancer | RejectedConnectionCount<br><br>suma > 0% durante 1 minuto, 5 veces consecutivas. | Solicitud LoadBalancer rechazada: número de conexiones<br><br>CloudWatch alarma si el número de conexiones que se rechazaron porque el balanceador de carga alcanzó su máximo |
| Objetivo de Application Load Balancer | TargetConnectionErrorCount<br><br>(HTTPCode_TARGET_5xx_COUNT/RequestCount) *100<br><br>suma > 15% durante 1 minuto, 5 veces consecutivas. | $ {ElasticLoadBalancingV2::TargetGroup:FullName} - Recuento de errores de conexión al LoadBalancer destino de la aplicación: $ {ElasticLoadBalancingV2:TargetGroup: :UUID}<br><br>CloudWatch alarma por un exceso de códigos de respuesta HTTP 5XX generados por un objetivo. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| Objetivo de Application Load Balancer | ApplicationLoadBalancerTargetGroupErrorCount<br><br>suma > 0% durante 1 minuto, 5 veces consecutivas. | $ {ElasticLoadBalancingV2::TargetGroup:FullName} - Número de errores HTTP 5XX de Application LoadBalancer Target: $ {ElasticLoadBalancingV2:TargetGroup: :UUID}<br><br>CloudWatch se emitirá una alarma si el número de conexiones entre el balanceador de cargas y las instancias registradas no se estableció correctamente. |
| Instancia Amazon EC2: todas OSs | CPUUtilization*<br><br>> 95% durante 5 minutos, 6 veces consecutivas, si la instancia no responde a un comando de sondeo de Systems Manager. | $ {EC2::InstanceId}: CPU demasiado alta<br><br>CloudWatch alarma. El uso elevado de la CPU es un indicador de un cambio en el estado de la aplicación, como puntos muertos, bucles infinitos, ataques maliciosos y otras anomalías.<br><br>Son alarmas. Direct-Customer-Alerts |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
| --- | --- | --- |
| Instancia Amazon EC2: todas OSs | StatusCheckFailed<br><br>> 0% durante 5 minutos, 3 veces consecutivas. | $ {EC2::InstanceId}: No se pudo comprobar el estado<br><br>CloudWatch alarma. La comprobación de estado fallida indica que una instancia de Amazon EC2 con el ID especificado no pasó una o más de sus comprobaciones de estado automatizadas. Esto significa que la instancia tiene un problema que impide que funcione correctamente o que no se pueda acceder a ella. |
| Instancia de Amazon EC2: Linux | Mem_used_percent mínimo<br><br>>= 95% durante 5 minutos, 6 veces consecutivas. | $ {EC2::InstanceId}: Sin memoria<br><br>CloudWatch alarma. Memoria libre indica que la memoria disponible (RAM) en la instancia de Amazon EC2 especificada ha caído por debajo de un umbral definido. Esto puede provocar problemas de memoria, bloqueos del sistema e indica que la instancia podría necesitar más RAM.<br><br>Se trata de Direct-Customer-Alerts alarmas. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
| --- | --- | --- |
| Instancia de Amazon EC2: Linux | Promedio de swap_used _percent<br><br>**>=** 95% durante 5 minutos, 6 veces consecutivas. | $ {EC2::InstanceId}: Sin intercambio<br><br>CloudWatch alarma. El promedio de swap_used _percent en una instancia de Amazon EC2 indica que el porcentaje promedio del espacio de intercambio asignado actualmente en uso ha superado un umbral predefinido. Esto puede provocar una degradación del rendimiento, cuellos de botella y problemas de memoria.<br><br>Son alarmas. Direct-Cu stomer-Alerts |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
| --- | --- | --- |
| Instancia de Amazon EC2: Linux | Porcentaje máximo de disk_used_percent<br><br>>= 95% durante 5 minutos, 6 veces consecutivas. | $ {EC2::InstanceId}: Uso del disco demasiado alto: $ {EC2: :Disk: :UUID}<br><br>CloudWatch alarma. El uso del disco demasiado alto indica que el uso del disco en un Amazon EC2 específico o en el disco identificado se acerca a su capacidad. Esto puede provocar una degradación del rendimiento, errores en las aplicaciones e inestabilidad del sistema.<br><br>Se trata de Direct-Customer-Alerts alarmas. |
| Instancia de Amazon EC2: Windows | % mínimo de memoria: bytes comprometidos en uso<br><br>>= 95% durante 5 minutos, 6 veces consecutivas. | $ {EC2::InstanceId}: Sin memoria<br><br>CloudWatch alarma. Memoria libre indica que la memoria disponible (RAM) en la instancia de Amazon EC2 especificada ha caído por debajo de un umbral definido. Esto puede provocar problemas de memoria, bloqueos del sistema e indica que la instancia podría necesitar más RAM.<br><br>Se trata de Direct-Customer-Alerts alarmas. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| Instancia de Amazon EC2: Windows | LogicalDisk % máximo de espacio libre<br><br><= 5% durante 5 minutos, 6 veces consecutivas. | $ {EC2::InstanceId}: Uso del disco demasiado alto: $ {EC2: :Disk: :UUID}<br><br>CloudWatch alarma. Indica que el porcentaje de espacio libre en un disco lógico (una partición del sistema de archivos) dentro de una instancia Amazon EC2 de Windows ha superado un umbral predefinido. La escasez de espacio en disco puede provocar una escasez de espacio en disco<br><br>Son Direct-Customer-Alerts alarmas. |
| Amazon EFS | AMSEFSBurstCreditBalanceExhausted.<br><br>BurstCreditBalance menos de 1000 durante quince minutos. | $ {EFS::FileSystemId}: EFS: Saldo crediticio reventado<br><br>CloudWatch alarma en el sistema BurstCreditBalance de archivos Amazon EFS. |
| Amazon EFS | AMSEFSClientConnectionsLimit.<br><br>ClientConnections > 24 000 durante quince minutos. | $ {EFS::FileSystemId}: EFS: límite de conexiones de clientes<br><br>CloudWatch alarma en el sistema ClientConnections de archivos Amazon EFS. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| Amazon EFS | AMSEFSThroughputUtilization Limit.<br><br>Utilización del rendimiento de EFS superior al 80% durante una hora. | $ {EFS::FileSystemId}: EFS: límite de utilización del rendimiento<br><br>CloudWatch alarma sobre la utilización del rendimiento del sistema de archivos Amazon EFS. |
| Amazon EFS | AMSEFSPercentIOLimit.<br><br>Porcentaje IOLimit > 95 durante setenta y cinco minutos. | $ {EFS::FileSystemId}: EFS: Porcentaje IOLimit<br><br>CloudWatch alarma sobre el porcentaje IOLimit del sistema de archivos Amazon EFS. |
| Amazon EKS | Consulte Amazon EKSAlertas de referencia en la supervisión y la gestión de incidentes para Amazon EKS en AMS Accelerate. | |
| Instancia de Elastic Load Balancing | SpilloverCountBackendConnectionErrors<br><br>> 1 durante 1 minuto, 15 veces consecutivas. | Alarma clásica de conteo LoadBalancer de derrames<br><br>CloudWatch alarma si hay un número excesivo de solicitudes rechazadas porque la cola de espera está llena. |
| Instancia de Elastic Load Balancing | HTTPCode_ELB_5xx_Count<br><br>suma > 0 durante 5 minutos, 3 veces consecutivas. | CloudWatch alarma por un número excesivo de códigos de respuesta HTTP 5XX que se originan en el balanceador de cargas. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| Instancia de Elastic Load Balancing | SurgeQueueLength<br><br>> 100 durante 1 minuto, 15 veces consecutivas. | Alarma LoadBalancer clásica de longitud de cola de espera.<br><br>CloudWatch alarma si hay un número excesivo de solicitud es pendientes de enrutamie nto. |
| FSx para ONTAP | AMSFSXONTAPIOPSUti lization.<br><br>Utilización de IOPS de FSX:ONTAP superior al 80% durante dos horas. | $ {FSx::}: Utilización de IOPS en FSX:ONTAP FileSystemId<br><br>CloudWatch alarma sobre el límite de utilización de IOPS de la instancia de ONTAP. FSx |
| FSx para ONTAP | AMSFSXONTAPThrough putUtilización.<br><br>FSX: utilización del rendimien to de ONTAP superior al 80% durante dos horas. | $ {FSx::}: Utilización del rendimiento de FSX:ONTAP FileSystemId<br><br>CloudWatch alarma sobre el límite de rendimiento del volumen de ONTAP. FSx |
| FSx para ONTAP | AMSFSXONTAPVolumeI nodeUtilization.<br><br>FSX:ONTAP Utilización de inodo superior al 80% durante dos horas. | $ {FSx::} :$ {: :ONTAP::F ileSystemId} Utilización de inodo FSx FSX:ONTAP VolumeId<br><br>CloudWatch alarma sobre el límite de utilización de la capacidad de archivos del volumen de ONTAP. FSx |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| FSx para ONTAP | AMSFSXONTAPVolumeCapacityUtilization.<br><br>Utilización de la capacidad de volumen de FSX:ONTAP superior al 80% durante dos horas. | $ {FSx::FileSystemId} :$ {: :ONTAP::} FSx VolumeId<br><br>CloudWatch alarma sobre el límite de utilización de la capacidad de volumen del FSx volumen ONTAP. |
| FSx para Windows File Server | AMSFSXWindowsThroughputUtilization.<br><br>FSX: Utilización del rendimiento de Windows superior al 80% durante dos horas. | $ {FSx::FileSystemId}: FSX:Utilización del rendimiento de Windows<br><br>CloudWatch alarma sobre el límite de rendimiento de la instancia del servidor de archivos FSx de Windows. |
| FSx para el servidor de archivos de Windows | AMSFSXWindowsIOPSUtilization.<br><br>FSX: Utilización de IOPS de Windows superior al 80% durante dos horas. | $ {FSx::FileSystemId}: FSX:Utilización de IOPS de Windows<br><br>CloudWatch alarma sobre el límite de utilización de IOPS de la instancia del servidor de archivos FSx de Windows. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| GuardDuty Servicio | No aplicable; se supervisan todos los hallazgos (con fines de amenaza). Cada hallazgo corresponde a una alerta.<br><br>Cambios en los GuardDuty hallazgos. Entre estos cambios se incluyen los resultados recién generados, y todos los casos posteriores de resultados. | Para obtener una lista de los tipos de GuardDuty búsqueda compatibles, consulte Tipos de búsqueda GuardDuty activos. |
| Estado | Panel de AWS Health | Las notificaciones se envían cuando hay cambios en el estado de Panel de AWS Health (AWS Health) eventos que requieren la acción de AMS Operations en relación con los servicios supervisa dos por AMS. Para obtener más información, consulte Servicios compatibles. |
| IAM | El perfil de instancia de IAM de Amazon EC2 no existe.<br><br>Falta el perfil de instancia de IAM. | Para obtener instrucciones sobre la sustitución de un perfil de instancia de IAM de Amazon EC2, consulte la documentación de IAM en Replace IAM role. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
| --- | --- | --- |
| IAM | El perfil de instancia de IAM de Amazon EC2 tiene demasiadas políticas.<br><br>El perfil de instancia de IAM tiene 10 políticas y no se pueden añadir políticas adicionales. | • Modifique la cuota AWS de servicio de IAM para aumentar a 20 el número de políticas administradas por función. Para obtener información sobre las cuotas de servicio, consulte Visualización de las cuotas de servicio.<br>• Reduzca el número de políticas administradas por debajo de la cuota de IAM actual eliminando las políticas administradas innecesarias para la función de IAM asociada a estas instancias. Asegúrese de mantener las políticas exigidas por AMS.<br>• Reduzca el número de políticas gestionadas por debajo de la cuota de IAM actual consolidando las políticas para la función de IAM asociada a estas instancias. Asegúrese de mantener las políticas exigidas por AMS.<br><br>Para conocer las políticas requeridas por AMS, consulte la Guía del usuario de AMS |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| | | Accelerate:Detalles de cambio de permisos de IAM. |
| Macie | Alertas recién generadas y actualizaciones de las alertas existentes.<br><br>Macie encuentra cualquier cambio en los resultado s. Entre estos cambios se incluyen los resultados recién generados, y todos los casos posteriores de resultados. | Alerta de Amazon Macie. Para obtener una lista de los tipos de alertas de Amazon Macie compatibles, consulte Análisis de los hallazgos de Amazon Macie. Tenga en cuenta que Macie no está activado para todas las cuentas. |
| NATGateways | PacketsDropCount : Alarma si packetsdropcount es > 0 en un período de 15 minutos | NatGateway PacketsDr opCount<br><br>Un valor mayor que cero puede indicar que existe un problema transitorio con la gateway NAT. |
| NATGateways | ErrorPortAllocation : Alarma si las pasarelas NAT no pudieron asignar el puerto durante un período de evaluación de más de 15 minutos | NatGateway ErrorPortAllocatio n<br><br>Número de veces que la gateway NAT no pudo asignar un puerto de origen. Un valor superior a cero indica que hay demasiadas conexiones simultáneas abiertas. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| OpenSearch clúster | ClusterStatus<br><br>el máximo rojo es >= 1 durante 1 minuto, 1 vez consecutiva. | ClusterStatus Rojo<br><br>CloudWatch alarma. La clave de AWS KMS cifrado que se utiliza para cifrar los datos en reposo de su dominio está deshabilitada. Vuelva a habilitarla para restablecer las operaciones normales. Para obtener más información, consulta Red Cluster Status. |
| Dominio OpenSearch | KMSKeyError<br><br>>= 1 durante 1 minuto, 1 vez consecutiva. | Error de clave KMS<br><br>CloudWatch alarma. Al menos una partición principal y sus réplicas no están asignados a un nodo. Para obtener más información, consulta Cifrado de datos en reposo para Amazon OpenSearch Service. |
| Dominio OpenSearch | KMSKeyInaccesible<br><br>>= 1 durante 1 minuto, 1 vez consecutiva. | Error de clave KMS inaccesib le<br><br>CloudWatch alarma. Al menos una partición principal y sus réplicas no están asignados a un nodo. Para obtener más información, consulta Cifrado de datos en reposo para Amazon OpenSearch Service. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| Dominio OpenSearch | ClusterStatus<br><br>el máximo amarillo es >= 1 durante 1 minuto, 1 vez consecutiva. | ClusterStatus Amarillo<br><br>Al menos una partición de réplica no está asignada a un nodo. Para obtener más información, consulte Estado del clúster amarillo. |
| Dominio OpenSearch | FreeStorageSpace<br><br>el mínimo es <= 20480 durante 1 minuto, 1 vez consecutiva. | Poco espacio de almacenam iento libre<br><br>El espacio de almacenam iento disponible de un nodo en su clúster se redujo hasta los 20 GiB. Para obtener más información, consulta Falta de espacio de almacenamiento disponible. |
| Dominio OpenSearch | ClusterIndexWritesBlocked<br><br>>= 1 durante 5 minutos, 1 vez consecutiva. | El índice de clústeres está bloqueado<br><br>El clúster bloquea las solicitud es de escritura. Para obtener más información, consulte ClusterBlockException. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| Dominio OpenSearch | Nodos<br><br>< x como mínimo durante 1 día, 1 vez consecutiva. | Nodos inactivos<br><br>x es el número de nodos del clúster. Esta alarma indica que al menos un nodo del clúster se mantuvo inaccesible durante un día. Para obtener más información, consulte Nodos de clúster fallidos. |
| Dominio OpenSearch | CPUUtilization<br><br>una media superior al 80% durante 15 minutos, 3 veces consecutivas. | Uso elevado de la CPU en el nodo de datos<br><br>Es habitual el uso del 100% de la CPU, pero un uso medio alto continuado es problemát ico. Considera la posibilidad de ajustar el tamaño de un tipo de instancia existente o de añadir instancias. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| Dominio OpenSearch | JVMMemoryPresión<br><br>máximo >= 80% durante 5 minutos, 3 veces consecuti vas. | Uso elevado de memoria en el nodo de datos<br><br>El clúster podría encontrar errores de memoria insuficie nte si aumenta el uso. Piense en realizar un escalado vertical. OpenSearch utiliza la mitad de la RAM de una instancia para el montón Java, hasta un tamaño de montón de 32 GiB. Puede escalar las instancias verticalmente hasta 64 GiB de RAM y después escalarlas horizontalmente mediante el agregado de instancias. |
| Dominio OpenSearch | Maestro CPUUtilization<br><br>promedio >= 50% durante 15 minutos, 3 veces consecuti vas. | Master Nodes: uso elevado de la CPU<br><br>Considere la posibilidad de utilizar tipos de instancias más grandes para sus nodos maestros dedicados. Debido al rol que desempeñan en la estabilidad del clúster y las implementaciones blue/ green, los nodos principales dedicados deberían tener un uso de CPU medio menor que los nodos de datos. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| Dominio OpenSearch | JVMMemoryPresión maestra<br><br>máximo >= 80% durante 15 minutos, 1 vez consecutiva. | Presión alta de memoria JVM en el nodo principal<br><br>Considere la posibilidad de utilizar tipos de instancias más grandes para sus nodos maestros dedicados. Debido al rol que desempeñan en la estabilidad del clúster y las implementaciones blue/green, los nodos principales dedicados deberían tener un uso de CPU medio menor que los nodos de datos. |
| OpenSearch instancia | AutomatedSnapshotFailure<br><br>el máximo es >= 1 durante 1 minuto, 1 vez consecutiva. | Fallo automatizado en las instantáneas<br><br>CloudWatch alarma. Se produjo un error en una instantánea automatiz ada. Este error suele ser el resultado de un estado rojo del clúster. Para obtener más información, consulte Red Cluster Status. |
| Amazon RDS | Utilización media de la CPU<br><br>> 90% durante 15 minutos, 2 veces consecutivas. | $ {RDS:: DBInstance Identifie r}: CPUUtilization<br><br>CloudWatch alarmas. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| Amazon RDS | Suma de DiskQueueDepth<br><br>> 75% durante 1 minuto, 15 veces consecutivas. | $ {RDS:: DBInstance Identifier}: DiskQueue<br><br>CloudWatch alarmas. |
| Amazon RDS | Promedio FreeStorageSpace<br><br>< 1.073.741.824 bytes durante 5 minutos, 2 veces consecutivas. | $ {RDS:: Identifier}: DBInstance FreeStorageSpace<br><br>CloudWatch alarmas. |
| Amazon RDS | Alerta de bajo almacenamiento<br><br>Se activa cuando se ha agotado el almacenamiento asignado a la instancia de base de datos. | RDS-EVENT-0007, consulte los detalles en Uso de la notificación de eventos de Amazon RDS. |
| Amazon RDS | Fallo en la instancia de base<br><br>Se ha producido un error en la instancia de base de datos debido a una configuración incompatible o a un problema de almacenamiento subyacente. Comience a point-in-time-restore para la instancia de base de datos. | RDS-EVENT-0031, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| Amazon RDS | No se intentó la conmutación por error del RDS -0034.<br><br>Amazon RDS no está intentando realizar la conmutación por error solicitad a porque recientemente se ha producido una conmutaci ón por error en la instancia de base de datos. | RDS-EVENT-0034, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |
| Amazon RDS | RDS: parámetros no válidos de la instancia de base de datos 0035<br><br>Por ejemplo, MySQL no se pudo iniciar porque un parámetro relacionado con la memoria está establecido en un valor demasiado alto para esta clase de instancia, por lo que debería modificar el parámetro de memoria y reiniciar la instancia de base de datos. | RDS-EVENT-0035, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |
| Amazon RDS | Instancia de IDs base de datos de subred no válida<br><br>La instancia de base de datos está en una red incompati ble. Algunas de las subredes especificadas no IDs son válidas o no existen. | Evento de servicio. RDS-EVENT-0036, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| Amazon RDS | Error de lectura y réplica de la instancia de base de datos RDS-0045<br><br>Se ha producido un error en el proceso de replicación de una réplica de lectura. Para obtener más información, consulte el mensaje del evento. Para obtener información sobre cómo solucionar errores de réplica de lectura, consulte Solución de problemas de réplica de lectura de MySQL. | RDS-EVENT-0045, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |
| Amazon RDS | RDS-0057: Error al crear la cuenta de usuario de statspack<br><br>Se ha finalizado la replicación en la réplica de lectura. | Evento de servicio. RDS-EVENT-0057, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |
| Amazon RDS | La replicación de lectura de la instancia de base de datos RDS-0058 ha finalizado<br><br>Error al crear la cuenta del usuario PERFSTAT de Statspack. Elimine la cuenta antes de añadir la opción Statspack. | Evento de servicio. RDS-EVENT-0058, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| Amazon RDS | Inicio de recuperación de instancias de base de datos<br><br>La instancia de base de datos de SQL Server está restablec iendo su imagen reflejada. El desempeño se degradará hasta que se restablezca la imagen reflejada. Se ha encontrado una base de datos con un modelo de recuperac ión no completa (non-FULL ). El modelo de recuperac ión volvió a ser COMPLETO y se inició la recuperación duplicada. (<dbname>: <recovery model found>[,...]) | Evento de servicio. RDS-EVENT-0066: consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |
| Amazon RDS | Ha fallado la conmutación por error de un clúster de bases de datos. | RDS-EVENT-0069, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| Amazon RDS | Depósito de S3 de recuperación de permisos no válidos<br><br>El rol de IAM que se utiliza para obtener acceso al bucket de Amazon S3 para las operaciones nativas de copia de seguridad y restauración de SQL Server se ha configurado incorrectamente. Para obtener más información, consulte Configuración de Native Backup and Restore. | Evento de servicio. RDS-EVENT-0081: consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |
| Amazon RDS | Aurora no ha podido copiar los datos de copia de seguridad de un bucket de Amazon S3. | RDS-EVENT-0082, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |
| Amazon RDS | Alerta de almacenamiento bajo cuando la instancia de base de datos ha consumido más del 90% del almacenamiento asignado. | Evento de servicio. RDS-EVENT-0089: consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |
| Amazon RDS | El servicio de notificaciones cuando se produce un error de escalado en el clúster de base de datos Aurora Serverless. | Evento de servicio. RDS-EVENT-0143: consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| Amazon RDS | La instancia de base de datos se encuentra en un estado no válido. No es necesaria ninguna acción. El escalado automático se volverá a intentar más tarde. | RDS-EVENT-0219, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |
| Amazon RDS | La instancia de base de datos alcanzó el umbral de almacenamiento completo y se cerró la base de datos. | RDS-EVENT-0221, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |
| Amazon RDS | Este evento indica que el escalado automático del almacenamiento de instancias de Amazon RDS no puede escalarse. Puede haber varios motivos por los que el escalado automático haya fallado. | RDS-EVENT-0223, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |
| Amazon RDS | El escalado automático del almacenamiento ha desencadenado una tarea de escala de almacenamiento pendiente que alcanzaría el umbral máximo de almacenamiento. | RDS-EVENT-0224, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| Amazon RDS | La instancia de base de datos tiene un tipo de almacenam iento que no está disponibl e actualmente en la zona de disponibilidad. El escalado automático se volverá a intentar más tarde. | RDS-EVENT-0237, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |
| Amazon RDS | Amazon RDS no ha podido aprovisionar capacidad para el proxy porque no hay suficient es direcciones IP disponibles en las subredes. | RDS-EVENT-0243, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |
| Amazon RDS | Su espacio de almacenam iento Cuenta de AWS ha superado la cuota de almacenamiento permitida. | RDS-EVENT-0254, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS. |
| Clúster de Amazon Redshift | El estado del clúster cuando no está en modo de mantenimiento<br><br>< 1 durante 5 minutos | RedshiftClusterHealthStatus<br><br>Para obtener más informaci ón, consulte Supervisión de Amazon Redshift mediante CloudWatch métricas. |
| Site-to-Site VPN | VPNTunnelAbajo<br><br>TunnelState <= 0 durante 1 minuto, 20 veces consecuti vas. | $ {AWS::EC2::VpnConn ectionId} - Abajo VPNTunnel<br><br>TunnelState es 0 cuando ambos túneles están caídos, .5 cuando un túnel está arriba y 1.0 cuando ambos túneles están arriba. |

| Tipo de servicio/recurso | Fuente de alerta y condición de activación | Nombre y notas de la alerta |
|---|---|---|
| Agente de Systems Manager | Instancias EC2 no administr adas por Systems Manager<br><br>El agente SSM no está instalado. El agente SSM está instalado en la instancia, pero el servicio del agente no se está ejecutando. El agente SSM no tiene una ruta de red hacia el servicio AWS Systems Manager. | Existen otras condiciones que provocan interrupciones en el agente de Systems Manager; para obtener más informaci ón, consulte Solución de problemas de disponibilidad de nodos gestionados. |

Para obtener información sobre las medidas correctivas, consulte. Remediación automática de alertas por parte de AMS

Vea el vídeo de Andrew para obtener más información (7:03)

## Notificaciones de incidentes compatibles con las aplicaciones en AMS

Utilice las notificaciones de incidentes automatizadas compatibles con las aplicaciones para personalizar su experiencia de comunicación en los casos de asistencia que AMS cree en su nombre. Al utilizar esta función, AMS recupera las preferencias de carga de trabajo personalizadas AWS Service Catalog AppRegistrypara enriquecer las comunicaciones sobre incidentes de AMS con metadatos sobre sus aplicaciones y personalizar la gravedad de los casos de soporte creados por AMS en su nombre. Para utilizar esta función, primero debe incorporarse a AWS Service Catalog AppRegistry.

Para obtener más información sobre los valores predeterminados de supervisión de AMS Accelerate, consulte. Supervisión y gestión de eventos en AMS Accelerate

# AppRegistry Incorpore y cree aplicaciones

Para incorporarse a AppRegistry, consulte Primeros pasos AppRegistry en la Guía AWS Service Catalog AppRegistry del administrador. Tras la incorporación, utilice uno de los siguientes métodos para crear aplicaciones:

1. AWS consola: para obtener más información sobre cómo crear una aplicación AppRegistry a través de la AWS consola, consulte Creación de aplicaciones en la Guía del AWS Service Catalog AppRegistry administrador.
2. CloudFormation: Puede definir su AppRegistry aplicación del mismo modo que define cualquier otro recurso. Para obtener más información, consulte la referencia de tipos de recursos de AWS Service Catalog AppRegistry en la Guía del usuario de CloudFormation .
3. Automatización AMS: para simplificar el proceso de registro de la solicitud, AMS le proporciona el documento `AWSManagedServices-CreateAppRegistryApplication` de automatización SSM. Para utilizar este método, invoque el documento desde la AWS Systems Manager consola en https://console.aws.amazon.com/systems-manager/o con el comando AWS CLI descrito en el siguiente ejemplo.

```
# The following registers a new application with customized severity
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["normal"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# The following registers a new application with no customizations
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# You can also register applications using CloudFormation stacks
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
```

```
  --parameters '{"ResourceAssociationType":["STACKS"],"AppTagValue":
[""],"CFNStackNames":["arn:aws:cloudformation:us-east-1:123456789012:stack/
stack-2343eddq/1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p"],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
```

## Cree etiquetas para permitir el enriquecimiento de mayúsculas y minúsculas

Debe etiquetar las aplicaciones para que AMS pueda acceder a los metadatos de las aplicaciones. En la siguiente tabla se enumeran las etiquetas obligatorias.

Las etiquetas con el prefijo `ams:rt:` se aplican mediante Resource Tagger.

| Clave de etiqueta | Valor de etiqueta |
|---|---|
| gestionado por AMS | true |
| ams:rt:ams-managed | true |

## Personalice la gravedad de los casos de soporte de AMS para sus aplicaciones

Puede personalizar la gravedad de los casos de soporte creados por AMS especificando el grado de importancia de su solicitud para su organización. Esta configuración se controla mediante un grupo de atributos asociado a la aplicación en AppRegistry. El nombre del grupo de atributos debe coincidir con el siguiente patrón:

```
AMS.<ApplicationName>.CommunicationOptions
```

En el patrón anterior, `ApplicationName` debe coincidir con el nombre utilizado AppRegistry al crear la aplicación.

Contenido de ejemplo:

```
{
```

```
"SchemaVersion": "1.0",
"Criticality": "low"
}
```

SchemaVersion

Esto determina la versión del esquema que está utilizando y el subconjunto de funciones disponibles para su uso.

| Versión del esquema | Característica |
| --- | --- |
| 1.0 | Gravedad de los casos de soporte personalizada en función del valor de criticidad |

Criticidad

La importancia de esta solicitud determina la gravedad de los casos de soporte creados por los sistemas automatizados de AMS.

Valores válidos:

```
low|normal|high|urgent|critical
```

Para obtener más información sobre los niveles de gravedad, consulte SeverityLevella referencia de la AWS Support API.

Obligatorio: sí

## Revisa los permisos necesarios

Para utilizar esta función, AMS necesita tener acceso a los siguientes permisos: AWS Identity and Access Management

- objetivo: ListRoleTags
- objetivo: ListUserTags
- API de etiquetado de grupos de recursos: GetResources
- catálogo de servicios: registro de aplicaciones: GetApplication
- catálogo de servicios - registro de aplicaciones: ListAssociatedAttributeGroups
- catálogo de servicios - registro de aplicaciones: GetAttributeGroup

> **Important**
>
> Asegúrese de que no haya una política de IAM o una política de control de servicios (SCP) que deniegue las acciones anteriores.

El rol realiza las llamadas a la `ams-access-admin` API. El siguiente es un ejemplo de lo que puede ver:

```
arn:aws:sts::111122223333:assumed-role/ams-access-admin/AMS-AMSAppMetadataLookup-*
```

# Acelere el administrador de alarmas

AMS Accelerate aplica alarmas a sus AWS recursos mediante el administrador de alarmas basado en etiquetas para implementar una estrategia de monitoreo básica y garantizar que todos sus AWS recursos estén monitoreados y protegidos. Al integrarse con el administrador de alarmas basado en etiquetas, puede personalizar la configuración de sus AWS recursos en función de su tipo, plataforma y otras etiquetas, para garantizar que los recursos estén monitorizados. Alarm Manager se implementa en su cuenta de Accelerate durante la incorporación.

## Cómo funciona Alarm Manager

Cuando su cuenta se incorpora a AMS Accelerate, se implementan dos documentos JSON, denominados perfiles de configuración, en su cuenta de. AWS AppConfig Ambos documentos de perfil se encuentran en la aplicación Alarm Manager y en el entorno de infraestructura AMS Accelerate.

Los dos perfiles de configuración se denominan AMSManagedAlarmas (el perfil de configuración predeterminado) y CustomerManagedAlarms(el perfil de configuración de personalización).

- Perfil de configuración predeterminado:
  - La configuración que se encuentra en este perfil contiene la configuración predeterminada que AMS Accelerate implementa en todas las cuentas de los clientes. Esta configuración contiene la política de supervisión predeterminada de AMS Accelerate.

> **Important**
>
> No modifique este perfil porque AMS Accelerate puede actualizarlo en cualquier momento y borrar los cambios que haya realizado.

  - Si desea modificar o deshabilitar alguna de estas definiciones, consulte Modificación de la configuración predeterminada de la alarma Accelerate yDesactivación de la configuración de alarma Accelerate predeterminada.
- Perfil de configuración de personalización:
  - Usted administra en su totalidad cualquier configuración de este perfil; AMS Accelerate no sobrescribe este perfil, a menos que lo solicite explícitamente.
  - Puede especificar cualquier definición de alarma personalizada que desee en este perfil y también puede especificar modificaciones en la configuración predeterminada gestionada por AMS Accelerate. Para obtener más información, consulte Modificación de la configuración predeterminada de la alarma Accelerate y Desactivación de la configuración de alarma Accelerate predeterminada.
  - Si actualiza este perfil, Alarm Manager aplicará automáticamente los cambios en todos los recursos relevantes de su cuenta. AWS
  - Puede actualizar este perfil mediante las Consola de administración de AWS CLI/SDK herramientas de AWS. Consulte la Guía AWS AppConfig del usuario para obtener instrucciones sobre cómo actualizar una configuración.
  - Al principio, el perfil de personalización está vacío; sin embargo, se aplica cualquier definición de alarma incluida en el documento de perfil, además de la configuración predeterminada.

Todas las CloudWatch alarmas creadas por el administrador de alarmas contienen la clave de etiqueta ams:alarm-manager:managed y el valor de etiqueta true. Esto es para garantizar que el administrador de alarmas administre solo las alarmas que cree y no interfiera con ninguna de sus propias alarmas. Puedes ver estas etiquetas mediante la CloudWatch ListTagsForResourceAPI de Amazon.

> **Important**
>
> Si las definiciones de alarma personalizadas y las definiciones de alarma predeterminadas se especifican con el mismo ID de configuración (consultePerfil de configuración de

Accelerate: monitoreo), las definiciones personalizadas tienen prioridad sobre las reglas predeterminadas.

## Cómo empezar con Accelerate Alarm Manager

De forma predeterminada, cuando se incorpora AMS Accelerate, la configuración se despliega de forma que se defina AWS AppConfig una línea base de alarma para sus recursos. Las definiciones de alarma se aplican solo a los recursos con las etiquetas ams:rt: *. Recomendamos que estas etiquetas se apliquen mediante la Acelere el etiquetador de recursos siguiente configuración: configure una configuración básica de etiquetador de recursos para que AMS Accelerate sepa qué recursos desea administrar.

Utilice Resource Tagger para aplicar la clave de etiqueta ams:rt:ams-managed con el valor true a todos los recursos que desee que AMS Accelerate supervise.

El siguiente es un ejemplo de perfil de personalización de Resource Tagger que puedes usar para habilitar la monitorización de todas tus EC2 instancias de Amazon. Para obtener información general, consulte Acelere el etiquetador de recursos.

```
{
    "AWS::EC2::Instance": {
        "AMSManageAllEC2Instances": {
            "Enabled": true,
            "Filter": {
                "InstanceId": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

Para obtener información sobre cómo aplicar esta configuración de Resource Tagger, consulte. Ver o realizar cambios en la configuración del etiquetador de recursos

# Acelere las etiquetas de Alarm Manager

De forma predeterminada, cuando se incorpora AMS Accelerate, la configuración se despliega de forma que se defina AWS AppConfig una línea base de alarma para sus recursos. Las definiciones de alarma se aplican solo a los recursos con las etiquetas ams:rt: *. Recomendamos que estas etiquetas se apliquen mediante la Acelere el etiquetador de recursos siguiente configuración: configure una configuración básica de etiquetador de recursos para que AMS Accelerate sepa qué recursos desea administrar.

Utilice Resource Tagger para aplicar la clave de etiqueta ams:rt:ams-managed con el valor true a todos los recursos que desee que AMS Accelerate supervise.

Temas


- Acelere las etiquetas con Resource Tagger
- Acelere las etiquetas sin el etiquetador de recursos
- Acelera las etiquetas usando CloudFormation
- Acelera las etiquetas con Terraform


## Acelere las etiquetas con Resource Tagger

El administrador de alarmas basado en etiquetas gestiona el ciclo de vida de las CloudWatch alarmas por recurso; sin embargo, requiere que los recursos gestionados tengan etiquetas específicas definidas por AMS Accelerate. Para usar el etiquetador de recursos para aplicar el conjunto predeterminado de alarmas administradas por AMS a instancias basadas en Linux y Windows, siga estos pasos.

1. Navegue hasta la AppConfigconsola de su cuenta.
2. Selecciona la ResourceTagger aplicación.
3. Seleccione la pestaña Perfiles de configuración y, a continuación, seleccione CustomerManagedTags.
4. Haga clic en Crear para crear un perfil nuevo.
5. Seleccione JSON y defina su configuración. Para ver más ejemplos de definición de filtros y plataformas, consulteAcelere el etiquetador de recursos.

```
{
"AWS::EC2::Instance": {
   "MonitorAllInstances": {
```

```
        "Enabled": true,
        "Filter": {
            "Platform": "*"
        },
        "Tags": [
            {
                "Key": "ams:rt:ams-managed",
                "Value": "true"
            }
        ]
    }
}
}
```

6. Haga clic en Crear versión de configuración alojada.
7. Haga clic en Iniciar implementación.
8. Defina los siguientes detalles de despliegue:

```
Environment: AMSInfrastructure Hosted configuration version: <Select the version
 that you have just created>
               Deployment Strategy: AMSNoBakeDeployment
```

9. Haga clic en Iniciar despliegue.

Las instancias se etiquetan con ellas`"ams:rt:ams-managed": "true"`, lo que garantiza que `"ams:rt:ams-monitoring-policy-platform": "ams-monitored-linux"` sean adicionales `"ams:rt:ams-monitoring-policy": "ams-monitored"` y se apliquen a las instancias. A continuación, estas etiquetas dan como resultado la creación de las alarmas adecuadas para la instancia. Para obtener más información acerca de este proceso, consulte Supervisión en Accelerate.

Vea el vídeo de Himanshu para obtener más información (11:04)

## Acelere las etiquetas sin el etiquetador de recursos

El administrador de alarmas basado en etiquetas gestiona el ciclo de vida de las CloudWatch alarmas por recurso; sin embargo, requiere que los recursos gestionados tengan etiquetas específicas definidas por AMS Accelerate. AMS Accelerate proporciona un perfil de configuración predeterminado que supone que Resource Tagger ha aplicado las etiquetas.

Si desea utilizar un método alternativo para aplicar etiquetas a sus recursos, como Terraform y no el CloudFormation etiquetador de recursos, debe deshabilitar el etiquetador de recursos para

que no aplique etiquetas a sus recursos y compita con el método de etiquetado que elija. Para obtener instrucciones sobre cómo cambiar el perfil de configuración personalizado del etiquetador de recursos para habilitar el modo de solo lectura, consulte. Impedir que Resource Tagger modifique los recursos

Una vez que el etiquetador de recursos se haya configurado en modo de solo lectura y se haya implementado el perfil de configuración, utilice el método de etiquetado que haya elegido para aplicar etiquetas a los recursos de acuerdo con las siguientes pautas:

| Tipo de recurso | Clave de etiqueta | Valor de etiqueta |
|---|---|---|
| Todos los recursos compatibles (descritos en esta tabla) | ams:rt: ams-monitoring-policy | monitoreado por ams |
| EC2 instancias (Linux) | ams: rt: ams-monitoring-policy-platform | ams-monitored-linux |
| EC2 instancias (Windows) | ams: rt: ams-monitoring-policy-platform | ams-monitored-windows |
| OpenSearch Dominio con KMS | ams:rt: ams-monitoring-with-kms | ams-monitored-with-kms |
| OpenSearch Dominio con nodo maestro dedicado | ams:rt: ams-monitoring-with-master | ams-monitored-with-master |

Los recursos que tienen estas claves y valores de etiquetas son gestionados por el AMS Accelerate Alarm Manager.

## Acelera las etiquetas usando CloudFormation

> **Note**
>
> Asegúrese de haber configurado Resource Tagger en modo de solo lectura antes de aplicar las etiquetas; de lo contrario CloudFormation, Resource Tagger podría modificar las etiquetas en función del perfil de configuración. Para obtener información sobre cómo configurar Resource Tagger en modo de solo lectura y directrices sobre cómo proporcionar sus propias etiquetas, consulte. Acelere las etiquetas sin el etiquetador de recursos

Para aplicar etiquetas mediante este CloudFormation método, puede aplicarlas a nivel de pila (consulte Etiquetas de CloudFormation recursos) o a nivel de recurso individual (por ejemplo, consulte Creación de etiquetas de EC2 instancia).

A continuación, se muestra un ejemplo de cómo aplicar las etiquetas de gestión de alarmas de AMS Accelerate a una EC2 instancia de Amazon gestionada por CloudFormation:

```
Type: AWS::EC2::Instance
Properties:
 InstanceType: "t3.micro"

 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

El siguiente es un ejemplo de cómo puede aplicar las etiquetas de administración de alarmas de AMS Accelerate a un grupo de Auto Scaling administrado por CloudFormation. Tenga en cuenta que el grupo Auto Scaling propagará sus etiquetas a EC2 las instancias de Amazon que cree:

```
Type: AWS::AutoScaling::AutoScalingGroup
Properties:
 AutoScalingGroupName: "TestASG"

 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

## Acelera las etiquetas con Terraform

> **Note**
>
> Asegúrese de haber configurado Resource Tagger en modo de solo lectura antes de aplicar las etiquetas; de lo contrario CloudFormation, Resource Tagger podría modificar las etiquetas

en función del perfil de configuración. Para obtener información sobre cómo configurar Resource Tagger en modo de solo lectura y directrices sobre cómo proporcionar sus propias etiquetas, consulte. Acelere las etiquetas sin el etiquetador de recursos

Para obtener una descripción de cómo administrar las etiquetas de recursos con Terraform, consulte la documentación de Terraform sobre el etiquetado de recursos.

A continuación, se muestra un ejemplo de cómo aplicar las etiquetas de gestión de alarmas de AMS Accelerate a una EC2 instancia de Amazon gestionada por Terraform.

```
resource "aws_instance" "test_linux_instance" {
     # ...ami and other properties...

     instance_type = "t3.micro"

     tags = {
       "aws:rt:ams-monitoring-policy" = "ams-monitored"
       "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
     }
   }
```

El siguiente es un ejemplo de cómo puede aplicar etiquetas de administración de alarmas AMS a un grupo de Auto Scaling administrado por Terraform. Tenga en cuenta que el grupo Auto Scaling propaga sus etiquetas a las EC2 instancias que crea:

```
 resource "aws_autoscaling_group" "test_asg" {
 name = "terraform-test"
 # ...other properties...

 tags = {
   "aws:rt:ams-monitoring-policy" = "ams-monitored"
   "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
 }
}
```

## Perfiles de configuración de Accelerate Alarm Manager

Cuando su cuenta se incorpora a AMS Accelerate, se implementan en su cuenta dos documentos JSON, denominados perfiles de configuración AWS AppConfig (consulte Qué es AWS AppConfig).

Ambos documentos de perfil se encuentran en la aplicación Alarm Manager y en el entorno de infraestructura AMS Accelerate.

Temas


- Perfil de configuración de Accelerate: monitoreo
- Perfil de configuración de Accelerate: sustitución de pseudoparámetros
- Ejemplos de configuración de alarmas de Acelerate
- Visualización de la configuración de Accelerate Alarm Manager
- Cambiar la configuración de alarmas de Accelerate
- Modificación de la configuración predeterminada de la alarma Accelerate
- Implementación: acelere los cambios de configuración de alarmas
- Revertir Acelera los cambios de alarma
- Retener alarmas de Accelerate
- Desactivación de la configuración de alarma Accelerate predeterminada


## Perfil de configuración de Accelerate: monitoreo

Tanto el documento de perfil de configuración predeterminado como el documento de perfil de configuración de personalización siguen la misma estructura:

```
{
  "<ResourceType>": {
      "<ConfigurationID>": {
          "Enabled": true,

          "Tag": {
              "Key": "...",
              "Value": "..."
          },
          "AlarmDefinition": {
              ...
          }
      },
      "<ConfigurationID>": {
          ...
      }
  },
  "<ResourceType>": {
```

```
        ...
    }
}
```

- ResourceType: Esta clave debe ser una de las siguientes cadenas admitidas. La configuración de este objeto JSON se referirá únicamente al tipo de AWS recurso especificado. Tipos de recursos admitidos:

```
AWS::EC2::Instance
AWS::EC2::Instance::Disk
AWS::RDS::DBInstance
AWS::Elasticsearch::Domain
AWS::OpenSearch::Domain
AWS::Redshift::Cluster
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::ElasticLoadBalancingV2::LoadBalancer::TargetGroup
AWS::ElasticLoadBalancing::LoadBalancer
AWS::FSx::FileSystem::ONTAP
AWS::FSx::FileSystem::ONTAP::Volume
AWS::FSx::FileSystem::Windows
AWS::EFS::FileSystem
AWS::EC2::NatGateway
AWS::EC2::VPNConnection
```

- ID de configuración: esta clave debe ser única en el perfil y debe tener un nombre exclusivo para el siguiente bloque de configuración. Si especifica un ID de configuración en el perfil de personalización que sea igual al especificado en el perfil predeterminado, se aplicará el bloque de configuración definido en el perfil de personalización.
  - Habilitado: (opcional, default=true) Especifique si el bloque de configuración entrará en vigor. Establézcalo en false para deshabilitar un bloque de configuración. Un bloque de configuración deshabilitado se comporta como si no estuviera presente en el perfil.
  - Etiqueta: especifique la etiqueta a la que se aplica esta definición de alarma. A cualquier recurso (del tipo de recurso adecuado) que tenga esta clave y valor de etiqueta se le creará una CloudWatch alarma con la definición dada. Este campo es un objeto JSON con los siguientes campos:
    - Clave: la clave de la etiqueta que debe coincidir. Ten en cuenta que si utilizas Resource Tagger para aplicar las etiquetas al recurso, la clave de la etiqueta siempre empezará por ams:rt:.
    - Valor: el valor de la etiqueta que debe coincidir.

- AlarmDefinition: define la alarma que se va a crear. Se trata de un objeto JSON cuyos campos se pasan tal cual a la llamada a la CloudWatch `PutMetricAlarm` API (con la excepción de los pseudoparámetros; para obtener más información, consulte[Perfil de configuración de Accelerate: sustitución de pseudoparámetros](#)). Para obtener información sobre los campos que son obligatorios, consulta la PutMetricAlarmdocumentación.

  OR

  CompositeAlarmDefinition: Define la alarma compuesta que se va a crear. Al crear una alarma compuesta, se especifica una expresión de regla para la alarma que tiene en cuenta el estado de alarma de otras alarmas que se hayan creado. Se trata de un objeto JSON cuyos campos se pasan tal cual a. `CloudWatchPutCompositeAlarm` La alarma compuesta entra en estado ALARM solo si se cumplen todas las condiciones de la regla. Las alarmas especificadas en la expresión de regla de una alarma compuesta pueden incluir alarmas de métricas y otras alarmas compuestas. Para obtener información sobre qué campos son obligatorios, consulta la PutCompositeAlarmdocumentación.

  Ambas opciones proporcionan los siguientes campos:

  - AlarmName: especifique el nombre de la alarma que desea crear para el recurso. Este campo tiene todas las mismas reglas que las especificadas en la PutMetricAlarmdocumentación; sin embargo, dado que el nombre de la alarma debe ser único en una región, el administrador de alarmas tiene un requisito adicional: debe especificar el pseudoparámetro identificador único en el nombre de la alarma (de lo contrario, Alarm Manager añade el identificador único del recurso al principio del nombre de la alarma). Por ejemplo, para el tipo de AWS::EC2::Instancerecurso, debe especificarlo `${EC2::InstanceId}` en el nombre de la alarma o se añadirá implícitamente al principio del nombre de la alarma. Para ver la lista de identificadores, consulte. [Perfil de configuración de Accelerate: sustitución de pseudoparámetros](#)

    Todos los demás campos son los que se especifican en la documentación PutMetricAlarmo en la PutCompositeAlarmdocumentación.

  - AlarmRule: especifique qué otras alarmas se van a evaluar para determinar el estado de esta alarma compuesta. Para cada alarma a la que haga referencia, debe existir CloudWatch o especificarse en el perfil de configuración de Alarm Manager de su cuenta.

> **Important**
>
> Puede especificarlo CompositeAlarmDefinitionen el documento de configuración de Alarm Manager AlarmDefinitiono en él, pero no se pueden usar al mismo tiempo.

En el siguiente ejemplo, el sistema crea una alarma cuando dos alarmas métricas especificadas superan su umbral:

```
{
  "AWS::EC2::Instance": {
    "LinuxResourceAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:mylinuxinstance",
        "Value": "true"
      },
      "CompositeAlarmDefinition": {
        "AlarmName": "${EC2::InstanceId} Resource Usage High",
        "AlarmDescription": "Alarm when a linux EC2 instance is using too much CPU and
 too much Disk",
        "AlarmRule": "ALARM(\"${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}\") AND ALARM(\"${EC2::InstanceId}: CPU Too High\")"
      }
    }
  }
}
```

> **Important**
>
> Cuando Alarm Manager no puede crear o eliminar una alarma debido a una configuración defectuosa, envía la notificación al tema de SNS Direct-Customer-Alerts. Se llama a esta alarma. AlarmDependencyError
> Le recomendamos encarecidamente que confirme su suscripción a este tema de SNS. Para recibir los mensajes publicados sobre un tema, debe suscribir un punto final al tema. Para obtener más información, consulte el paso 1: Crear un tema.

> **Note**
>
> Cuando se crean las alarmas de detección de anomalías, Alarm Manager crea automáticamente los modelos de detección de anomalías necesarios para las métricas especificadas. Cuando se eliminan las alarmas de detección de anomalías, Alarm Manager no elimina los modelos de detección de anomalías asociados.
> Amazon CloudWatch limita el número de modelos de detección de anomalías que puedes tener en una AWS región determinada. Si superas la cuota de modelos, Alarm Manager no creará nuevas alarmas de detección de anomalías. Debe eliminar los modelos no utilizados o ponerse en contacto con su socio de AMS para solicitar un aumento del límite.
> Muchas de las definiciones de alarma básicas proporcionadas por AMS Accelerate incluyen como objetivo el tema del SNS, el tema del MMS. Se utiliza en el servicio de monitorización AMS Accelerate y es el mecanismo de transporte para que las notificaciones de alarma lleguen a AMS Accelerate. No especifique MMS-Topic como objetivo para ninguna alarma que no sea la proporcionada en la línea de base (ni anule las mismas), ya que el servicio ignora las alarmas desconocidas. Esto no hace que AMS Accelerate actúe sobre sus alarmas personalizadas.

## Perfil de configuración de Accelerate: sustitución de pseudoparámetros

En cualquiera de los perfiles de configuración, puede especificar pseudoparámetros que se sustituirán in situ de la siguiente manera:

- Global: en cualquier parte del perfil:
  - $ {AWS::AccountId}: reemplazado por tu ID AWS de cuenta
  - $ {AWS::Partition}: se reemplaza por la partición en la que se encuentra Región de AWS el recurso (esto es «aws» para la mayoría Regiones de AWS); para obtener más información, consulte la entrada correspondiente a la partición en la referencia del ARN.
  - $ {AWS::Region}: se sustituye por el nombre de la región en la que se despliega el recurso (por ejemplo, us-east-1)
- En un bloque de tipos AWS::EC2::Instancede recurso:
  - $ {EC2::InstanceId}: (identificador) reemplazado por el ID de instancia de su instancia de Amazon EC2.
  - $ {EC2::InstanceName}: reemplazado por el nombre de su instancia de Amazon EC2. Si el nombre de la instancia no está definido, se sustituye por el ID de la instancia de Amazon EC2.

- En un bloque de tipo de recurso AWS::EC2::Instance: :Disk:
  - $ {EC2::InstanceId}: (identificador) Se ha sustituido por el ID de instancia de su instancia de Amazon EC2.
  - $ {EC2::InstanceName}: se ha sustituido por el nombre de la instancia de Amazon EC2. Si el nombre de la instancia no está definido, se sustituye por el ID de la instancia de Amazon EC2.
  - $ {EC2: :Disk: :Device}: se reemplaza por el nombre del disco. (Solo para Linux, en instancias administradas por el CloudWatch agente).
  - $ {EC2: :Disk::FSType}: reemplazado por el tipo de sistema de archivos del disco. (Solo para Linux, en instancias administradas por). CloudWatchAgent
  - $ {EC2: :Disk: :Path}: se ha sustituido por la ruta del disco. (Solo para Windows, esta es la etiqueta de la unidad (por ejemplo, c:/), solo en una instancia administrada por el CloudWatch agente).
  - $ {EC2: :Disk: :UUID}: (identificador) Sustituido por un UUID generado que identifique el disco de forma exclusiva, debe especificarse en el nombre de la alarma, ya que una alarma por tipo de AWS::EC2::Instance::Disk recurso creará una alarma por volumen. Al especificar $ {EC2: :Disk: :UUID} se mantiene la exclusividad de los nombres de las alarmas.
- En un bloque de tipos de recurso: AWS::OpenSearch::Domain
  - $ {OpenSearch::DomainName}: (identificador) reemplazado por el nombre de tu OpenSearch dominio.
- En un bloque AWS::Elasticsearch::Domainde tipo de recurso:
  - $ {Elasticsearch::DomainName}: (identificador) reemplazado por el nombre de tu dominio de Elasticsearch.
- En un bloque de tipo de recurso AWS::ElasticLoadBalancing::LoadBalancer:
  - $ {ElasticLoadBalancing:LoadBalancer: :Name}: (identificador) reemplazado por el nombre de tu Load Balancer V1.
- En un bloque de tipo AWS::ElasticLoadBalancingV2::LoadBalancerde recurso:
  - $ {ElasticLoadBalancingV2::LoadBalancer: :Arn}: reemplazado por el ARN de tu Load Balancer V2.
  - $ {ElasticLoadBalancingV2::LoadBalancer}: reemplazado por el ARN de tu Load Balancer V2.
  - $ {ElasticLoadBalancingV2:LoadBalancer: :Name}: (identificador) reemplazado por el nombre de tu Load Balancer V2.
  - $ {ElasticLoadBalancingV2::LoadBalancer::FullName}: reemplazado por el nombre completo de tu Load Balancer V2.

- En un bloque de tipo TargetGroup de recurso AWS::ElasticLoadBalancingV2::LoadBalancer::
  - $ {ElasticLoadBalancingV2::TargetGroup::FullName}: (identificador) reemplazado por el nombre del grupo objetivo de tu Load Balancer V2.
  - $ {ElasticLoadBalancingV2:TargetGroup: :UUID}: (identificador) reemplazado por un UUID generado para tu Load Balancer de V2.
  - $ {ElasticLoadBalancingV2:::LoadBalancer:FullName}: se ha sustituido por el nombre completo de tu Load Balancer V2.
- En un bloque AWS::EC2::NatGatewayde tipo de recurso:
  - $ {NatGateway::NatGatewayId}: (identificador) reemplazado por el ID de la puerta de enlace NAT.
- En un bloque de tipo de DBInstance recurso de AWS: :RDS:
  - $ {RDS:: DBInstance Identifier}: (identifier) reemplazado por el identificador de su instancia de base de datos de RDS.
- En un bloque de tipo AWS::Redshift::Clusterde recurso:
  - $ {Redshift::ClusterIdentifier}: (identifier) reemplazado por tu identificador de clúster de Redshift.
- En un bloque de tipo de VPNConnection recurso de AWS: :EC2::
  - $ {AWS::EC2::VpnConnectionId}: (identificador) reemplazado por su ID de VPN.
- En un bloque AWS::EFS::FileSystemde tipo de recurso:
  - $ {EFS::FileSystemId}: (identificador) Sustituido por el ID del sistema de archivos de su sistema de archivos EFS.
- En un bloque de tipo de recurso AWS::FSx::FileSystem: :ONTAP:
  - $ {FSx::FileSystemId}: (identificador) Sustituido por el ID del sistema de archivos de su sistema de archivos FSX.
  - $ {FSx:: :Throughput}FileSystem: se ha sustituido por el rendimiento de su sistema de archivos FSX.
  - $ {FSx::: :Iops}FileSystem: se ha sustituido por las IOPS del sistema de archivos FSX.
- En un bloque de tipo de recurso AWS::FSx::FileSystem: :ONTAP: :Volume:
  - $ {FSx::FileSystemId}: (identificador) Sustituido por el ID del sistema de archivos de su sistema de archivos FSX.
  - $ {FSx: :ONTAP::VolumeId}: (identificador) Sustituido por el ID del volumen.
- En un bloque de AWS::FSx::FileSystemtipos de recursos: :Windows:

- $ {FSx::FileSystemId}: (identificador) Sustituido por el ID del sistema de archivos de su sistema de archivos FSX.
- $ {FSx:: :Throughput}FileSystem: se ha sustituido por el rendimiento de su sistema de archivos FSX.

> **Note**
>
> Todos los parámetros marcados con un identificador se utilizan como prefijo para el nombre de las alarmas creadas, a menos que especifique ese identificador en el nombre de la alarma.

## Ejemplos de configuración de alarmas de Acelerate

En el siguiente ejemplo, el sistema crea una alarma para cada disco conectado a la instancia de Linux correspondiente.

```
{
    "AWS::EC2::Instance::Disk": {
        "LinuxDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mylinuxinstance",
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "disk_used_percent",
                "Namespace": "CWAgent",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
                        "Name": "device",
                        "Value": "${EC2::Disk::Device}"
                    },
                    {
                        "Name": "fstype",
                        "Value": "${EC2::Disk::FSType}"
                    }
```

```
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
}
```

En el siguiente ejemplo, el sistema crea una alarma para cada disco conectado a la instancia de Windows correspondiente.

```
{
     "AWS::EC2::Instance::Disk": {
        "WindowsDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mywindowsinstance",
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "LogicalDisk % Free Space",
                "Namespace": "CWAgent",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
                        "Name": "objectname",
                        "Value": "LogicalDisk"
                    },
                    {
                        "Name": "instance",
                        "Value": "${EC2::Disk::Path}"
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
}
```

## Visualización de la configuración de Accelerate Alarm Manager

Tanto las AMSManagedalarmas como las CustomerManagedAlarmspuede revisar GetConfiguration. AppConfig

El siguiente es un ejemplo de la `GetConfiguration` llamada:

```
aws appconfig get-configuration --application AMSAlarmManager --environment
 AMSInfrastructure --configuration AMSManagedAlarms --client-id
      any-string outfile.json
```

- Aplicación: esta AppConfig es la unidad lógica para proporcionar capacidades; para el administrador de alarmas, es `AMSAlarmManager`
- Medio ambiente: este es el AMSInfrastructure entorno
- Configuración: para ver las alarmas de referencia de AMS Accelerate, el valor es`AMSManagedAlarms`; para ver las definiciones de alarmas del cliente, la configuración es `CustomerManagedAlarms`
- ID de cliente: se trata de un identificador de instancia de aplicación único, que puede ser cualquier cadena
- Las definiciones de alarmas se pueden ver en el archivo de salida especificado, que en este caso es `outfile.json`

Puede ver qué versión de la configuración está implementada en su cuenta consultando las implementaciones anteriores en el AMSInfrastructure entorno.

## Cambiar la configuración de alarmas de Accelerate

Para añadir o actualizar nuevas definiciones de alarmas, puede implementar el documento Uso CloudFormation para implementar Accelerate los cambios de configuración de configuración o invocar la CreateHostedConfigurationVersionAPI.

Se trata de un comando de línea de comandos de Linux que genera el valor del parámetro en base64, que es lo que espera el comando AppConfig CLI. Para obtener más información, consulte la AWS CLI documentación, Binary/Blob (objeto binario grande).

Por ejemplo:

```
aws appconfig create-hosted-configuration-version --application-id application-id --
configuration-profile-id configuration-profile-id --content base64-string
```

```
      --content-type application/json
```

- ID de aplicación: ID de la aplicación AMS AlarmManager; puede averiguarlo con la llamada a la API. ListApplications
- ID del perfil de configuración: ID de la configuración CustomerManagedAlarms; puede averiguarlo con la llamada a la ListConfigurationProfilesAPI.
- Contenido: cadena en base64 del contenido, que se creará creando un documento y codificándolo en base64: cat alarms-v2.json | base64 (consulte Binary/Blob (objeto binario grande)).

  Tipo de contenido: tipo MIME, ya que las definiciones de las alarmas están escritas en JSON. `application/json`

> **Important**
>
> Limite el acceso a las acciones de la StopDeploymentAPI StartDeploymenty a las de la API a usuarios de confianza que entiendan las responsabilidades y las consecuencias de implementar una nueva configuración en sus destinos.

Para obtener más información sobre cómo utilizar las AppConfig funciones de AWS para crear e implementar una configuración, consulte Trabajar con AWS AppConfig.

## Modificación de la configuración predeterminada de la alarma Accelerate

Si bien no puede modificar el perfil de configuración predeterminado, puede reemplazar los valores predeterminados especificando un bloque de configuración en su perfil de personalización con el mismo ID de configuración que el bloque de configuración predeterminado. Si lo hace, todo el bloque de configuración sobrescribe el bloque de configuración predeterminado al que se debe aplicar la configuración de etiquetado.

Por ejemplo, considere el siguiente perfil de configuración predeterminado:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
```

```
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    }
                ],
                "Threshold": 5,
                ...
            }
        }
    }
}
```

Para cambiar el umbral de esta alarma a 10, debe proporcionar la definición completa de la alarma, no solo las partes que desee cambiar. Por ejemplo, puede proporcionar el siguiente perfil de personalización:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    }
                ],
                "Threshold": 10,
                ...
```

```
            }
        }
    }
}
```

> **Important**
>
> Recuerde implementar los cambios de configuración después de haberlos realizado. En SSM AppConfig, debe implementar una nueva versión de la configuración después de crearla.

## Implementación: acelere los cambios de configuración de alarmas

Una vez finalizada la personalización, debe implementarla, ya sea con AppConfig o CloudFormation.

Temas

- Uso AppConfig para implementar Accelerate los cambios de configuración de alarmas
- Uso CloudFormation para implementar Accelerate los cambios de configuración

### Uso AppConfig para implementar Accelerate los cambios de configuración de alarmas

Una vez completada la personalización, AppConfig utilícela para implementar los cambios con StartDeployment.

```
  aws appconfig start-deployment --application-id application_id
   --environment-id environment_id Vdeployment-strategy-id
   deployment_strategy_id --configuration-profile-id configuration_profile_id --
configuration-version 1
```

- ID de aplicación: identificador de la aplicación`AMSAlarmManager`, lo puedes encontrar con la llamada a la ListApplicationsAPI.
- ID de entorno: puedes encontrarlo en la llamada a la ListEnvironmentsAPI.
- ID de estrategia de despliegue: puedes encontrarlo en la llamada a la ListDeploymentStrategiesAPI.
- ID del perfil de configuración: ID de`CustomerManagedAlarms`; puede encontrarlo con la llamada a la ListConfigurationProfilesAPI.
- Versión de configuración: la versión del perfil de configuración que se va a implementar.

> **Important**
>
> Alarm Manager aplica las definiciones de alarma tal como se especifican en los perfiles de configuración. Cualquier modificación manual que realice con el Consola de administración de AWS CloudWatch CLI/SDK en las CloudWatch alarmas se revierte automáticamente, así que asegúrese de que los cambios estén definidos a través del Administrador de alarmas. Para saber qué alarmas crea el administrador de alarmas, puede buscar la `ams:alarm-manager:managed` etiqueta con el valor. `true`
> Limite el acceso a las acciones de la StopDeploymentAPI StartDeployment y a las de la API a usuarios de confianza que entiendan las responsabilidades y las consecuencias de implementar una nueva configuración en sus objetivos.

Para obtener más información sobre cómo utilizar las AppConfig funciones de AWS para crear e implementar una configuración, consulte la AppConfig documentación de AWS.

Uso CloudFormation para implementar Accelerate los cambios de configuración

Si desea implementar su perfil de `CustomerManagedAlarms` configuración mediante CloudFormation, puede usar las siguientes CloudFormation plantillas. Coloque la configuración JSON que desee en el `AMSAlarmManagerConfigurationVersion.Content` campo.

Al implementar las plantillas en una CloudFormation pila o conjunto de pilas, la implementación del `AMSResourceTaggerDeployment` recurso fallará si no se ha seguido el formato JSON requerido para la configuración. Consulte Perfil de configuración de Accelerate: monitoreo para obtener más información sobre el formato esperado.

Para obtener ayuda sobre la implementación de estas plantillas como una CloudFormation pila o conjunto de pilas, consulte la CloudFormation documentación de AWS correspondiente a continuación:

- Creación de una pila en la CloudFormation consola de AWS
- Creación de una pila con AWS CLI
- Crear un conjunto de pilas

> **Note**
>
> Si despliega una versión de configuración mediante una de estas plantillas y, posteriormente, elimina la CloudFormation pila o el conjunto de pilas, la versión de configuración de la plantilla permanecerá como la versión implementada actualmente y no se realizará ningún despliegue adicional. Si desea volver a la configuración predeterminada, tendrá que implementar manualmente una configuración vacía (es decir, solo {}) o actualizar la pila a una configuración vacía, en lugar de eliminar la pila.

JSON

```
{
  "Description": "Custom configuration for the AMS Alarm Manager.",
  "Resources": {
    "AMSAlarmManagerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "Content": "{}",
        "ContentType": "application/json"
      }
    },
    "AMSAlarmManagerDeployment": {
      "Type": "AWS::AppConfig::Deployment",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "ConfigurationVersion": {
          "Ref": "AMSAlarmManagerConfigurationVersion"
        },
```

```
        "DeploymentStrategyId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-Deployment-StrategyID"
        },
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-EnvironmentId"
        }
      }
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Alarm Manager.
Resources:
  AMSAlarmManagerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      Content: |
        {

        }
      ContentType: application/json
  AMSAlarmManagerDeployment:
    Type: AWS::AppConfig::Deployment
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      ConfigurationVersion:
        !Ref AMSAlarmManagerConfigurationVersion
      DeploymentStrategyId:
        !ImportValue AMS-Alarm-Manager-Configuration-Deployment-StrategyID
      EnvironmentId:
        !ImportValue AMS-Alarm-Manager-Configuration-EnvironmentId
```

## Revertir Acelera los cambios de alarma

Puede revertir las definiciones de alarmas mediante el mismo mecanismo de despliegue especificando una versión anterior del perfil de configuración y ejecutándola StartDeployment.

## Retener alarmas de Accelerate

Cuando se eliminan los recursos supervisados por AMS, Alarm Manager elimina automáticamente cualquier alarma creada por Alarm Manager para esos recursos. Si necesita conservar determinadas alarmas con fines de auditoría, cumplimiento o históricos, utilice la función de retención de etiquetas de Alarm Manager.

Para conservar una alarma incluso después de eliminar el recurso supervisado, añada una `"ams:alarm-manager:retain"` etiqueta a la configuración personalizada de la alarma, como se muestra en el siguiente ejemplo.

```
{
  "AWS::EC2::Instance": {
    "AMSCpuAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:ams-monitoring-policy",
        "Value": "ams-monitored"
      },
      "AlarmDefinition": {
        "AlarmName": "${EC2::InstanceId}: CPU Too High",
        "AlarmDescription": "AMS Baseline Alarm for EC2 CPUUtilization",
        [...]
        "Tags": [
          {
            "Key": "ams:alarm-manager:retain",
            "Value": "true"
          }
        ]
      }
    }
  }
}
```

Alarm Manager no elimina automáticamente una alarma configurada con la `"ams:alarm-manager:retain"` etiqueta cuando finaliza el recurso monitoreado. La alarma retenida permanece activa CloudWatch indefinidamente hasta que la elimines manualmente mediante CloudWatch.

## Desactivación de la configuración de alarma Accelerate predeterminada

AMS Accelerate proporciona el perfil de configuración predeterminado de su cuenta en función de las alarmas de referencia. Sin embargo, esta configuración predeterminada se puede deshabilitar anulando cualquiera de las definiciones de alarma. Para deshabilitar una regla de configuración predeterminada, anule el ID de configuración de la regla en su perfil de configuración de personalización y especifique el campo habilitado con el valor false.

Por ejemplo, si la siguiente configuración estaba presente en el perfil de configuración predeterminado:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                ...
            }
        }
    }
```

Puede deshabilitar esta regla de etiquetado si incluye lo siguiente en su perfil de configuración de personalización:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": false
        }
    }
}
```

Para realizar estos cambios, se debe llamar a la CreateHostedConfigurationVersionAPI junto con el documento de perfil JSON (consulteCambiar la configuración de alarmas de Accelerate) y, posteriormente, se debe implementar (consulteImplementación: acelere los cambios de configuración de alarmas). Tenga en cuenta que, al crear la nueva versión de configuración, también debe incluir en el documento de perfil JSON todas las alarmas personalizadas creadas anteriormente que desee.

> **Important**
>
> Cuando AMS Accelerate actualiza el perfil de configuración predeterminado, no se calibra en función de las alarmas personalizadas configuradas, por lo que debe revisar los cambios en las alarmas predeterminadas cuando los anule en su perfil de configuración de personalización.

## Creación de CloudWatch alarmas adicionales para Accelerate

Puede crear CloudWatch alarmas adicionales para AMS Accelerate mediante CloudWatch métricas y alarmas personalizadas para EC2 instancias de Amazon.

Cree su script de monitoreo de aplicaciones y una métrica personalizada. Para obtener más información y acceder a scripts de ejemplo, consulte Supervisión de métricas de memoria y disco para instancias de Amazon EC2 Linux.

Los scripts de CloudWatch monitoreo para EC2 las instancias Amazon de Linux muestran cómo producir y consumir CloudWatch métricas personalizadas. Estos scripts Perl de muestra contienen un ejemplo totalmente funcional que informa sobre métricas de memoria, intercambio y utilización del espacio en disco de una instancia de Linux.

> **Important**
>
> AMS Accelerate no supervisa CloudWatch las alarmas que usted crea.

# Remediación automática de alertas por parte de AMS

Tras la verificación, AWS Managed Services (AMS) corrige automáticamente determinadas alertas según las condiciones y los procesos específicos que se describen en esta sección.

| Nombre de la alerta | Description (Descripción) | Umbrales | Action |
|---|---|---|---|
| Falló la comprobac | Posibles errores de hardware o un estado de fallo de la instancia. | El sistema ha detectado un estado de error al | La corrección automátic a de AMS valida primero si se puede acceder a la |

| Nombre de la alerta | Description (Descripción) | Umbrales | Action |
|---|---|---|---|
| ión de estado | | menos una vez en los últimos 15 minutos. | instancia. Si no se puede acceder a la instancia, se detiene y se reinicia. La parada y el inicio permiten que la instancia migre a un nuevo hardware subyacente. Para obtener más información, consulte la siguiente sección «Automatización de la corrección de errores en la comprobación de estado de EC2». |
| AMSLinuxDiskUsage | Se activa cuando se está agotando el espacio de disco utilizado en 1 punto de montaje (espacio designado en un volumen) de la instancia EC2. | El umbral supera el valor definido 6 veces en los últimos 30 minutos. | La corrección automática de AMS elimina primero los archivos temporales. Si esto no libera suficiente espacio en disco, amplía el volumen para evitar tiempos de inactividad si el volumen se llena. |
| AMSWindowsDiskUsage | Cuando se esté agotando el espacio de disco utilizado en 1 punto de montaje (espacio designado en un volumen) de la instancia EC2. | El umbral supera el valor definido 6 veces durante los últimos 30 minutos. | La corrección automática de AMS elimina primero los archivos temporales. Si esto no libera suficiente espacio en disco, amplía el volumen para evitar tiempos de inactividad si el volumen se llena. |

| Nombre de la alerta | Description (Descripción) | Umbrales | Action |
| --- | --- | --- | --- |
| RDS-EVENT-0089 | La instancia de base de datos ha consumido más del 90 % del almacenamiento asignado. | El almacenamiento está asignado en más del 90%. | La corrección automática de AMS valida primero que la base de datos esté en un estado modificable y disponible o que esté lleno de almacenamiento. A continuación, intenta aumentar el almacenamiento asignado, las IOPS y el rendimiento del almacenamiento mediante un conjunto de cambios. CloudFormation Si ya se ha detectado una desviación de la pila, recurre a la API de RDS para evitar el tiempo de inactividad.<br><br>Puede inhabilitar esta función añadiendo la siguiente etiqueta a la instancia de base de datos de RDS: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".` |

| Nombre de la alerta | Description (Descripción) | Umbrales | Action |
| --- | --- | --- | --- |
| RDS-EVENT-0007 | Se agotó el almacenamiento asignado a la instancia de base de datos. Para resolverlo, asigne almacenamiento adicional. | El almacenamiento está asignado al 100%. | La corrección automática de AMS valida primero que la base de datos esté en un estado modificable y disponible o que esté lleno de almacenamiento. A continuación, intenta aumentar el almacenamiento asignado, las IOPS y el rendimiento del almacenamiento mediante un conjunto de cambios. CloudFormation Si ya se ha detectado una desviación de la pila, recurre a la API de RDS para evitar el tiempo de inactividad.<br><br>Puede inhabilitar esta función añadiendo la siguiente etiqueta a la instancia de base de datos de RDS: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".` |

| Nombre de la alerta | Description (Descripción) | Umbrales | Action |
| --- | --- | --- | --- |
| RDS-EVENT-0224 | El almacenamiento asignado solicitado alcanza o supera el umbral de almacenamiento máximo configurado. | Se ha agotado el umbral de almacenamiento máximo de la instancia de base de datos o es superior o igual al almacenamiento asignado solicitado. | La corrección automática de AMS valida primero que la cantidad de almacenamiento de RDS solicitada supere el umbral máximo de almacenamiento. Si se confirma, AMS intenta aumentar el umbral máximo de almacenamiento en un 30% con un CloudFormation conjunto de cambios o directamente a la API de RDS si no se aprovisionan los recursos. CloudFormation<br><br>Puede inhabilitar esta función añadiendo la siguiente etiqueta a la instancia de base de datos de RDS: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".` |

| Nombre de la alerta | Description (Descripción) | Umbrales | Action |
| --- | --- | --- | --- |
| Capacidad de almacenamiento de RDS | Queda menos de 1 GB en el almacenamiento asignado a la instancia de base de datos. | El almacenamiento está asignado en un 99%. | La corrección automática de AMS valida primero que la base de datos esté en un estado modificable y disponible o que esté lleno de almacenamiento. A continuación, intenta aumentar el almacenamiento asignado, las IOPS y el rendimiento del almacenamiento mediante un conjunto de cambios. CloudFormation Si ya se ha detectado una desviación de la pila, recurre a la API de RDS para evitar el tiempo de inactividad.<br><br>Puede inhabilitar esta función añadiendo la siguiente etiqueta a la instancia de base de datos de RDS: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".` |

| Nombre de la alerta | Description (Descripción) | Umbrales | Action |
| --- | --- | --- | --- |
| AMSFSXONTAPVolumeCapacityUtilization | El volumen de Amazon FSx for NetApp ONTAP ha consumido más del almacenamiento asignado por defecto (80%). | FSx para ONTAP, la utilización de la capacidad de volumen es superior al 80% durante dos horas (valor predeterminado). | La corrección automática de AMS primero valida que el estado del ciclo de vida del volumen se encuentra en un estado modificable y, a continuación, amplía el tamaño del volumen en un 10% y, al mismo tiempo, lo compara con la capacidad máxima del sistema de archivos. Si el sistema de archivos carece de capacidad de almacenamiento suficiente para la expansión del volumen, tanto el volumen como el sistema de archivos se expanden juntos. Esta expansión está limitada a un máximo de tres veces en un período de siete días. El límite máximo de almacenamiento al que se amplía AMS Automation es de 5120 GiB.<br><br>**Note**<br>Si el LUN iSCSI está configurado en la parte superior del |

| Nombre de la alerta | Description (Descripción) | Umbrales | Action |
| --- | --- | --- | --- |
| | | | volumen, amplíe el LUN iSCSI a nivel del sistema operativo. Para obtener más información, consulte ¿Por qué mi LUN FSx para ONTAP está en modo de solo lectura? |

## Fallo en la comprobación del estado de EC2: notas sobre la automatización de la remediación

Cómo funciona la corrección automática de AMS con problemas de error en la comprobación de estado de EC2:

- Si no se puede acceder a su instancia de Amazon EC2, debe detenerla y volver a iniciarla para poder migrarla a un nuevo hardware y recuperarla.
- Si la raíz del problema está en el sistema operativo (falta de dispositivos en fstab, el núcleo está dañado, etc.), la automatización no podrá recuperar la instancia.
- Si la instancia pertenece a un grupo de Auto Scaling, la automatización no realiza ninguna acción: la acción de AutoScalingGroup escalado reemplaza a la instancia.
- Si la instancia tiene habilitada la recuperación automática de EC2, la corrección no se lleva a cabo.

## Automatización de la corrección del uso de volúmenes de EC2

Cómo funciona la corrección automática de AWS Managed Services (AMS) con los problemas de uso de volúmenes de EC2:

- La automatización primero valida si la expansión del volumen es necesaria y si se puede realizar. Si la expansión se considera adecuada, la automatización puede aumentar la capacidad de volumen. Este proceso automatizado equilibra la necesidad de crecimiento con una expansión limitada y controlada.
- Antes de ampliar un volumen, la automatización realiza tareas de limpieza (Windows: Disk Cleaner, Linux: Logrotate y eliminación del registro del agente Simple Service Manager) en la instancia para intentar liberar espacio.

> **Note**
>
> Las tareas de limpieza no se ejecutan en las instancias de la familia EC2 «T» porque dependen de los créditos de la CPU para seguir funcionando.

- En Linux, la automatización solo admite la ampliación de los sistemas de archivos tipo A EXT4 y EXT2 EXT3 XFS.
- En Windows, la automatización solo es compatible con el Sistema de archivos de nueva tecnología (NTFS) y el Sistema de archivos resiliente (ReFS).
- La automatización no amplía los volúmenes que forman parte del administrador de volúmenes lógicos (LVM) o de una matriz RAID.
- La automatización no amplía los volúmenes del almacén de instancias.
- La automatización no actúa si el volumen afectado ya es superior a 2 TiB.
- La expansión mediante la automatización está limitada a un máximo de tres veces por semana y cinco veces en total durante la vida útil del sistema.
- La automatización no amplía el volumen si la expansión anterior se produjo en las últimas seis horas.

Cuando estas reglas impiden que la automatización tome medidas, AMS se pondrá en contacto con usted mediante una solicitud de servicio saliente para determinar las siguientes acciones a tomar.

## Automatización de la corrección de eventos de bajo almacenamiento en Amazon RDS

Cómo funciona la corrección automática de AWS Managed Services (AMS) con los problemas de eventos de bajo almacenamiento de Amazon RDS:

- Antes de intentar ampliar el almacenamiento de la instancia de Amazon RDS, la automatización realiza varias comprobaciones para garantizar que la instancia de Amazon RDS se encuentra en un estado modificable y disponible, o con almacenamiento lleno.
- Cuando se detecta CloudFormation una desviación de pila, la corrección se realiza a través de la API de Amazon RDS.
- Según el evento desencadenante, la corrección modifica las propiedades`MaxAllocatedStorage`,, o. `AllocatedStorage` `Iops` `StorageThroughput` Las demás propiedades de la instancia de Amazon RDS no se modifican. Para obtener más información, consulte Configuración de las instancias de base de datos.
- La acción de corrección no se ejecuta en los siguientes escenarios:
  - El estado de la instancia de Amazon RDS no es «disponible» ni «lleno de almacenamiento».
  - El almacenamiento de instancias de Amazon RDS no se puede modificar actualmente (por ejemplo, si el almacenamiento se ha modificado en las últimas seis horas).
  - La instancia de Amazon RDS tiene activado el almacenamiento con autoscalamiento.
- La corrección se limita a una expansión cada seis horas y a no más de tres expansiones en un período continuo de catorce días.
- Cuando se producen estas situaciones, AMS se pone en contacto con usted para informarle sobre un incidente saliente para determinar las siguientes medidas.

## Automatización de la remediación de volúmenes y capacidad de ONTAP

Cómo funciona la corrección automática de AWS Managed Services (AMS) con los problemas de capacidad de volumen de ONTAP:

- Antes de ampliar el volumen, la automatización valida que el estado del ciclo de vida del volumen se encuentre en un estado modificable.
- La automatización amplía el tamaño del volumen en un 10% y, al mismo tiempo, lo compara con la capacidad máxima del sistema de archivos.
- Si el sistema de archivos no tiene suficiente capacidad de almacenamiento para soportar la expansión del volumen, se ampliarán tanto el volumen como la capacidad del sistema de archivos.
- La corrección está limitada a no más de tres actualizaciones en un período de siete días.
- El límite máximo de almacenamiento al que se amplía AMS Automation es de 5120 GiB.
- Si el LUN iSCSI está configurado en la parte superior del volumen, debe expandir manualmente el LUN iSCSI en el nivel del sistema operativo una vez finalizada la corrección automática. Para

obtener más información, consulte ¿Por qué mi LUN FSx para ONTAP está en modo de solo lectura?

# Uso de Amazon EventBridge Managed Rules en AMS

AMS Accelerate utiliza Amazon EventBridge Managed Rules. Una regla gestionada es un tipo de regla único que está directamente vinculada a AMS. Estas reglas coinciden con los eventos entrantes y los envían a los destinos para su procesamiento. Las reglas administradas están predefinidas por AMS e incluyen los patrones de eventos que el servicio requiere para administrar las cuentas de los clientes y, a menos que se defina lo contrario, solo el servicio propietario puede utilizar estas reglas administradas.

Las reglas gestionadas de AMS Accelerate están vinculadas al principio `events.managedservices.amazonaws.com` del servicio. Estas reglas gestionadas se gestionan a través de la función `AWSServiceRoleForManagedServices_Events`vinculada al servicio. Para eliminar estas reglas, se requiere una confirmación especial por parte del cliente. Para obtener más información, consulte Eliminar reglas administradas para AMS.

Para obtener más información sobre las reglas, consulta Reglas en la Guía del EventBridge usuario de Amazon.

## Amazon EventBridge Managed Rules implementadas por AMS

Reglas EventBridge gestionadas por Amazon

| Nombre de la regla | Description (Descripción) | Definición |
|---|---|---|
| AmsAccessRolesRule | Esta regla tiene en cuenta las modificaciones en las funciones y políticas específicas de AMS Accelerate. | { "source": ["aws.iam"], "detail-type": ["AWS API Call via CloudTrail"], "detail": { "eventName": [ "DeleteRole", "DeletePolicy", "CreatePolicyVersion", "AttachRolePolicy", "DetachRolePolicy" ], |

| Nombre de la regla | Description (Descripción) | Definición |
| --- | --- | --- |

```
     "requestParameters": {
        "$or": [
            {
                "roleName": [
                    "ams-access-admin",
                    "ams-access-admin-operations",
                    "ams-access-operations",
                    "ams-access-read-only",
                    "ams-access-security-analyst",
                    "ams-access-security-analyst-
read-only"
                ]
            },
            {
                "policyArn": [
                    "arn:*:iam::*:policy/ams-ac
cess-allow-pass-role",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-cloudshell-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-operations-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-update-iam-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-ssr-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-read-only-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-extended-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-admin-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-admin-operations-policy"
                ]
            },
         ]
       },
   },
}
```

| Nombre de la regla | Description (Descripción) | Definición |
| --- | --- | --- |
| | | |
| AMSCoreRegla | Esta regla reenvía los AWS Config CloudWatch eventos de Amazon a los servicios de corrección y supervisión de AMS Config, respectivamente. Los AWS Config eventos se crean y se resuelven. AWS Systems Manager OpsItems Las CloudWatch alarmas del monitor de CloudWatch eventos de Amazon. | <pre>{<br>    {<br>        "source": ["aws.config", "aws.cloudwatch"],<br>        "detail-type": ["Config Rules Compliance Change", "CloudWatch Alarm State Change"],<br>    }<br>}</pre> |

## Creación de reglas gestionadas para AMS

No necesitas crear manualmente Amazon EventBridge Managed Rules. Cuando te incorporas a AMS en la consola de AWS administración AWS CLI, la o la AWS API, AMS las crea automáticamente.

## Edición de reglas gestionadas para AMS

AMS no permite editar las reglas gestionadas. AMS predefine el nombre y el patrón de eventos de cada regla gestionada.

## Eliminar reglas administradas para AMS

No es necesario eliminar manualmente las reglas gestionadas. Cuando te desconectas de AMS en la consola AWS de administración, en la AWS CLI AWS API o en la consola, AMS limpia los recursos y elimina automáticamente todas las reglas gestionadas que son propiedad de AMS.

En caso de que AMS no elimine las reglas gestionadas durante la desconexión, también puedes utilizar la EventBridge consola de Amazon, la AWS CLI o la AWS API para eliminar manualmente las reglas gestionadas. Para ello, primero debes abandonar AMS y forzar la eliminación de las reglas gestionadas.

# Remediador de confianza en AMS

Trusted Remediator es una solución de AWS Managed Services que automatiza la corrección y las AWS Trusted Advisorrecomendaciones AWS Security Hub CSPM. AWS Compute Optimizer Trusted Remediator crea recomendaciones cuando Security Hub Trusted Advisor, CSPM y Compute Optimizer le indican oportunidades para reducir costos, mejorar la disponibilidad del sistema, optimizar el rendimiento o cerrar brechas de seguridad. Cuentas de AWS Con Trusted Remediator, puede abordar estas recomendaciones de seguridad, rendimiento, optimización de costes, tolerancia a fallos y límites de servicio de una manera segura y estandarizada que utilice las mejores prácticas establecidas. Trusted Remediator le permite configurar una solución de remediación y se ejecuta automáticamente según un cronograma que usted cree, lo que simplifica el proceso de remediación. Este enfoque simplificado aborda los problemas de manera coherente y eficiente y sin intervención manual.

## Ventajas clave de Trusted Remediator

Los principales beneficios de Trusted Remediator son los siguientes:

- Mejora de la seguridad, el rendimiento y la optimización de los costes: Trusted Remediator le ayuda a mejorar la seguridad general de sus cuentas, a optimizar la utilización de los recursos y a reducir los costes operativos.
- Instalación y configuración de autoservicio: puede configurar Trusted Remediator para que se ajuste a sus requisitos y preferencias.
- Trusted Advisor Comprobaciones automatizadas, controles CSPM de Security Hub y corrección de AWS Compute Optimizer recomendaciones: tras la configuración, Trusted Remediator ejecuta automáticamente las acciones de corrección para las comprobaciones seleccionadas. Esta automatización elimina la necesidad de intervención manual.
- Implementación de las mejores prácticas: las acciones correctivas se basan en las mejores prácticas establecidas, por lo que los problemas se abordan de manera estandarizada y eficaz.
- Ejecución programada: puede elegir el programa de remediación que se adapte a sus day-to-day flujos de trabajo operativos.

Trusted Remediator le permite abordar de forma proactiva los problemas identificados en sus AWS entornos, lo que le ayuda a cumplir con las mejores prácticas y a mantener una infraestructura de nube segura, rentable y de alto rendimiento.

## Cómo funciona Trusted Remediator

A continuación se muestra un ejemplo del flujo de trabajo de Trusted Remediator:

Trusted Remediator evalúa las recomendaciones de Security Hub Trusted Advisor, CSPM y Compute Optimizer para usted y las crea. Cuentas de AWS AWS Systems Manager OpsItems OpsCenter A continuación, puede utilizar los documentos de automatización de Trusted Remediator para corregir los problemas de forma automática o manual. OpsItems Los siguientes son detalles de cada tipo de remediación:

- Corrección automatizada: Trusted Remediator ejecuta el documento de automatización y supervisa la ejecución. Una vez finalizado el documento de automatización, Trusted Remediator resuelve el problema.
- Solución manual: Trusted Remediator crea la solución para que usted la OpsItem revise. Tras la revisión, se inicia el documento de automatización.

Los registros de corrección se almacenan en un bucket de Amazon S3. Puede usar los datos del depósito de S3 para crear paneles rápidos personalizados para la elaboración de informes. AMS también proporciona informes a pedido para Trusted Remediator. Para recibir estos informes, póngase en contacto con su CSDM. Para obtener más información, consulte Informes de Trusted Remediator.

## Términos clave de Trusted Remediator

Los siguientes son términos que es útil conocer cuando se utiliza Trusted Remediator en AMS:

- AWS Trusted Advisor, AWS Security Hub y AWS Compute Optimizer: Servicios de optimización de la nube proporcionados por AWS. Trusted Advisor, Security Hub CSPM y Compute Optimizer inspeccionan AWS su entorno y ofrecen recomendaciones basadas en las mejores prácticas en las seis categorías siguientes:
  - Optimización de costos
  - Desempeño
  - Seguridad
  - Tolerancia a errores
  - Excelencia operativa
  - Límites de los servicios

  Para obtener más información, consulte AWS Trusted Advisor, AWS Security Hub y AWS Compute Optimizer.
- Trusted Remediator: una solución de corrección de AMS para Trusted Advisorrealizar comprobaciones, AWS Security Hub CSPMrecomendaciones y recomendaciones. AWS Compute Optimizer Trusted Remediator le ayuda a corregir de forma segura las Trusted Advisor comprobaciones, los controles CSPM de Security Hub y las recomendaciones de Compute Optimizer con las mejores prácticas conocidas para mejorar la seguridad, el rendimiento y reducir los costes. Trusted Remediator es fácil de instalar y configurar. La configuración se realiza una vez y Trusted Remediator ejecuta las correcciones según la programación que prefiera (diaria o semanalmente).
- AWS Systems Manager Documento SSM: archivo JSON o YAML que define las acciones que se AWS Systems Manager realizan en sus recursos. AWS El documento SSM sirve como especificación declarativa para automatizar las tareas operativas en varios AWS recursos e instancias.

- AWS Systems Manager OpsCenter OpsItem: un recurso de administración de problemas operativos en la nube que le ayuda a rastrear y resolver los problemas operativos en su AWS entorno. OpsItems proporcionan una visión y un sistema de gestión centralizados para los datos operativos y los problemas en todos Servicios de AWS los recursos. Cada uno OpsItem representa un problema operativo, como un posible riesgo de seguridad, un problema de rendimiento o un incidente operativo.
- Configuración: una configuración es un conjunto de atributos almacenados en AWS AppConfig, una capacidad de AWS Systems Manager. La aplicación Trusted Remediator AWS AppConfig ayuda a configurar las correcciones a nivel de cuenta. Puede utilizar la AWS AppConfig consola o la API para editar las configuraciones.
- Modo de ejecución: el modo de ejecución es un atributo de configuración que determina cómo ejecutar la corrección para cada resultado de Trusted Advisor comprobación y las recomendaciones de Compute Optimizer y Security Hub CSPM. Se admiten cuatro modos de ejecución: automatizado, manual, condicional e inactivo.
- Anulación de recursos: esta función utiliza etiquetas de recursos para anular la configuración de recursos específicos.
- Registro de elementos de corrección: un archivo de registro en el depósito de registros de S3 sobre correcciones de Trusted Remediator. El registro de elementos de corrección se crea cuando se crean las correcciones. OpsItems Este archivo de registro contiene la corrección de la ejecución manual OpsItems y la corrección de la ejecución automática. OpsItems Utilice este archivo de registro para realizar un seguimiento de todos los elementos de corrección.
- Registro de ejecución de correcciones automatizado: un archivo de registro en el depósito de registros de S3 sobre correcciones de Trusted Remediator. El registro de ejecución de correcciones automatizadas se crea cuando se completa la ejecución automatizada de un documento SSM. Este registro contiene los detalles de la ejecución de SSM para la corrección automática de las ejecuciones. OpsItems Utilice este archivo de registro para realizar un seguimiento de las correcciones automatizadas.

## Comience con Trusted Remediator en AMS

Trusted Remediator está disponible en AMS sin coste adicional. Trusted Remediator admite configuraciones de cuenta única y de cuentas múltiples.

## Incorporado a Trusted Remediator

Para incorporar sus cuentas de AMS a Trusted Remediator, envíe un correo electrónico a sus arquitectos de nube o gerentes de prestación de servicios en la nube ()CSDMs. En el mensaje, incluya la siguiente información:

- Cuentas de AWS: el número de identificación de la cuenta de doce dígitos. Todas las cuentas que desee incorporar a Trusted Remediator deben pertenecer al mismo cliente de Accelerate.
  - Cuenta de administrador delegado: la cuenta que se utiliza para Trusted Advisor que Compute Optimizer y Security Hub CSPM comprueben la configuración de cuentas únicas o múltiples.
  - Cuentas de miembro: son las cuentas vinculadas a la cuenta de administrador delegado. Estas cuentas heredan las configuraciones de la cuenta de administrador delegado. Puede tener una cuenta de miembro o varias cuentas de miembro.

    > **Note**
    >
    > Las cuentas de los miembros heredan las configuraciones de la cuenta de administrador delegado. Si necesita configuraciones diferentes para cuentas específicas, incorpore varias cuentas de administrador delegado con las configuraciones que prefiera. Planifique la estructura de la cuenta y las configuraciones con sus arquitectos de nube antes de incorporarla.

- Regiones de AWS: El Regiones de AWS lugar donde se encuentran sus recursos. Para ver una lista Regiones de AWS, consulta Servicios de AWS por región.
- Calendario y hora de remediación: su programa de remediación preferido (diario o semanal). Trusted Remediator recopila las Trusted Advisor comprobaciones e inicia la reparación a la hora programada. Por ejemplo, puede configurar el programa de remediación para la 1:00 a.m. del domingo de cada semana, hora estándar del este de Australia.
- Correo electrónico de notificación: Trusted Remediator utiliza el correo electrónico de notificación para notificarle diariamente si hay soluciones. El asunto del correo electrónico de notificación es «Resumen de las correcciones de Trusted Remediator» y el contenido proporciona información sobre las correcciones de Trusted Remediator ejecutadas en las últimas 24 horas.

> **Note**
>
> Revise sus aplicaciones y recursos después de cada corrección programada. Para obtener asistencia adicional, póngase en contacto con AMS.

Tras enviar la solicitud de incorporación con los detalles necesarios a su CA o CSDM, AMS incorporará sus cuentas a Trusted Remediator. Trusted Remediator utiliza AWS AppConfig, una capacidad de AWS Systems Manager, para definir la configuración de las comprobaciones. Trusted Advisor Estas configuraciones son un conjunto de atributos que se almacenan en AWS AppConfig. Para evitar cargos no autorizados a sus recursos, todas las Trusted Advisor comprobaciones admitidas se configuran como inactivas cuando las cuentas se incorporan a Trusted Remediator. Una vez que se haya incorporado, podrá utilizar la AWS AppConfig consola o la API para gestionar las configuraciones. Estas configuraciones le ayudan a corregir automáticamente Trusted Advisor comprobaciones específicas o a evaluar y corregir manualmente las comprobaciones restantes. Las configuraciones son altamente personalizables, lo que le permite aplicar configuraciones para cada Trusted Advisor comprobación. Para obtener más información, consulte Configurar la corrección de Trusted Advisor comprobaciones en Trusted Remediator.

## Elija las comprobaciones y recomendaciones que desee corregir

De forma predeterminada, el modo de ejecución de correcciones está inactivo para todas las Trusted Advisor comprobaciones, las recomendaciones de Compute Optimizer y las recomendaciones de CSPM de Security Hub de su configuración. Esto evita la corrección no autorizada y protege los recursos. AMS proporciona documentos de automatización de SSM seleccionados para la corrección de los Trusted Advisor cheques.

Para seleccionar las comprobaciones que desea corregir con Trusted Remediator, complete los siguientes pasos:

1. Revise la lista de recomendaciones de Compute Optimizer compatibles Trusted Advisor, las recomendaciones de Security Hub CSPM y el nombre de los documentos de automatización de SSM asociados para decidir qué comprobaciones y recomendaciones desea corregir con Trusted Remediator.
2. Actualiza tu configuración para activar la corrección de las Trusted Advisor comprobaciones seleccionadas, las recomendaciones de Compute Optimizer y las recomendaciones de CSPM

de Security Hub. Para obtener instrucciones sobre cómo seleccionar las comprobaciones, consulte. Configurar la corrección de Trusted Advisor comprobaciones en Trusted Remediator

### Realice un seguimiento de sus correcciones en Trusted Remediator

Tras actualizar la configuración a nivel de cuenta, Trusted Remediator crea una para cada corrección. OpsItems Trusted Remediator ejecuta el documento SSM para la corrección automática de acuerdo con su programa de remediación. OpsItems Para obtener instrucciones sobre cómo ver todas las correcciones OpsItems desde la OpsCenter consola de Systems Manager, consulteRealice un seguimiento de las correcciones en Trusted Remediator.

### Ejecute las correcciones manuales en Trusted Remediator

Puedes corregir manualmente las Trusted Advisor comprobaciones y las recomendaciones de Compute Optimizer y Security Hub CSPM. Al iniciar una corrección manual, Trusted Remediator crea una ejecución manual. OpsItem Debe revisar e iniciar el documento de automatización de SSM para corregir el. OpsItems Para obtener más información, consulte Ejecute las correcciones manuales en Trusted Remediator.

## Recomendaciones de Compute Optimizer respaldadas por Trusted Remediator

En la siguiente tabla, se enumeran las recomendaciones de Compute Optimizer compatibles, los documentos de automatización de SSM, los parámetros preconfigurados y el resultado esperado de los documentos de automatización. Revisa el resultado esperado para ayudarte a entender los posibles riesgos en función de los requisitos de tu empresa antes de utilizar un documento de automatización de SSM para corregir las comprobaciones.

Asegúrate de que la regla de configuración correspondiente para cada comprobación de Compute Optimizer esté presente en las comprobaciones compatibles para las que deseas habilitar la corrección. Para obtener más información, consulta Cómo suscribirse a las AWS Compute Optimizer comprobaciones Trusted Advisor.

| Opción de optimización | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| Redimensionamiento | | |

| Opción de optimización | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
| --- | --- | --- |
| Recomendaciones de instancias de Amazon EC2 | AWSManagedServices-TrustedRemediatorResizeInstanceByComputeOptimizerRecommendation<br><br>El tipo de instancia de Amazon EC2 se actualizó de acuerdo con las recomendaciones de Compute Optimizer. Se eligen las opciones más óptimas manteniendo los mismos parámetros de plataforma (arquitectura, hipervisor, interfaz de red, tipo de virtualización, etc.) si existe la opción. | • MinimumDaysSinceLastChange: el parámetro para especificar el número mínimo de días transcurridos desde el último cambio de tipo de instancia. El valor predeterminado es de 7 días.<br><br>Sin restricciones<br>• Crear AMIBefore cambio de tamaño: para crear la AMI de la instancia como copia de seguridad antes de cambiar el tamaño, establézcala en «true». Para no crear una copia de seguridad, establézcala en «false». El valor predeterminado es “verdadero”.<br><br>Sin restricciones |

| Opción de optimización | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
| --- | --- | --- |
| Recomendaciones de volumen de Amazon EBS | AWSManagedServices-ModifyEBSVolume<br><br>El volumen de Amazon EBS se modifica de acuerdo con las recomendaciones de Compute Optimizer. La modificación puede incluir el tipo de volumen, el tamaño, las IOPS y la generación de volúmenes (gp2, gp3, etc.). | • CreateSnapshot: Para crear una instantánea antes de modificar el volumen, establézcalo en «true». Para no crear una instantánea, establézcala en «false». El valor predeterminado es «verdadero».<br><br>Sin restricciones<br>• VolumeType: El tipo de volumen deseado. Si no se especifica ningún tipo, se conserva el tipo existente.<br><br>Sin restricciones<br>• VolumeSize: El tamaño deseado del volumen, en GiB. El tamaño del volumen objetivo debe ser mayor o igual al tamaño actual del volumen. Si no se especifica ningún tamaño, se conserva el tamaño existente.<br><br>Sin restricciones<br>• Iops: el número solicitado de I/O operaciones por segundo (IOPS). Este parámetro solo es válido para los volúmenes io1, io2 y gp3.<br><br>Sin restricciones<br>• Rendimiento: el rendimiento para aprovisionar un volumen, con un máximo de 1000 MiB/s. Este parámetro solo es válido para los volúmenes gp3. |

| Opción de optimización | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
| --- | --- | --- |
| | | Sin restricciones<br>• RemediateStackDrift: Para iniciar la corrección de la desviación, si alguna desviación se debe a una modificación del volumen, establézcala en «true». Para no intentar corregir las desviaciones, establézcalo en «false». El valor predeterminado es “verdadero”.<br>Sin restricciones |
| Recomenda ciones de funciones Lambda | AWSManagedServices-TrustedR emediatorOptimizeLambdaMemory<br>AWS Lambda memoria de funciones optimizada de acuerdo con las recomendaciones de Compute Optimizer. | RecommendedMemorySize : tamaño de memoria personalizado, si es diferente de las opciones recomenda das.<br>Sin restricciones |
| Recursos inactivos | | |

| Opción de optimización | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| Volumen Amazon EBS inactivo | AWSManagedServices-DeleteUnusedEBSVolume<br><br>Se eliminará el volumen Amazon EBS no adjunto. | • CreateSnapshot: Para crear una instantánea antes de eliminar el volumen, establézcalo en «true». Para no crear una instantánea, establézcala en «false». El valor predeterminado es «verdadero».<br><br>Sin restricciones<br>• MinimumUnattachedDays: mínimo de días sin adjuntar del volumen de Amazon EBS para eliminar, hasta 62 días. El valor predeterminado es 7.<br><br>Sin restricciones |
| Instancia Amazon EC2 inactiva | AWSManagedServices-StopECInstancia 2<br><br>Se detendrá la instancia Amazon EC2 inactiva. | ForceStopWithInstanceStore: Para forzar la detención de las instancias que utilizan el almacén de instancias, establézcalo en «true». Para no forzar la parada, establézcalo en «false». El valor predeterminado «false» impide que la instancia se detenga.<br><br>Sin restricciones |

| Opción de optimización | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| Instancia de Amazon RDS inactiva | AWSManagedServices-StopIdleRDSInstance<br><br>Detenga una instancia de Amazon RDS inactiva. Los motores compatibles son: MariaDB, Microsoft SQL Server, MySQL, Oracle y PostgreSQL. Este documento no se aplica a Aurora MySQL ni a Aurora PostgreSQL. La instancia se detendrá durante un máximo de 7 días y se volverá a lanzar automáticamente. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |

## Trusted Advisor comprobaciones compatibles con Trusted Remediator

En la siguiente tabla se enumeran las Trusted Advisor comprobaciones admitidas, los documentos de automatización de SSM, los parámetros preconfigurados y el resultado esperado de los documentos de automatización. Revise el resultado esperado para ayudarle a comprender los posibles riesgos en función de los requisitos de su empresa antes de utilizar un documento de automatización de SSM para la corrección de los controles.

Asegúrese de que la regla de configuración correspondiente a cada Trusted Advisor comprobación esté presente en las comprobaciones compatibles para las que desee habilitar la corrección. Para obtener más información, consulta Ver las AWS Trusted Advisor comprobaciones impulsadas por AWS Config. Si una comprobación tiene AWS Security Hub CSPM los controles correspondientes, asegúrese de que el control CSPM del Security Hub esté activado. Para obtener más información, consulte Habilitar los controles en Security Hub CSPM. Para obtener información sobre la gestión de los parámetros preconfigurados, consulte Configurar la corrección de comprobaciones de Trusted Advisor en Trusted Remediator.

## Trusted Advisor comprobaciones de optimización de costes compatibles con Trusted Remediator

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
|---|---|---|
| Z4 AUBRNSmz<br><br>Direcciones IP elásticas no asociadas | AWSManagedServices-TrustedR emediatorReleaseElasticIP<br><br>Libera una dirección IP elástica que no está asociada a ningún recurso. | No se permiten parámetros preconfig urados.<br><br>No hay restricciones |
| c18d2gz150: se detuvieron las instancias de Amazon EC2 | AWSManagedServices-Terminat eEC2 InstanceStoppedForPeriodOfT ime: Se cancelan las instancias de Amazon EC2 detenidas durante varios días. | • Crear AMIBefore terminación: para crear la AMI de la instancia como respaldo antes de terminar la instancia Amazon EC2, elija. `true` Para no crear una copia de seguridad antes de la finalización, elija. `false` El valor predeterm inado es `true`.<br>• AllowedDays: El número de días que la instancia estuvo detenida antes de ser cancelada. El valor predeterminado es 30.<br><br>Sin restricciones |
| c18d2gz128<br><br>Repositorio de Amazon ECR sin política de ciclo de vida configura da | AWSManagedServices-TrustedR emediatorPutECRLifecyclePolicy<br><br>Crea una política de ciclo de vida para el repositorio especificado si aún no existe una política de ciclo de vida. | ImageAgeLimit: El límite de edad máximo en días (de 1 a 365) para «cualquier» imagen del repositorio de Amazon ECR.<br><br>Sin restricciones |
| DAvU99Dc4C | AWSManagedServices-DeleteUn usedEBSVolume | • CreateSnapshot: Si se establece en`true`, la automatización crea |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
| --- | --- | --- |
| Volúmenes de Amazon EBS infrautilizados | Elimina los volúmenes de Amazon EBS infrautilizados si los volúmenes no se adjuntaron durante los últimos 7 días. De forma predeterminada, se crea una instantánea de Amazon EBS. | una instantánea del volumen de Amazon EBS antes de eliminarlo. El ajuste predeterminado es `true`. Los valores válidos son `true` y `false` (distinguen mayúsculas de minúsculas).<br>• MinimumUnattachedDays: Un mínimo de días sin adjuntar del volumen de EBS que se debe eliminar, hasta un máximo de 62 días. Si se establece en`0`, el documento SSM no comprueba el período sin adjuntar y elimina el volumen si el volumen no está adjunto actualmente. El valor predeterminado es. 7<br><br>Sin restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| hola M8 LMh88u<br><br>Balanceadores de carga inactivos | AWSManagedServices-DeleteIdleClassicLoadBalancer<br><br>Elimina un Classic Load Balancer inactivo si no se utiliza y no hay ninguna instancia registrada. | IdleLoadBalancerDays: el número de días durante los que el Classic Load Balancer ha solicitado 0 conexiones antes de considerarlo inactivo. El valor predeterminado es de siete días.<br><br>Si la ejecución automática está habilitada, la automatización elimina los balanceadores de carga clásicos inactivos si no hay instancias de back-end activas. Para todos los balanceadores de carga clásicos inactivos que tienen instancias de back-end activas, pero que no tienen instancias de back-end en buen estado, no se usa la corrección automática OpsItems y para la remediación manual se crea. |
| TI39HalfU8<br><br>Amazon RDS Idle DB Instances | AWSManagedServices-StopIdleRDSInstance<br><br>Se detiene la instancia de base de datos de Amazon RDS que ha estado inactiva durante los últimos siete días. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
| --- | --- | --- |
| COr6dfpM05<br><br>AWS Lambda funciones sobreapro visionadas para el tamaño de la memoria | AWSManagedServices-ResizeLa mbdaMemory<br><br>AWS Lambda el tamaño de la memoria de la función se redimensi ona al tamaño de memoria recomendado proporcionado por. Trusted Advisor | RecommendedMemorySize: la asignación de memoria recomenda da para la función Lambda. El rango de valores está entre 128 y 10240.<br><br>Si el tamaño de la función Lambda se modificó antes de que se ejecutara la automatización, esta automatización podría sobrescribir la configuración con el valor recomenda do por. Trusted Advisor |
| QCH7dWoux1<br><br>Utilización baja de instancias de Amazon EC2 | AWSManagedServices-StopEC2I nstance (documento SSM predeterm inado para el modo de ejecución automática y manual).<br><br>Se detienen las instancias Amazon EC2 de baja utilización. | ForceStopWithInstanceStore: Se configura en `true` para forzar la detención de las instancias mediante el almacén de instancias. De lo contrario, establézcala en `false`. El valor predeterminado de `false` impide que la instancia se detenga. Los valores válidos son verdadero o falso (distingue entre mayúsculas y minúsculas).<br><br>Sin restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
| --- | --- | --- |
| QCH7DWOUx1<br><br>Utilización baja de instancias de Amazon EC2 | AWSManagedServices-ResizeInstanceByOneLevel<br><br>El tamaño de la instancia Amazon EC2 se reduce en un tipo de instancia del mismo tipo de familia de instancias. La instancia se detiene e inicia durante la operación de cambio de tamaño y vuelve al estado inicial una vez finalizada la ejecución del documento SSM. Esta automatización no admite el cambio de tamaño de las instancias que se encuentran en un grupo de Auto Scaling. | • MinimumDaysSinceLastChange: Número mínimo de días desde el último cambio de tipo de instancia. Si el tipo de instancia se modificó dentro de un tiempo específico, el tipo de instancia no cambiará. Se usa `0` para omitir esta validación. El valor predeterminado es 7.<br>• Crear AMIBefore cambio de tamaño: para crear la AMI de la instancia como copia de seguridad antes de cambiar el tamaño, elija`true`. Para no crear una copia de seguridad, elija`false`. El valor predeterminado es `false`. Los valores válidos son `true` y `false` (distinguen mayúsculas de minúsculas).<br>• ResizeIfStopped: Para continuar con el cambio de tamaño de la instancia, incluso si la instancia está detenida, elija`true`. Para no cambiar automáticamente el tamaño de la instancia si está detenida, elija`false`. Los valores válidos son `true` y `false` (distinguen mayúsculas de minúsculas).<br><br>Sin restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
|---|---|---|
| QCH7DWOUx1<br><br>Utilización baja de instancias de Amazon EC2 | AWSManagedServices-TerminateInstance<br><br>Las instancias de Amazon EC2 poco utilizadas se cancelan si no forman parte de un Auto Scaling Group y la protección de terminación no está habilitada. De forma predeterminada, se crea una AMI. | Crear AMIBefore terminación: defina esta opción en `true` o `false` para crear una AMI de instancia como respaldo antes de terminar la instancia EC2. El valor predeterminado es `true`. Los valores válidos son `true` y `false` (distinguen mayúsculas de minúsculas).<br><br>Sin restricciones |
| G31sq1e9u<br><br>Underutilized Amazon Redshift Clusters | AWSManagedServices-PauseRedshiftCluster<br><br>El clúster de Amazon Redshift está en pausa. | No se permiten parámetros preconfig urados.<br><br>No hay restricciones |
| c1cj39rr6v<br><br>Configuración de anulación de carga multipart e incompleta de Amazon S3 | AWSManagedServices-TrustedRemediatorEnableS3AbortIncompleteMultipartUpload<br><br>El bucket de Amazon S3 está configurado con una regla de ciclo de vida para anular las cargas de varias partes que permanecen incompletas después de ciertos días. | DaysAfterInitiation: el número de días transcurridos los cuales Amazon S3 detiene una carga multiparte incompleta. El valor predeterminado es de 7 días.<br><br>Sin restricciones |
| c1z7kmr00n<br><br>Recomendaciones de optimización de costos de Amazon EC2 para instancias | Utilice las recomendaciones de instancias de Amazon EC2 y la instancia de Amazon EC2 inactiva de. Recomendaciones de Compute Optimizer respaldadas por Trusted Remediator | No se permiten parámetros preconfig urados.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
| --- | --- | --- |
| c1z7kmr02n<br><br>Recomenda ciones de optimización de costos de Amazon EBS para volúmenes | Utilice las recomendaciones de volumen de Amazon EBS y el volumen de Amazon EBS inactivo desde. Recomendaciones de Compute Optimizer respaldadas por Trusted Remediator | No se permiten parámetros preconfig urados.<br><br>No hay restricciones |
| c1z7kmr03n<br><br>Recomenda ciones de optimización de costos de Amazon RDS para instancias de base de datos | Utilice la instancia inactiva de Amazon RDS deRecomendaciones de Compute Optimizer respaldadas por Trusted Remediator. | No se permiten parámetros preconfig urados.<br><br>No hay restricciones |
| c1z7kmr05n<br><br>AWS Lambda recomenda ciones de optimización de costes para las funciones | Utilice las recomendaciones de funciones Lambda de. Recomenda ciones de Compute Optimizer respaldadas por Trusted Remediator | No se permiten parámetros preconfig urados.<br><br>No hay restricciones |

## Trusted Advisor controles de seguridad compatibles con Trusted Remediator

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| 12Fnkpl8Y5<br><br>Exposed Access Keys | AWSManagedServices-TrustedRemediatorDeactivateIAMAccessKey<br><br>La clave de acceso IAM expuesta está desactivada. | No se permiten parámetros preconfigurados.<br><br>Las aplicaciones configuradas con una clave de acceso de IAM expuesta no se pueden autenticar. |
| Hs4Ma3G127: el registro de ejecución de API Gateway REST WebSocket y API debe estar habilitado<br><br>Verificación APIGatewaycorrespondiente AWS Security Hub CSPM: 1. | AWSManagedServices-TrustedRemediatorEnableAPIGateWayExecutionLogging<br><br>El registro de ejecución está habilitado en la fase de la API. | LogLevel: Nivel de registro para habilitar el registro de la ejecución , `ERROR` - El registro solo está habilitado para los errores. `INFO` - El registro está habilitado para todos los eventos.<br><br>Debe conceder permiso a API Gateway para leer y escribir los registros de su cuenta a CloudWatch fin de habilitar el registro de ejecución; consulte Configurar el CloudWatch registro para REST APIs en API Gateway para obtener más información. |
| Hs4Ma3G129: las etapas de la API REST de API Gateway deberían tener el rastreo habilitado AWS X-Ray<br><br>Verificación APIGatewa | AWSManagedServices-EnableApiGateWayXRayTracing<br><br>El rastreo de X-Ray está habilitado en la fase API. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
| --- | --- | --- |
| ycorrespondiente AWS Security Hub CSPM: 3. | | |
| Hs4Ma3G202 - Los datos de la caché de la API REST de API Gateway deben cifrarse en reposo<br><br>Verificación APIGatewaycorrespondiente AWS Security Hub CSPM: 5. | AWSManagedServices-EnableAPIGatewayCacheEncryption<br><br>Habilite el cifrado en reposo para los datos de la caché de la API REST de API Gateway si la etapa de la API REST de API Gateway tiene la caché habilitada. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
| --- | --- | --- |
| Hs4Ma3G177 - AWS Security Hub CSPM Comprobación correspondiente: los grupos de escalado automático asociados a un balancead or de cargas deben usar las comprobaciones de estado del balanceador de cargas .1 AutoScaling | AWSManagedServices-TrustedR emediatorEnableAutoScalingG roupELBHealthCheck<br><br>Las comprobaciones de estado de Elastic Load Balancing están habilitadas para el grupo Auto Scaling. | HealthCheckGracePeriod: La cantidad de tiempo, en segundos, que Auto Scaling espera antes de comprobar el estado de una instancia de Amazon Elastic Compute Cloud que ha entrado en servicio.<br><br>La activación de las comprobaciones de estado de Elastic Load Balancing puede provocar el reemplazo de una instancia en ejecución si alguno de los balanceadores de carga de Elastic Load Balancing adjuntos al grupo de Auto Scaling indica que está en mal estado. Para obtener más información, consulte Adjuntar un balanceador de cargas de Elastic Load Balancing a su grupo de Auto Scaling. |
| Hs4Ma3G245: las CloudForm ation pilas deben integrarse con Amazon Simple Notification Service<br><br>Verificación correspondiente AWS Security Hub CSPM CloudFormation: 1. | AWSManagedServices-EnableCF NStackNotification<br><br>Asocie una CloudFormation pila a un tema de Amazon SNS para la notificación. | NotificaciónARNs: uno ARNs de los temas de Amazon SNS que se van a asociar a las pilas seleccionadas CloudFormation .<br><br>Para habilitar la corrección automátic a, se debe `NotificationARNs` proporcionar el parámetro preconfig urado. |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
| --- | --- | --- |
| Hs4Ma3G210: las distribuciones deben tener el registro habilitad o CloudFront<br><br>Verificación correspondiente AWS Security Hub CSPM : CloudFront2. | AWSManagedServices-EnableCl oudFrontDistributionLogging<br><br>El registro está habilitado para las CloudFront distribuciones de Amazon. | • BucketName: el nombre del depósito de Amazon S3 en el que desea almacenar los registros de acceso.<br>• S3KeyPrefix: el prefijo de la ubicación en el depósito de S3 de los registros de CloudFront distribución de Amazon.<br>• IncludeCookies: Indica si se deben incluir las cookies en los registros de acceso.<br><br>Para habilitar la corrección automátic a, se deben proporcionar los siguientes parámetros preconfig urados:<br><br>• BucketName<br>• S3KeyPrefix<br>• IncludeCookies<br><br>Para conocer estas restricciones de corrección, consulte ¿Cómo activo el registro en mi distribución? CloudFront |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
| --- | --- | --- |
| Hs4Ma3G109: CloudTrail la validación del archivo de registro debe estar habilitada<br><br>Comprobación correspondiente AWS Security Hub CSPM CloudTrail: 4. | AWSManagedServices-TrustedRemediatorEnableCloudTrailLogValidation<br><br>Permite la validación CloudTrail del registro de senderos. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
| --- | --- | --- |
| Hs4Ma3G108: las CloudTrail rutas deberían integrarse con Amazon Logs CloudWatch<br><br>Verificación correspondiente AWS Security Hub CSPM CloudTrail: 5. | AWSManagedServices-Integrat eCloudTrailWithCloudWatch<br><br>AWS CloudTrail está integrado con CloudWatch Logs. | • CloudWatchLogsLogGroupName: nombre del grupo de CloudWatc h registros al que se envían los CloudTrail registros. Debe utilizar un grupo de registro que exista en su cuenta.<br>• CloudWatchLogsRoleName: Nombre de la función de IAM que debe asumir el punto final de CloudWatch Logs para escribir en el grupo de registros de un usuario. Debe utilizar un rol que ya exista en su cuenta.<br><br>Para habilitar la corrección automátic a, se deben proporcionar los siguientes parámetros preconfig urados:<br><br>• CloudWatchLogsLogGroupName<br>• CloudWatchLogsRoleName |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
| --- | --- | --- |
| Hs4Ma3G217: CodeBuild los entornos de proyecto deben tener una configuración de registro AWS<br><br>Verificación correspondiente AWS Security Hub CSPM CodeBuild: 4. | AWSManagedServices-TrustedRemediatorEnableCodeBuildLoggingConfig<br><br>Habilita el registro del CodeBuild proyecto. | No se permiten parámetros preconfig urados.<br><br>No hay restricciones |
| Hs4Ma3G306 - Los clústeres de base de datos de Neptune deberían tener habilitada la protección de eliminación<br><br>AWS Security Hub CSPM Comprobación correspondiente: Neptune.4 | AWSManagedServices-TrustedRemediatorEnableNeptuneDBClusterDeletionProtection<br><br>Habilita la protección contra la eliminación del clúster de Amazon Neptune. | No se permiten parámetros preconfig urados.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| Hs4Ma3G308: Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones<br><br>AWS Security Hub CSPM Verificación correspondiente: documento DB.5 | AWSManagedServices-TrustedRemediatorEnableDocumentDBClusterDeletionProtection<br><br>Habilita la protección contra la eliminación del clúster de Amazon DocumentDB. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| Hs4Ma3G323 - Las tablas de DynamoDB deben tener habilitada la protección de eliminación<br><br>AWS Security Hub CSPM Comprobación correspondiente: DynamoDB.6 | AWSManagedServices-TrustedRemediatorEnableDynamoDBTableDeletionProtection<br><br>Permite la protección contra la eliminación de tablas DynamoDB que no son de AMS. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| EPS02JT06w: Instantáneas públicas de Amazon EBS | AWSManagedServices-TrustedRemediatorDisablePublicAccessOnEBSSnapshot<br><br>El acceso público a la instantánea de Amazon EBS está deshabilitado. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
| --- | --- | --- |
| Hs4Ma3G118: Los grupos de seguridad predeterminados de VPC no deberían permitir el tráfico entrante o saliente<br><br>Verificación correspondiente AWS Security Hub CSPM: EC2.2 | AWSManagedServices-TrustedRemediatorRemoveAllRulesFromDefaultSG<br><br>Se eliminan todas las reglas de entrada y salida del grupo de seguridad predeterminado. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| Hs4Ma3G117: Los volúmenes EBS adjuntos deben cifrarse en reposo<br><br>Verificación correspondiente AWS Security Hub CSPM : EC2.3 | AWSManagedServices-EncryptInstanceVolume<br><br>El volumen de Amazon EBS adjunto a la instancia está cifrado. | • KMSKeyID: ID de AWS KMS clave o ARN para cifrar el volumen.<br>• DeleteStaleNonEncryptedSnapshotBackups: un indicador que decide si se debe eliminar la copia de seguridad instantánea de los volúmenes antiguos no cifrados.<br><br>La instancia se reinicia como parte de la corrección y es posible revertirla si `DeleteStaleNonEncryptedSnapshotBackups` está configurada de esta manera, lo que ayuda a `false` la restauración. |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
| --- | --- | --- |
| Hs4Ma3G120: las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico<br><br>Verificación correspondiente AWS Security Hub CSPM : EC2.4 | AWSManagedServices-TerminateInstance(documento SSM predeterminado para el modo de ejecución automática y manual)<br><br>Las instancias de Amazon EC2 detenidas durante 30 días se cancelan. | Crear AMIBefore terminación:. Para crear la AMI de la instancia como respaldo antes de terminar la instancia EC2, elija. `true` Para no crear una copia de seguridad antes de la finalización, elija. `false` El valor predeterminado es `true`.<br><br>Sin restricciones |
| Hs4Ma3G120: las instancias EC2 detenidas deben eliminarse después de un período de tiempo específico<br><br>Verificación correspondiente AWS Security Hub CSPM : EC2.4 | AWSManagedServices-TerminateEC2 InstanceStoppedForPeriodOfTime: Las instancias de Amazon EC2 detenidas durante el número de días definido en Security Hub (el valor predeterminado es 30) se cancelan. | Crear AMIBefore terminación: para crear la AMI de la instancia como respaldo antes de terminar la instancia EC2, elija. `true` Para no crear una copia de seguridad antes de la finalización, elija. `false` El valor predeterminado es `true`.<br><br>Sin restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
| --- | --- | --- |
| Hs4Ma3G121: el cifrado por defecto de EBS debe estar activado<br><br>Verificación correspondiente AWS Security Hub CSPM : EC2.7 | AWSManagedServices-EncryptEBSByDefault<br><br>El cifrado de Amazon EBS está habilitado de forma predeterminada para el Región de AWS | No se permiten parámetros preconfigurados.<br><br>El cifrado de manera predeterminada es una configuración específica de la región. Si lo habilita para una región, no podrá deshabilitarlo para volúmenes o instantáneas individuales de esa región. |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
| --- | --- | --- |
| Hs4Ma3G124: Las instancias de Amazon EC2 deben utilizar la versión 2 del servicio de metadatos de instancias () IMDSv2<br><br>Verificación correspondiente AWS Security Hub CSPM : EC2.8 | AWSManagedServices-TrustedRemediatorHabilitar instancia EC2 IMDSv2<br><br>Las instancias de Amazon EC2 utilizan Instance Metadata Service versión 2 ()IMDSv2. | • IMDSv1MetricCheckPeriod: El número de días (42-455) necesarios para analizar las métricas de uso de IMDSv1. CloudWatch Si la instancia de Amazon EC2 se creó dentro del período de tiempo especificado, el análisis comienza a partir de la fecha de creación de la instancia.<br>• HttpPutResponseHopLimit: el número máximo de saltos de red permitidos para el token de metadatos de la instancia. Este valor se puede configurar entre saltos 1 y2. Un límite de saltos de 1 restringe el acceso del token a los procesos que se ejecutan directamente en la instancia, mientras que un límite de saltos de 2 permite el acceso desde los contenedores que se ejecutan en la instancia.<br><br>Sin restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| Hs4Ma3G207: las subredes EC2 no deberían asignar automáticamente direcciones IP públicas<br><br>Verificación correspondiente AWS Security Hub CSPM : EC2.15 | AWSManagedServices-UpdateAutoAssignPublicIpv4 direcciones<br><br>Las subredes de VPC están configuradas para no asignar automáticamente direcciones IP públicas. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| Hs4Ma3G209: se eliminan las listas de control de acceso a la red no utilizadas<br><br>Verificación correspondiente AWS Security Hub CSPM : EC2.16 | AWSManagedServices-DeleteUnusedNACL<br><br>Elimine la ACL de red no utilizada | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| Hs4Ma3G215: Deben eliminarse los grupos de seguridad de Amazon EC2 no utilizados<br><br>Verificación correspondiente AWS Security Hub CSPM : EC2.22 | AWSManagedServices-DeleteSecurityGroups<br><br>Elimine los grupos de seguridad no utilizados. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| Hs4Ma3G247: Amazon EC2 Transit Gateway no debería aceptar automáticamente las solicitudes de adjuntos de VPC<br><br>Verificación correspondiente AWS Security Hub CSPM : EC2.23 | AWSManagedServices-TrustedRemediatorDisableTGWAutoVPCAttach- Desactiva la aceptación automática de las solicitudes de adjuntos de VPC para la Amazon EC2 Transit Gateway especificada que no sea AMS. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
|---|---|---|
| Hs4Ma3G235: los repositorios privados de ECR deberían tener configurada la inmutabilidad de etiquetas<br><br>Verificación correspondiente AWS Security Hub CSPM : ECR.2 | AWSManagedServices-TrustedRemediatorSetImageTagImmutability<br><br>Establece la configuración de mutabilidad de la etiqueta de imagen en INMUTABLE para el repositorio especificado. | No se permiten parámetros preconfig urados.<br><br>No hay restricciones |
| Hs4Ma3G216: los repositorios de ECR deben tener configura da al menos una política de ciclo de vida<br><br>Verificación AWS Security Hub CSPM correspondiente: ECR.3 | AWSManagedServices-PutECRRepositoryLifecyclePolicy<br><br>El repositorio de ECR tiene configura da una política de ciclo de vida. | LifecyclePolicyText: El texto de la política del repositorio JSON que se aplicará al repositorio.<br><br>Para habilitar la corrección automátic a, se deben proporcionar los siguientes parámetros preconfig urados:<br><br>LifecyclePolicyText |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| Hs4Ma3G325: los clústeres EKS deben tener habilitado el registro de auditoría<br><br>Verificación correspondiente AWS Security Hub CSPM : EKS.8 | AWSManagedServices-TrustedRemediatorEnableEKSAuditLog<br><br>El registro de auditoría está habilitado para el clúster EKS. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| Hs4Ma3G183: el balanceador de carga de aplicaciones debe configurarse para eliminar los encabezados HTTP<br><br>Verificación AWS Security Hub CSPM correspondiente: ELB.4 | AWSConfigRemediation-DropInvalidHeadersForALB<br><br>Application Load Balancer está configurado para campos de encabezado no válidos. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
| --- | --- | --- |
| Hs4Ma3G184: Debe habilitar se el registro de los balancead ores de carga de aplicaciones y los balancead ores de carga clásicos<br><br>Verificación correspondiente AWS Security Hub CSPM : ELB.5 | AWSManagedServices-EnableEL BLogging (documento SSM predeterminado para el modo de ejecución automática y manual)<br><br>El registro de Application Load Balancer y Classic Load Balancer está habilitado. | • BucketName: el nombre del depósito (no el ARN). Asegúrese de que la política de bucket esté configurada correctamente para el registro.<br>• S3KeyPrefix: el prefijo de la ubicación en el bucket de Amazon S3 para los registros de Elastic Load Balancing.<br><br>Para habilitar la corrección automátic a, se deben proporcionar los siguientes parámetros preconfig urados:<br><br>• BucketName<br>• S3KeyPrefix<br><br>El bucket de Amazon S3 debe tener una política de bucket que conceda permiso a Elastic Load Balancing para escribir los registros de acceso en el bucket. |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
| --- | --- | --- |
| Hs4Ma3G184: El registro de los balanceadores de carga de aplicaciones y los balanceadores de carga clásicos debe estar habilitado<br><br>Verificación correspondiente AWS Security Hub CSPM : ELB.5 | AWSManagedServices-EnableELBLoggingV2<br><br>El registro de Application Load Balancer y Classic Load Balancer está habilitado. | • TargetBucketTagKey: el nombre de la etiqueta (distingue entre mayúsculas y minúsculas) que se utiliza para identificar el bucket de Amazon S3 de destino. Utilícela junto con `TargetBucketTagValue` la etiqueta del bucket que servirá como bucket de destino para el registro de acceso.<br>• TargetBucketTagValue: el valor de la etiqueta (distingue entre mayúsculas y minúsculas) que se utiliza para identificar el bucket de Amazon S3 de destino. Utilícelo junto con el bucket `TargetBucketTagKey` para etiquetar el bucket que servirá como bucket de destino para el registro de acceso.<br>• S3BucketPrefix: el prefijo (jerarquía lógica) del bucket de Amazon S3. El prefijo que especifique no debe incluir la cadena `AWSLogs`. Para obtener más información, consulte Organizar objetos con prefijos.<br><br>Para habilitar la corrección automática, se deben proporcionar los siguientes parámetros preconfigurados:<br>• TargetBucketTagKey<br>• TargetBucketTagValue<br>• S3BucketPrefix |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| | | El bucket de Amazon S3 debe tener una política de bucket que conceda permiso a Elastic Load Balancing para escribir los registros de acceso en el bucket. |
| Hs4Ma3G326: La configuración de acceso público del bloque Amazon EMR debe estar habilitada<br><br>AWS Security Hub CSPM Verificación correspondiente: EMR.2 | AWSManagedServices-TrustedRemediatorEnableEMRBlockPublicAccess<br><br>La configuración de acceso público del bloqueo de Amazon EMR está activada en la cuenta. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| Hs4Ma3G135: las AWS KMS claves no deben borrarse involuntariamente<br><br>Verificación correspondiente AWS Security Hub CSPM : KMS.3 | AWSManagedServices-CancelKeyDeletion<br><br>AWS KMS se cancela la eliminación de la clave. | No se permite ningún parámetro preconfigurado.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| Hs4Ma3G299 - Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas<br><br>AWS Security Hub CSPM Verificación correspondiente: documento DB.3 | AWSManagedServices-TrustedRemediatorDisablePublicAccessOnDocumentDBSnapshot<br><br>Elimina el acceso público de la instantánea manual del clúster de Amazon DocumentDB. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| Hs4Ma3G319 - Los firewalls de Network Firewall deben tener habilitada la protección de eliminación<br><br>Verificación AWS Security Hub CSPM correspondiente NetworkFirewall: 9. | AWSManagedServices-TrustedRemediatorEnableNetworkFirewallDeletionProtection- Habilita la protección de eliminación para AWS Network Firewall. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| Hs4Ma3G223: los OpenSearch dominios deben cifrar los datos enviados entre nodos<br><br>Verificación correspondiente AWS Security Hub CSPM OpenSearch: 3. | AWSManagedServices-EnableOpenSearchNodeToNodeEncryption<br><br>El cifrado de nodo a nodo está habilitado para el dominio. | No se permiten parámetros preconfigurados.<br><br>Una vez activado el node-to-node cifrado, no se puede deshabilitar la configuración. En su lugar, haz una instantánea manual del dominio cifrado, crea otro dominio, migra tus datos y, a continuación, elimina el dominio anterior. |
| Hs4Ma3G222: el registro de errores de OpenSearch dominio en los registros debe estar habilitado CloudWatch<br><br>Verificación correspondiente AWS Security Hub CSPM : Opensearch.4 | AWSManagedServices-EnableOpenSearchLogging<br><br>El registro de errores está activado para el dominio. OpenSearch | CloudWatchLogGroupArn: El ARN de un grupo de registros de Amazon CloudWatch Logs.<br><br>Para habilitar la corrección automática, se debe proporcionar el siguiente parámetro preconfigurado:. CloudWatchLogGroupArn<br><br>La política CloudWatch de recursos de Amazon debe configurarse con permisos. Para obtener más información, consulta Cómo habilitar los registros de auditoría en la Guía del usuario OpenSearch de Amazon Service. |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| Hs4Ma3G221: los OpenSearch dominios deben tener habilitado el registro de auditoría<br><br>Verificación correspondiente AWS Security Hub CSPM : Opensearch.5 | AWSManagedServices-EnableOpenSearchLogging<br><br>OpenSearch los dominios están configurados con el registro de auditoría activado. | CloudWatchLogGroupArn: el ARN del grupo de CloudWatch registros en el que se van a publicar los registros.<br><br>Para habilitar la corrección automática, se debe proporcionar el siguiente parámetro preconfigurado: CloudWatchLogGroupArn<br><br>La política CloudWatch de recursos de Amazon debe configurarse con permisos. Para obtener más información, consulta Cómo habilitar los registros de auditoría en la Guía del usuario OpenSearch de Amazon Service. |
| Hs4Ma3G220: Las conexiones a los OpenSearch dominios deben cifrarse mediante TLS 1.2<br><br>Verificación correspondiente AWS Security Hub CSPM : Opensearch.8 | AWSManagedServices-EnableOpenSearchEndpointEncryptionTLS1.2<br><br>La política de TLS está configurada como `policy-MIN-TLS-1-2-2019-07` y solo se permiten las conexiones cifradas a través de HTTPS (TLS). | No se permiten parámetros preconfigurados.<br><br>Se requieren conexiones a los OpenSearch dominios para usar TLS 1.2. El cifrado de los datos en tránsito puede afectar al rendimiento. Pruebe sus aplicaciones con esta función para comprender el perfil de rendimiento y el impacto del TLS. |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| Hs4Ma3G194: La instantánea de Amazon RDS debe ser privada<br><br>Verificación correspondiente AWS Security Hub CSPM : RDS.1 | AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2<br><br>El acceso público a la instantánea de Amazon RDS está deshabilitado. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| Hs4Ma3G192: las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible AWS<br><br>Verificación correspondiente AWS Security Hub CSPM : RDS.2 | AWSManagedServices-TrustedRemediatorDisablePublicAccessOnRDSInstance<br><br>Inhabilite el acceso público a la instancia de base de datos de RDS. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
| --- | --- | --- |
| Hs4Ma3G189: la supervisión mejorada está configurada para las instancias de base de datos de Amazon RDS<br><br>Verificación correspondiente AWS Security Hub CSPM : RDS.6 | AWSManagedServices-TrustedRemediatorEnableRDSEnhancedMonitoring<br><br>Habilite una supervisión mejorada para las instancias de base de datos de Amazon RDS | • MonitoringInterval: El intervalo, en segundos, entre los puntos en los que se recopilan las métricas de supervisión mejorada para la instancia de base de datos. Los intervalos válidos son 0, 1, 5, 10, 15, 30 y 60. Para deshabilitar la recopilación de métricas de monitorización mejorada, especifique 0.<br>• MonitoringRoleName: el nombre de la función de IAM que permite a Amazon RDS enviar métricas de supervisión mejoradas a Amazon CloudWatch Logs. Si no se especifica un rol, se usa o `rds-monitoring-role` se crea el rol predeterminado, si no existe.<br><br>Si se habilita la supervisión mejorada antes de la ejecución de la automatización, esta automatización podría sobrescribir los ajustes con los MonitoringRoleName valores MonitoringInterval y configurados en los parámetros preconfigurados. |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
|---|---|---|
| Hs4Ma3G190: Los clústeres de Amazon RDS deben tener habilitada la protección de eliminación<br><br>Verificación correspondiente AWS Security Hub CSPM : RDS.7 | AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection<br><br>La protección contra la eliminación está habilitada para los clústeres de Amazon RDS. | No se permiten parámetros preconfig urados.<br><br>No hay restricciones |
| Hs4Ma3G198: Las instancias de base de datos de Amazon RDS deben tener habilitada la protección de eliminación<br><br>Verificación correspondiente AWS Security Hub CSPM : RDS.8 | AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection<br><br>La protección contra la eliminación está habilitada para las instancias de Amazon RDS. | No se permiten parámetros preconfig urados.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
| --- | --- | --- |
| Hs4Ma3G199: las instancias de base de datos de RDS deberían publicar los registros en Logs CloudWatch<br><br>Verificación correspondiente AWS Security Hub CSPM : RDS.9 | AWSManagedServices-TrustedRemediatorEnableRDSLogExports<br><br>La exportación de registros de RDS está habilitada para la instancia de base de datos de RDS o el clúster de base de datos de RDS. | No se permiten parámetros preconfig urados.<br><br>Se requiere el rol AWSServiceRoleForRDS vinculado al servicio. |
| Hs4Ma3G160: la autenticación de IAM debe configurarse para las instancias de RDS<br><br>Verificación correspondiente AWS Security Hub CSPM : RDS.10 | AWSManagedServices-UpdateRDSIAMDatabaseAuthentication<br><br>AWS Identity and Access Management la autenticación está habilitada para la instancia de RDS. | ApplyImmediately: Indica si las modificaciones de esta solicitud y las modificaciones pendientes se aplican de forma asíncrona lo antes posible. Para aplicar el cambio inmediata mente, elija. `true` Para programar el cambio para el siguiente período de mantenimiento, seleccione. `false`<br><br>Sin restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
| --- | --- | --- |
| Hs4Ma3G161: la autenticación de IAM debe configurarse para los clústeres de RDS<br><br>Verificación correspondiente AWS Security Hub CSPM : RDS.12 | AWSManagedServices-UpdateRDSIAMDatabaseAuthentication<br><br>La autenticación de IAM está habilitada para el clúster de RDS. | ApplyImmediately: Indica si las modificaciones de esta solicitud y las modificaciones pendientes se aplican de forma asíncrona lo antes posible. Para aplicar el cambio inmediatamente, seleccione. `true` Para programar el cambio para el siguiente período de mantenimiento, seleccione. `false`<br><br>Sin restricciones |
| Hs4Ma3G162: las actualizaciones automáticas de las versiones secundarias de RDS deberían estar habilitadas<br><br>Verificación correspondiente AWS Security Hub CSPM : RDS.13 | AWSManagedServices-UpdateRDSInstanceMinorVersionUpgrade<br><br>La configuración de actualización automática de versiones secundarias para Amazon RDS está habilitada. | No se permiten parámetros preconfigurados.<br><br>La instancia de Amazon RDS debe estar en ese `available` estado para que se produzca esta corrección. |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| Hs4Ma3G163: Los clústeres de bases de datos de RDS deben configurarse para copiar etiquetas en las instantáneas<br><br>Verificación correspondiente AWS Security Hub CSPM : RDS.16 | AWSManagedServices-UpdateRDSCopyTagsToSnapshots<br><br>`CopyTagtosnapshot` la configuración de los clústeres de Amazon RDS está habilitada. | No se permiten parámetros preconfigurados.<br><br>Las instancias de Amazon RDS deben estar en estado disponible para que se produzca esta corrección. |
| Hs4Ma3G164: las instancias de base de datos de RDS deben configurarse para copiar etiquetas en las instantáneas<br><br>Verificación correspondiente AWS Security Hub CSPM : RDS.17 | AWSManagedServices-UpdateRDSCopyTagsToSnapshots<br><br>`CopyTagsToSnapshot` la configuración de Amazon RDS está habilitada. | No se permiten parámetros preconfigurados.<br><br>Las instancias de Amazon RDS deben estar en estado disponible para que se produzca esta corrección. |
| RSS93 HQwa1<br><br>Instantáneas públicas de Amazon RDS | AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2<br><br>El acceso público a la instantánea de Amazon RDS está deshabilitado. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| Hs4Ma3G103: Los clústeres de Amazon Redshift deberían prohibir el acceso público<br><br>AWS Security Hub CSPM Comprobación correspondiente: Redshift.1 | AWSManagedServices-DisablePublicAccessOnRedshiftCluster<br><br>El acceso público al clúster de Amazon Redshift está deshabilitado. | No se permiten parámetros preconfigurados.<br><br>Al deshabilitar el acceso público, se bloquean todos los clientes que vienen de Internet. Además, el clúster de Amazon Redshift permanece en estado de modificación durante unos minutos mientras la corrección inhabilita el acceso público al clúster. |
| Hs4Ma3G106: Los clústeres de Amazon Redshift deben tener habilitado el registro de auditoría<br><br>AWS Security Hub CSPM Comprobación correspondiente: Redshift.4 | AWSManagedServices-TrustedRemediatorEnableRedshiftClusterAuditLogging<br><br>El registro de auditoría se habilita en el clúster de Amazon Redshift durante el período de mantenimiento. | No se permiten parámetros preconfigurados.<br><br>Para habilitar la corrección automática, se deben proporcionar los siguientes parámetros preconfigurados.<br><br>BucketName: El depósito debe estar en el mismo lugar. Región de AWS El clúster debe tener permisos de lectura y colocar objetos.<br><br>Si el registro del clúster de Redshift está habilitado antes de la ejecución de la automatización, esta automatización podría sobrescribir los ajustes de registro con `S3KeyPrefix` los valores `BucketName` y configurados en los parámetros preconfigurados. |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| Hs4Ma3G105: Amazon Redshift debería tener habilitadas las actualizaciones automáticas a las principales versiones<br><br>AWS Security Hub CSPM Comprobación correspondiente: Redshift.6 | AWSManagedServices-EnableRedshiftClusterVersionAutoUpgrade-Las principales actualizaciones de las versiones se aplican automáticamente al clúster durante el período de mantenimiento. No hay ningún tiempo de inactividad inmediato para el clúster de Amazon Redshift, pero su clúster de Amazon Redshift podría sufrir un tiempo de inactividad durante el período de mantenimiento si se actualiza a una versión principal. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| Hs4Ma3G104: Los clústeres de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado<br><br>AWS Security Hub CSPM Comprobación correspondiente: Redshift.7 | AWSManagedServices-TrustedRemediatorEnableRedshiftClusterEnhancedVPCRouting<br><br>El enrutamiento de VPC mejorado está habilitado para los clústeres de Amazon Redshift. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
| --- | --- | --- |
| Hs4Ma3G173: la configuración de acceso público del bloque S3 debe estar habilitada en el nivel del bucket<br><br>Verificación correspondiente AWS Security Hub CSPM: S3.8 | AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess<br><br>Los bloques de acceso público a nivel de bucket se aplican al bucket de Amazon S3. | No se permiten parámetros preconfigurados.<br><br>Esta corrección podría afectar a la disponibilidad de los objetos de S3. Para obtener información sobre cómo Amazon S3 evalúa el acceso, consulte Bloquear el acceso público a su almacenamiento de Amazon S3. |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
| --- | --- | --- |
| Hs4Ma3G230: el registro de acceso al servidor de bucket S3 debe estar habilitado<br><br>Verificación AWS Security Hub CSPM correspondiente: S3.9 | AWSManagedServices-EnableBucketAccessLogging(documento SSM predeterminado para el modo de ejecución automática y manual)<br><br>El registro de acceso al servidor Amazon S3 está activado. | • TargetBucket: El nombre del depósito de S3 para almacenar los registros de acceso al servidor.<br>• TargetObjectKeyFormat: formato de clave de Amazon S3 para objetos de registro (los valores distinguen entre mayúscula s y minúsculas). Para usar el formato simple de las claves S3 para los objetos de registro, elija`SimplePrefix` . Para usar la clave S3 particionada para los objetos de registro y usarla EventTime para el prefijo particionado, elija. `Partition edPrefixEventTime` Para usar la clave S3 particionada para los objetos de registro y usarla DeliveryTime para el prefijo particionado, elija. `Partition edPrefixDeliveryTime` Los valores admitidos son `SimplePre fix` , `PartitionedPrefixE ventTime` y `Partition edPrefixDeliveryTime` .<br><br>Para habilitar la corrección automátic a, se debe proporcionar el siguiente parámetro preconfigurado:. TargetBucket<br><br>El depósito de destino debe estar en el mismo depósito Región de |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
| --- | --- | --- |
| | | AWS y Cuenta de AWS al de origen, con los permisos correctos para la entrega de registros. Para obtener más información, consulte Habilitación del registro de acceso al servidor de Amazon S3. |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
| --- | --- | --- |
| Hs4Ma3G230: el registro de acceso al servidor de bucket S3 debe estar habilitado<br><br>Verificación AWS Security Hub CSPM correspondiente: S3.9 | AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2: El registro de buckets de Amazon S3 está activado. | • TargetBucketTagKey: El nombre de la etiqueta (distingue entre mayúsculas y minúsculas) para identificar el bucket de destino. Utilícelo TargetBucketTagValuepara etiquetar el depósito que se utilizará como depósito de destino para el registro de acceso.<br>• TargetBucketTagValue: El valor de la etiqueta (distingue entre mayúsculas y minúsculas) para identificar el depósito de destino, TargetBucketTagKeyutilícelo y etiquete el depósito para que se utilice como depósito de destino para el registro de acceso.<br>• TargetObjectKeyFormat: Formato de clave de Amazon S3 para objetos de registro (los valores distinguen entre mayúsculas y minúsculas): para usar el formato simple de las claves S3 para objetos de registro, elija SimplePrefix. Para usar la clave S3 particionada para los objetos de registro y usarla EventTime para el prefijo particionado, elija. PartitionedPrefixEventTime Para usar la clave S3 particionada para los objetos de registro y usarla DeliveryTime para el prefijo particionado, elija. PartitionedPrefixDeliveryTime El |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| | | valor predeterminado es PartitionedPrefixEventTime.<br><br>Para habilitar la corrección automática, se deben proporcionar los siguientes parámetros: TargetBucketTagKeyy TargetBucketTagValue.<br><br>El depósito de destino debe estar en el mismo depósito Región de AWS y Cuenta de AWS como el depósito de origen, con los permisos correctos para la entrega de registros. Para obtener más información, consulte Habilitación del registro de acceso al servidor de Amazon S3. |
| Pfx0 RwqBli<br><br>Permisos de bucket de Amazon S3 | AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess<br><br>Bloqueo del acceso público | No se permiten parámetros preconfigurados.<br><br>Esta comprobación consta de varios criterios de alerta. Esta automatización soluciona los problemas de acceso público. Trusted Advisor No se admite la corrección de otros problemas de configuración señalados por. Esta corrección sí permite corregir los buckets de S3 Servicio de AWS creados (por ejemplo, cf-templates-00000 0000000). |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
| --- | --- | --- |
| Hs4Ma3G272: Los usuarios no deberían tener acceso root a las instancia s de notebook SageMaker<br><br>Verificación SageMaker correspondiente AWS Security Hub CSPM: 3. | AWSManagedServices-TrustedR emediatorDisableSageMakerNo tebookInstanceRootAccess<br><br>El acceso root para los usuarios está deshabilitado en la instancia de SageMaker Notebook. | No se permiten parámetros preconfig urados.<br><br>Esta corrección provoca una interrupción si la instancia del SageMaker portátil está en ese estado. InService |
| Hs4Ma3G17 9: los temas de SNS deben cifrarse en reposo mediante AWS KMS<br><br>Verificación correspondiente AWS Security Hub CSPM : SNS.1 | AWSManagedServices-EnableSN SEncryptionAtRest<br><br>El tema de SNS está configurado con el cifrado del lado del servidor. | KmsKeyId: el ID de una clave maestra de cliente AWS gestionad a (CMK) para Amazon SNS o una CMK personalizada que se utilizará para el cifrado del lado del servidor (SSE). El valor predeterminado es. `alias/aws/sns`<br><br>Si se utiliza una AWS KMS clave personalizada, debe configurarse con los permisos correctos. Para obtener más información, consulte el tema Habilitar el cifrado del lado del servidor (SSE) para Amazon SNS |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
| --- | --- | --- |
| Hs4Ma3G158: los documentos SSM no deben ser públicos<br><br>Verificación correspondiente AWS Security Hub CSPM : SSM.4 | AWSManagedServices-TrustedRemediatorDisableSSMDocPublicSharing- Desactiva la compartición pública del documento SSM. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
| --- | --- | --- |
| Hs4Ma3G13 6: las colas de Amazon SQS deben cifrarse en reposo<br><br>Verificación correspondiente AWS Security Hub CSPM : SQS.1 | AWSManagedServices-EnableSQ SEncryptionAtRest<br><br>Los mensajes de Amazon SQS están cifrados. | • SqsManagedSseEnabled: Establecido en `true` para habilitar el cifrado de colas del lado del servidor mediante claves de cifrado propiedad de Amazon SQS, configurado en para `false` habilitar el cifrado de colas del lado del servidor mediante una clave. AWS KMS<br>• KMSKeyID: el ID o el alias de una clave maestra de cliente AWS gestionada (CMK) para Amazon SQS o una CMK personalizada que se utilizará para cifrar la cola en el servidor. Si no se proporcio na, se utiliza. alias/aws/sqs<br>• KmsDataKeyReusePeriodSecond s: El tiempo, en segundos, durante el que Amazon SQS puede reutilizar una clave de datos para cifrar o descifrar los mensajes antes de volver a llamar. AWS KMS Un entero que represent a segundos, entre 60 segundos (1 minuto) y 86 400 segundos (24 horas). Esta configuración se ignora si `SqsManagedSseEnabl ed` se establece en. `true`<br><br>Se rechazan ReceiveMessage las solicitudes anónimas SendMessa ge y a la cola cifrada. Todas las solicitudes hechas a las colas con |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
|---|---|---|
| | | SSE habilitado deben usar HTTPS y Signature Version 4. |

## Trusted Advisor las comprobaciones de tolerancia a errores son compatibles con Trusted Remediator

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
|---|---|---|
| c18d2gz138<br><br>Recuperación de Amazon DynamoDB Point-in-time | AWSManagedServices-TrustedRemediatorEnableDDBPITR<br><br>Permite point-in-time la recuperación de tablas de DynamoDB. | No se permiten parámetros preconfig urados.<br><br>No hay restricciones |
| R365S2qddf<br><br>Amazon S3 Bucket Versioning | AWSManagedServices-TrustedRemediatorEnableBucketVersioning<br><br>El control de versiones de bucket de Amazon S3 está activado. | No se permiten parámetros preconfig urados.<br><br>Esta corrección no permite corregir los buckets de S3 Servicio de AWS creados (por ejemplo, cf-templates-000000000000). |
| BueAdJ7nRP<br><br>Registro de bucket de Amazon S3 | AWSManagedServices-EnableBucketAccessLogging<br><br>El registro de buckets de Amazon S3 está activado. | • TargetBucket: el nombre del depósito de S3 para almacenar los registros de acceso al servidor.<br>• TargetObjectKeyFormat: formato de clave Amazon S3 para objetos de registro, si desea utilizar el formato simple de claves S3 para objetos de registro, elija`SimplePrefix` . Para usar la clave S3 particionada |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
| --- | --- | --- |
| | | para los objetos de registro y usarla EventTime para el prefijo particionado, elija. `Partition edPrefixEventTime` Para usar la clave S3 particionada para los objetos de registro y usarla DeliveryTime para el prefijo particionado, elija. `Partition edPrefixDeliveryTi me` El valor predeterminado es `PartitionedPrefixE ventTime` . Los valores válidos son`SimplePrefix` , `Partition edPrefixEventTime` y `PartitionedPrefixD eliveryTime` (distinguen mayúsculas de minúsculas).<br><br>Para habilitar la corrección automátic a, se deben proporcionar los siguientes parámetros preconfig urados:<br><br>• TargetBucket<br><br>El depósito de destino debe estar en el mismo depósito Región de AWS y Cuenta de AWS como el depósito de origen, con los permisos correctos para la entrega de registros. Para obtener más información, consulte Habilitación del registro de acceso al servidor de Amazon S3. |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| f2ik5r6dep<br><br>Amazon RDS Multi-AZ | AWSManagedServices-TrustedRemediatorEnableRDSMultiAZ<br><br>La implementación en zonas de disponibilidad múltiple está habilitada. | No se permiten parámetros preconfigurados.<br><br>Es posible que se produzca una degradación del rendimiento durante este cambio. |
| H7 IgTzj TYb<br><br>Instantáneas de Amazon EBS | AWSManagedServices-TrustedRemediatorCreateEBSSnapshot<br><br>EBSsnapshots Se crea Amazon. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| Top QPADk ZvH<br><br>Copias de seguridad de RDS | AWSManagedServices-EnableRDSBackupRetention<br><br>La retención de copias de seguridad de Amazon RDS está habilitada para la base de datos. | • BackupRetentionPeriod: El número de días (de 1 a 35) que se necesitan para conservar las copias de seguridad automatizadas.<br>• ApplyImmediately: Indica si el cambio de retención de la copia de seguridad de RDS y cualquier modificación pendiente se aplican de forma asíncrona lo antes posible. Elija `true` aplicar el cambio inmediatamente o programarlo `false` para el siguiente período de mantenimiento.<br><br>Si el `ApplyImmediately` parámetro está establecido en`true`, los cambios pendientes en la base de datos se aplican junto con la configuración RDSBackup de retención. |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
| --- | --- | --- |
| c1qf5bt013<br><br>Las instancias de base de datos de Amazon RDS tienen desactiva do el escalado automático del almacenamiento | AWSManagedServices-TrustedR emediatorEnableRDSInstanceS torageAutoScaling- El escalado automático del almacenamiento está habilitado para la instancia de base de datos de Amazon RDS. | • MaxAllocatedStorageIncrease Percentage: El porcentaje de aumento de la corriente Allocated Storage, para establecer el. MaxAllocatedStorage El valor predeterminado está establecido en26.<br><br>Debe establecer el umbral de almacenamiento máximo en al menos un 10% más que el almacenamiento asignado actualmente. Se recomienda establecer el umbral máximo de almacenamiento en al menos un 26% más. Para obtener más información, consulte Administr ar la capacidad automáticamente con el escalado automático del almacenamiento de Amazon Relational Database Service.<br><br>Sin restricciones |
| 7q GXs KlUw<br><br>Conexión Classic Load Balancer: Draining | AWSManagedServices-TrustedR emediatorEnableCLBConnectio nDraining<br><br>El drenaje de conexiones está activado en Classic Load Balancer. | ConnectionDrainingTimeout: El tiempo máximo, en segundos, para mantener abiertas las conexiones existentes antes de anular el registro de las instancias. El valor predeterm inado está establecido en segundos. `300`<br><br>Sin restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
|---|---|---|
| c18d2gz106<br><br>Amazon EBS no está incluido en el plan AWS Backup | AWSManagedServices-TrustedRemediatorAddVolumeToBackupPlan<br><br>Amazon EBS está incluido en el AWS Backup plan. | Remediation etiqueta el volumen de Amazon EBS con el siguiente par de etiquetas. El par de etiquetas debe coincidir con los criterios de selección de recursos basados en etiquetas de. AWS Backup<br><br>• TagKey<br>• TagValue<br><br>Sin restricciones |
| c18d2gz107<br><br>La tabla Amazon DynamoDB no está incluida en el plan AWS Backup | AWSManagedServices-TrustedRemediatorAddDynamoDBToBackupPlan<br><br>La tabla Amazon DynamoDB se incluye en el plan. AWS Backup | Remediation etiqueta Amazon DynamoDB con el siguiente par de etiquetas. El par de etiquetas debe coincidir con los criterios de selección de recursos basados en etiquetas de. AWS Backup<br><br>• TagKey<br>• TagValue<br><br>Sin restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| c18d2gz117<br><br>Amazon EFS no está incluido en el AWS Backup plan | AWSManagedServices-TrustedRemediatorAddEFSToBackupPlan<br><br>Amazon EFS está incluido en el AWS Backup plan. | Remediation etiqueta Amazon EFS con el siguiente par de etiquetas. El par de etiquetas debe coincidir con los criterios de selección de recursos basados en etiquetas de. AWS Backup<br><br>• TagKey<br>• TagValue<br><br>Sin restricciones |
| c18d2gz105<br><br>Equilibrador de carga cruzado del equilibrador de carga de red | AWSManagedServices-TrustedRemediatorEnableNLBCrossZoneLoadBalancing<br><br>El equilibrio de carga entre zonas está habilitado en Network Load Balancer. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| c1qf5bt026<br><br>El `synchronous_commit` parámetro Amazon RDS está desactivado | AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter<br><br>`synchronous_commit` El parámetro está activado en Amazon RDS. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| c1qf5bt030<br><br>El `innodb_flush_log_at_trx_commit` parámetro Amazon RDS no es 1 | AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter<br><br>`innodb_flush_log_at_trx_commit` El parámetro está establecido en 1 Amazon RDS. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| c1qf5bt031<br><br>El `sync_binlog` parámetro Amazon RDS está desactivado | AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter<br><br>`sync_binlog` El parámetro está activado en Amazon RDS. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| c1qf5bt036<br><br>La configuración de `innodb_default_row_format` parámetros de Amazon RDS no es segura | AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter<br><br>`innodb_default_row_format` El parámetro está establecido en `DYNAMIC` Amazon RDS. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| c18d2gz144<br><br>La supervisión detallada de Amazon EC2 no está habilitada | AWSManagedServices-TrustedRemediatorEnableEC2InstanceDetailedMonitoring<br><br>La monitorización detallada está habilitada para Amazon EC2. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |

## Trusted Advisor las comprobaciones de rendimiento son compatibles con Trusted Remediator

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
|---|---|---|
| COr6dfpM06<br><br>AWS Lambda funciones insuficie ntemente aprovisionadas para el tamaño de la memoria | AWSManagedServices-ResizeLa mbdaMemory<br><br>El tamaño de la memoria de las funciones Lambda se redimensiona al tamaño de memoria recomendado proporcionado por. Trusted Advisor | RecommendedMemorySize: la asignación de memoria recomenda da para la función Lambda. El rango de valores está entre 128 y 10240.<br><br>Si el tamaño de la función Lambda se modifica antes de la ejecución de la automatización, esta automatiz ación podría sobrescribir la configura ción con el valor recomendado por. Trusted Advisor |
| ZRxQlPsb6c<br><br>Uso elevado de instancias de Amazon EC2 | AWSManagedServices-ResizeIn stanceByOneLevel<br><br>Las instancias Amazon EC2 se redimensionan en un tipo de instancia superior en el mismo tipo de familia de instancias. Las instancias se detienen e inician durante la operación de cambio de tamaño y vuelven al estado inicial una vez finalizada la ejecución. Esta automatización no admite el cambio de tamaño de las instancias que se encuentran en un grupo de Auto Scaling. | • MinimumDaysSinceLastChange: El número mínimo de días transcurr idos desde el último cambio de tipo de instancia. Si el tipo de instancia se modificó dentro del tiempo especificado, el tipo de instancia no cambia. Se usa `0` para omitir esta validación. El valor predeterm inado es 7.<br>• Crear AMIBefore cambio de tamaño: para crear la AMI de la instancia como copia de seguridad antes de cambiar el tamaño, elija`true`. Para no crear una copia de seguridad, elija`false`. El valor predeterminado es `false`. Los valores válidos son `true` y `false` (distinguen mayúsculas de minúsculas). |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
|---|---|---|
| | | • ResizeIfStopped: Para continuar con el cambio de tamaño de la instancia, incluso si la instancia está detenida, elija`true`. Para no cambiar automáticamente el tamaño de la instancia si está detenida, elija`false`. Los valores válidos son `true` y `false` (distinguen mayúsculas de minúsculas).<br><br>Sin restricciones |
| c1qf5bt021<br><br>`innodb_ch ange_buff ering` Parámetro de Amazon RDS que utiliza un valor inferior al óptimo | AWSManagedServices-TrustedR emediatorRemediateRDSParame terGroupParameter<br><br>El valor del `innodb_change_buff ering` parámetro se establece en `NONE` Amazon RDS. | No se permiten parámetros preconfig urados.<br><br>No hay restricciones |
| c1qf5bt025<br><br>El `autovacuu m` parámetro Amazon RDS está desactivado | AWSManagedServices-TrustedR emediatorRemediateRDSParame terGroupParameter<br><br>`autovacuum` El parámetro está activado en Amazon RDS. | No se permiten parámetros preconfig urados.<br><br>No hay restricciones |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| c1qf5bt028<br><br>El `enable_indexonlyscan` parámetro Amazon RDS está desactivado | AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter<br><br>`enable_indexonlyscan` El parámetro está activado en Amazon RDS. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| c1qf5bt029<br><br>El `enable_indexscan` parámetro Amazon RDS está desactivado | AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter<br><br>`enable_indexscan` El parámetro está activado en Amazon RDS. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| c1qf5bt032<br><br>El `innodb_stats_persistent` parámetro Amazon RDS está desactivado | AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter<br><br>`innodb_stats_persistent` El parámetro está activado en Amazon RDS. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| c1qf5bt037<br><br>El `general_logging` parámetro Amazon RDS está activado | AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter<br><br>`general_logging` El parámetro está desactivado en Amazon RDS. | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |

## Trusted Advisor las comprobaciones de límites de servicio son compatibles con Trusted Remediator

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| IN7 J9 RR0l7<br><br>Dirección IP elástica de EC2-VPC | AWSManagedServices-UpdateVpcElasticIPQuota<br><br>Se solicita un nuevo límite para las direcciones IP elásticas de EC2-VPC. De forma predeterminada, el límite se incrementa en 3. | Incremento: el número para aumentar la cuota actual. El valor predeterminado es 3.<br><br>Si esta automatización se ejecuta varias veces antes de que la Trusted Advisor comprobación se actualice con el 0K estado, es posible que se produzca un aumento del límite superior. |
| mM7QQ0l7, J9<br><br>Gateways de Internet de VPC | AWSManagedServices-IncreaseServiceQuota- Se solicita un nuevo límite para las pasarelas de Internet de VPC. De forma predeterminada, el límite se incrementa en tres. | Incremento: el número para aumentar la cuota actual. El valor predeterminado es 3.<br><br>Si esta automatización se ejecuta varias veces antes de que la Trusted Advisor comprobación se actualice con el 0K estado, es posible que se produzca un aumento del límite superior. |
| JL7 J9 PP0l7<br><br>VPC | AWSManagedServices-IncreaseServiceQuota<br><br>Se solicita un nuevo límite para la VPC. De forma predeterminada, el límite se incrementa en 3. | Incremento: el número para aumentar la cuota actual. El valor predeterminado es 3.<br><br>Si esta automatización se ejecuta varias veces antes de que la Trusted Advisor comprobación se actualice con el 0K estado, es posible que se produzca un aumento del límite superior. |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| fW7 M9 HH0l7<br><br>Grupos de Auto Scaling | AWSManagedServices-IncreaseServiceQuota<br><br>Se solicita un nuevo límite para los grupos de Auto Scaling. De forma predeterminada, el límite se incrementa en 3. | Incremento: el número para aumentar la cuota actual. El valor predeterminado es 3.<br><br>Si esta automatización se ejecuta varias veces antes de que la Trusted Advisor comprobación se actualice con el 0K estado, es posible que se produzca un aumento del límite superior. |
| 3 Njm0 DJQO9<br><br>Grupos de opciones de RDS | AWSManagedServices-IncreaseServiceQuota<br><br>Se solicita un nuevo límite para los grupos de opciones de Amazon RDS. De forma predeterminada, el límite se incrementa en 3. | Incremento: el número para aumentar la cuota actual. El valor predeterminado es 3.<br><br>Si esta automatización se ejecuta varias veces antes de que la Trusted Advisor comprobación se actualice con el 0K estado, es posible que se produzca un aumento del límite superior. |
| EM8b3yLRTr<br><br>Application Load Balancers de ELB | AWSManagedServices-IncreaseServiceQuota<br><br>Se solicita un nuevo límite para los balanceadores de carga de aplicaciones ELB. De forma predeterminada, el límite se incrementa en 3. | Incremento: el número para aumentar la cuota actual. El valor predeterminado es 3.<br><br>Si esta automatización se ejecuta varias veces antes de que la Trusted Advisor comprobación se actualice con el 0K estado, es posible que se produzca un aumento del límite superior. |

| Compruebe la ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
|---|---|---|
| 8WiQ K YSt25<br><br>Network Load Balancers de ELB | AWSManagedServices-Increase ServiceQuota<br><br>Se solicita un nuevo límite para los balanceadores de carga de red ELB. De forma predeterminada, el límite se incrementa en 3. | Incremento: el número para aumentar la cuota actual. El valor predeterminado es 3.<br><br>Si esta automatización se ejecuta varias veces antes de que la Trusted Advisor comprobación se actualice con el 0K estado, es posible que se produzca un aumento del límite superior. |

## Trusted Advisor comprobaciones de excelencia operativa respaldadas por Trusted Remediator

| Compruebe la identificación y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
|---|---|---|
| c18d2gz125<br><br>La Amazon API Gateway no registra los registros de ejecución | AWSManagedServices-TrustedR emediatorEnableAPIGateWayEx ecutionLogging<br><br>El registro de ejecución está habilitad o en la fase API. | No se permiten parámetros preconfig urados.<br><br>Debe conceder permiso a API Gateway para leer y escribir los registros de su cuenta a CloudWatc h fin de habilitar el registro de ejecución; consulte Configurar el CloudWatch registro para REST APIs en API Gateway para obtener más información. |
| c18d2gz168<br><br>La protección contra eliminaci | AWSManagedServices-TrustedR emediatorEnableELBDeletionP rotection- La protección contra | No se permiten parámetros preconfig urados.<br><br>No hay restricciones |

| Compruebe la identificación y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
| --- | --- | --- |
| ón de Elastic Load Balancing no está habilitad a para los equilibradores de carga | eliminación está activada en el Elastic Load Balancer. | |
| c1qf5bt012<br><br>La información de rendimiento de Amazon RDS está desactivada | AWSManagedServices-TrustedR emediatorEnableRDSPerforman ceInsights<br><br>Performance Insights está activado en Amazon RDS. | • PerformanceInsightsRetentio nPeriod: El número de días necesarios para conservar los datos de Performance Insights. Valores válidos: 7 o mes * 31, donde el mes es un número de meses comprendido entre 1 y 23. Ejemplos: 93 (3 meses* 31), 341 (11 meses* 31), 589 (19 meses* 31) o731.<br>• PerformanceInsightsKMSKeyID : el identificador AWS KMS clave para el cifrado de los datos de Performance Insights. Si no especificas un valor para el PerformanceInsights KMSKey identificador, Amazon RDS utilizará la AWS KMS clave predeterminada.<br><br>Sin restricciones |

| Compruebe la identificación y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
| --- | --- | --- |
| c1fd6b96l4<br><br>Registros de acceso de Amazon S3 habilitados | AWSManagedServices-TrustedR emediatorEnableBucketAccess LoggingV2<br><br>El registro de acceso al bucket de Amazon S3 está activado. | • TargetBucketTagValue: Utilice el valor de la etiqueta (distingue entre mayúsculas y minúsculas) TargetBucketTagKey para identific ar el bucket de destino y etiquetar lo como bucket de destino para el registro de acceso.<br>• TargetObjectKeyFormat: formato de clave de Amazon S3 para objetos de registro (los valores distinguen entre mayúscula s y minúsculas). Para usar el formato simple de las claves S3 para los objetos de registro, elija`SimplePrefix` . Para usar la clave S3 particionada para los objetos de registro y usarla EventTime para el prefijo particionado, elija. `Partition edPrefixEventTime` Para usar la clave S3 particionada para los objetos de registro y usarla DeliveryTime para el prefijo particionado, elija. `Partition edPrefixDeliveryTime` Los valores admitidos son `SimplePre fix` , `PartitionedPrefixE ventTime` y `Partition edPrefixDeliveryTime` .<br><br>Para habilitar la corrección automátic a, se debe proporcionar el siguiente |

| Compruebe la identificación y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| | | parámetro preconfigurado: TargetBucketTagKeyy. TargetBucketTagValue<br><br>El depósito de destino debe estar en el mismo depósito Región de AWS y Cuenta de AWS como el depósito de origen, con los permisos correctos para la entrega de registros. Para obtener más información, consulte Habilitación del registro de acceso al servidor de Amazon S3. |

## Trusted Remediator apoya las recomendaciones de Security Hub (CSPM)

En la siguiente tabla se enumeran las recomendaciones de CSPM de Security Hub compatibles, los documentos de automatización de SSM, los parámetros preconfigurados y el resultado esperado de los documentos de automatización. Revise el resultado esperado para ayudarle a comprender los posibles riesgos en función de los requisitos de su empresa antes de utilizar un documento de automatización de SSM para corregir las comprobaciones.

Asegúrese de habilitar Security Hub CSPM para la cuenta. Para obtener más información, consulte Habilitar Security Hub CSPM.

| Compruebe el ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
|---|---|---|
| Centro de seguridad IAM-22<br><br>IAM.22: Deben eliminarse las credenciales de usuario de IAM | AWSManagedServices-TrustedRemediatorDeactivateIamUserUnusedCredentials | DeleteAccessKeys: Configúrelo en true para eliminar permanentemente las claves de acceso no utilizadas, o en false para desactivarlas (haciendo que estén inactivas pero se puedan recuperar).<br><br>Sin restricciones |

| Compruebe el ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfigurados compatibles |
| --- | --- | --- |
| que no se hayan utilizado durante 45 días. | | |
| Centro de seguridad IAM-3<br><br>IAM.3: Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos. | AWSManagedServices-TrustedRemediatorRotateIamAccessKeysOlderThan90 días | No se permiten parámetros preconfigurados.<br><br>No hay restricciones |
| Centro de seguridad IAM-8<br><br>IAM.8: Se deben eliminar las credenciales de usuario de IAM no utilizadas. | AWSManagedServices-TrustedRemediatorDeactivateIamUserUnusedCredentials | DeleteAccessKeys: Configúrelo en True para eliminar permanentemente las claves de acceso no utilizadas, o en False para desactivarlas (haciendo que estén inactivas pero se puedan recuperar).<br><br>Sin restricciones |

| Compruebe el ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
|---|---|---|
| security-hub-networkfirewall-10<br><br>NetworkFirewall.10: Los firewalls de Network Firewall deben tener habilitada la protección contra cambios de subred. | AWSManagedServices-TrustedRemediatorEnableNetworkFirewallSubnetChangeProtection | No se permiten parámetros preconfig urados.<br><br>No hay restricciones |
| security-hub-networkfirewall-2<br><br>NetworkFirewall.2: El registro de Network Firewall debe estar habilitado. | AWSManagedServices-TrustedRemediatorEnableNetworkFirewallCloudWatchLog | LogGroupName: el nombre del grupo de CloudWatch registros al que se van a enviar los registros.<br><br>LogTypes: los tipos de registros que se van a habilitar. Los valores válidos son `FLOW`, `ALERT`, `TLS`.<br><br>Sin restricciones |
| security-hub-stepfunctions-1<br><br>StepFunctions.1: Step Functions indica que las máquinas deberían tener el registro activado. | AWSManagedServices-TrustedRemediatorEnableStepFunctionsLogging | LogGroupName: el nombre del grupo de registros para el CloudWatch registro de Step Functions.<br><br>LoggingLevel: El nivel de registro de Step Functions. Los valores válidos son `ALL`, `ERROR`, `FATAL`. |

| Compruebe el ID y el nombre | Nombre del documento SSM y resultado esperado | Parámetros y restricciones preconfig urados compatibles |
|---|---|---|
| security-hub-lambda-7<br><br>Lambda.7: Las funciones de Lambda deben tener habilitado el rastreo activo de AWS X-Ray. | AWSManagedServices-TrustedRemediatorEnableLambdaXrayActiveTracing | No se permiten parámetros preconfig urados.<br><br>No hay restricciones |

## Configurar la corrección de Trusted Advisor comprobaciones en Trusted Remediator

Las configuraciones se almacenan AWS AppConfig como parte de la aplicación Trusted Remediator. Cada categoría de Trusted Advisor comprobación tiene un perfil de configuración independiente. Para obtener más información sobre Trusted Advisor las categorías, consulte Ver las categorías de verificación.

Puede configurar las correcciones por recurso o por Trusted Advisor comprobación. Puede aplicar excepciones mediante etiquetas de recursos.

> **Note**
>
> La corrección de Trusted Advisor los hallazgos se configura actualmente mediante AWS AppConfig, y esta función es totalmente compatible en la actualidad. AMS anticipa que esto cambiará en el futuro. Se recomienda evitar crear automatizaciones que dependan de ellas AWS AppConfig, ya que este método está sujeto a cambios. Tenga en cuenta que es posible que necesite actualizar o modificar las automatizaciones creadas en torno a la AWS AppConfig implementación actual en el futuro para garantizar la compatibilidad.
> El indicador de función Compute Optimizer -> Instancias EC2 tiene parámetros adicionales:
>
> - allow-upscale Para permitir la ampliación de instancias EC2, subaprovisionadas y no optimizadas. El valor predeterminado es “false”.

- min-savings-opportunity-percentageLa oportunidad mínima de porcentaje de ahorro para la remediación automatizada. El valor predeterminado es el 10%

## Configuraciones de corrección predeterminadas

Las configuraciones de las Trusted Advisor comprobaciones individuales se almacenan como AWS AppConfig indicadores. El nombre de la bandera coincide con el nombre del cheque. Cada configuración de verificación contiene los siguientes atributos:

- modo de ejecución: determina cómo Trusted Remediator realiza la corrección predeterminada:
  - Automatizado: Trusted Remediator corrige automáticamente los recursos creando un documento SSM OpsItem, ejecutándolo y resolviéndolo después tras una ejecución correcta. OpsItem
  - Manual: OpsItem se crea un documento SSM, pero no se ejecuta automáticamente. El documento SSM se revisa y se ejecuta manualmente desde OpsItem la AWS Systems Manager OpsCenter consola.
  - Condicional: la corrección está deshabilitada de forma predeterminada. Puede habilitarla para recursos específicos mediante etiquetas. Para obtener más información, consulte las siguientes secciones Personalice la remediación con etiquetas de recursos yPersonalice la remediación con etiquetas de anulación de recursos.
  - Inactivo: no se produce ninguna corrección y no OpsItem se crea ninguna. No puede anular el modo de ejecución de la Trusted Advisor comprobación que está configurada como inactiva.
- parámetros preconfigurados: introduzca valores para los parámetros del documento SSM necesarios para la corrección automática, en el formato de, separados por una coma (`Parameter=Value`,). Consulte los parámetros preconfigurados compatibles Trusted Advisor comprobaciones compatibles con Trusted Remediator para el documento SSM asociado a cada comprobación.
- alternative-automation-document: Este atributo ayuda a sustituir el documento de automatización existente por otro documento compatible (si está disponible para la comprobación específica). De forma predeterminada, este atributo no está seleccionado.

> **Note**
>
> El `alternative-automation-document` atributo no admite documentos de automatización personalizados. Puede utilizar los documentos de automatización de

Trusted Remediator compatibles existentes que figuran enTrusted Advisor comprobaciones compatibles con Trusted Remediator.
Por ejemplo, para comprobarloQch7DwouX1, hay tres documentos SSM asociados: AWSManagedServices-StopEC 2Instance, y AWSManagedServices-ResizeInstanceByOneLevel. AWSManagedServices-TerminateInstance El valor de `alternative-automation-document` puede ser uno de los dos AWSManagedServices-ResizeInstanceByOneLevel AWSManagedServices-TerminateInstance (AWSManagedServices-StopEC2Instance es el documento SSM predeterminado que se debe corregir). Qch7DwouX1

El valor de cada atributo debe coincidir con las restricciones de ese atributo.

**Tip**

Antes de aplicar las configuraciones predeterminadas a las Trusted Advisor comprobaciones, se recomienda considerar el uso de las funciones de etiquetado y anulación de recursos que se describen en las siguientes secciones. Las configuraciones predeterminadas se aplican a todos los recursos de la cuenta, lo que puede no ser conveniente en todos los casos.

A continuación, se muestra un ejemplo de captura de pantalla de una consola con el modo de ejecución configurado en Manual y los atributos que coinciden con sus restricciones.

## Personalice la remediación con etiquetas de recursos

Los manual-for-tagged-onlyatributos automated-for-tagged-onlyy de la configuración de comprobación le permiten especificar etiquetas de recursos para corregir las comprobaciones individuales. Se recomienda utilizar este método cuando se necesita aplicar un comportamiento de corrección coherente a un grupo de recursos que comparten la misma etiqueta o etiquetas. Las siguientes son descripciones de estas etiquetas:

- automated-for-tagged-only: especifique las etiquetas de recursos (uno o más pares de etiquetas, separadas por comas) para que las comprobaciones se corrijan automáticamente, independientemente del modo de ejecución predeterminado.

- manual-for-tagged-only: especifique las etiquetas de recursos (uno o más pares de etiquetas, separadas por comas) para las correcciones que deben ejecutarse manualmente, independientemente del modo de ejecución predeterminado.

Por ejemplo, si desea habilitar la corrección automática para todos los recursos que no son de producción y aplicar la corrección manual para los recursos de producción, puede establecer la configuración de la siguiente manera:

```
"execution-mode": "Conditional",
"automated-for-tagged-only": "Environment=Non-Production",
"manual-for-tagged-only": "Environment=Production",
```

Con las configuraciones anteriores configuradas en sus recursos, compruebe que el comportamiento de la corrección sea el siguiente:

- Los recursos etiquetados con la etiqueta «Entorno = no producción» se corrigen automáticamente.
- Los recursos etiquetados con la etiqueta «Medio ambiente = producción» requieren una intervención manual para su remediación.
- Los recursos sin la etiqueta «Medio ambiente» siguen el modo de ejecución predeterminado («Condicional», en este caso). Por lo tanto, no se realiza ninguna acción con los recursos restantes).

Para obtener asistencia adicional con sus configuraciones, póngase en contacto con su arquitecto de nube.

## Personalice la remediación con etiquetas de anulación de recursos

Las etiquetas de anulación de recursos permiten personalizar el comportamiento de corrección de los recursos individuales, independientemente de sus etiquetas. Al añadir una etiqueta específica a un recurso, se anula el modo de ejecución predeterminado para ese recurso y la comprobación. Trusted Advisor La etiqueta de anulación de recursos tiene prioridad sobre la configuración predeterminada y la configuración de etiquetado de recursos. Por lo tanto, si establece el modo de ejecución predeterminado en Automatizado, Manual o Condicional para un recurso mediante la etiqueta de anulación de recursos, anulará el modo de ejecución predeterminado y cualquier configuración de etiquetado de recursos.

Para anular el modo de ejecución de un recurso, complete los siguientes pasos:

1. Identifique los recursos para los que desea anular la configuración de corrección.
2. Determine el Trusted Advisor identificador de la verificación que desea anular. Puedes encontrar la verificación de los IDs registros admitidos Trusted Advisor . Trusted Advisor comprobaciones compatibles con Trusted Remediator
3. Añada una etiqueta a los recursos con la siguiente clave y valor:

   - Clave de etiqueta: `TR-`*`Trusted Advisor check ID`*`-Execution-Mode` (distingue entre mayúsculas y minúsculas)

     En el ejemplo de clave de etiqueta anterior, `Trusted Advisor check ID` sustitúyala por el identificador único de la Trusted Advisor marca que deseas anular.
   - Valor de etiqueta: utilice uno de los siguientes valores para el valor de etiqueta:
     - Automatizado: Trusted Remediator corrige automáticamente el recurso para esta Trusted Advisor comprobación.
     - Manual: OpsItem se crea una para el recurso, pero la corrección no se realiza automáticamente. La corrección se revisa y se ejecuta manualmente desde. OpsItem
     - Inactivo: la corrección y OpsItem la creación no se realizan para este recurso ni para la comprobación especificada Trusted Advisor .

Por ejemplo, para corregir automáticamente un volumen de Amazon EBS con el identificador de Trusted Advisor verificación, `DAvU99Dc4C` añada una etiqueta al volumen de EBS. La clave de la etiqueta es `TR-DAvU99Dc4C-Execution-Mode` y el valor de la etiqueta es. `Automated`

A continuación, se muestra un ejemplo de la consola que muestra la sección Etiquetas:

## Flujo de trabajo de decisiones en modo ejecución

Existen varios niveles para configurar el modo de ejecución de sus recursos y de cada Trusted Advisor comprobación. El siguiente diagrama muestra cómo Trusted Remediator decide qué modo de ejecución utilizar en función de sus configuraciones:

## Configurar tutoriales de remediación

Los siguientes tutoriales proporcionan ejemplos de cómo crear soluciones comunes en Trusted Remediator

## Corrija todos los recursos manualmente

Este ejemplo configura la corrección manual para todos los volúmenes de Amazon EBS con el identificador de Trusted Advisor comprobación DAv U99Dc4C (volúmenes de Amazon EBS subutilizados).

Configurar la corrección manual para los volúmenes de Amazon EBS con el identificador de comprobación U99Dc4C DAv

1. Abra la consola en appconfig. AWS AppConfig https://console.aws.amazon.com/systems-manager/

   Asegúrese de iniciar sesión con la cuenta de administrador delegado.
2. Seleccione Trusted Remediator en la lista de aplicaciones.
3. Elija el perfil de configuración de optimización de costes.
4. Seleccione el indicador de volúmenes de Amazon EBS infrautilizados.
5. Para el modo de ejecución, seleccione Manual.
6. Asegúrese de que los manual-for-tagged-onlyatributos automated-for-tagged-onlyy estén en blanco. Estos atributos se utilizan para anular el modo de ejecución predeterminado para los recursos con etiquetas coincidentes.

   A continuación se muestra un ejemplo de la sección Atributos con valores en blanco para automated-for-tagged-onlymanual-for-tagged-onlyy Manual para el modo de ejecución:

7. Seleccione Guardar para actualizar el valor y, a continuación, seleccione Guardar nueva versión para aplicar los cambios. Debe seleccionar Guardar nueva versión para que Trusted Remediator reconozca el cambio.
8. Asegúrese de que sus volúmenes de Amazon EBS no tengan una etiqueta con la claveTR-DAvU99Dc4C-Execution-Mode. Esta clave de etiqueta anula el modo de ejecución predeterminado para ese volumen de EBS.

## Corrija todos los recursos automáticamente, excepto los recursos seleccionados

En este ejemplo, se configura la corrección automática para todos los volúmenes de Amazon EBS con el identificador de Trusted Advisor comprobación DAv U99Dc4C (volúmenes de Amazon EBS subutilizados), con la excepción de los volúmenes especificados que no se van a corregir (denominados inactivos).

Configure la corrección automática para los volúmenes de Amazon EBS con el identificador de verificación DAv U99Dc4C, con la excepción de los recursos inactivos seleccionados

1. Abra la consola en appconfig. AWS AppConfig https://console.aws.amazon.com/systems-manager/

   Asegúrese de iniciar sesión con la cuenta de administrador delegado.
2. Seleccione Trusted Remediator en la lista de aplicaciones.
3. Elija el perfil de configuración de optimización de costes.
4. Seleccione el indicador de volúmenes de Amazon EBS infrautilizados.
5. Para el modo de ejecución, seleccione Automatizado.
6. Asegúrese de que los manual-for-tagged-onlyatributos automated-for-tagged-onlyy estén en blanco. Estos atributos se utilizan para anular el modo de ejecución predeterminado para los recursos con etiquetas coincidentes.

   A continuación se muestra un ejemplo de la sección Atributos con valores en blanco para automated-for-tagged-onlymanual-for-tagged-onlyy Automatizado para el modo de ejecución:

7. Seleccione Guardar para actualizar el valor y, a continuación, seleccione Guardar nueva versión para aplicar los cambios. Debe seleccionar Guardar nueva versión para que Trusted Remediator reconozca el cambio.

   En este punto, todos los volúmenes de Amazon EBS están configurados para su corrección automática.
8. Anule la corrección automática para volúmenes de Amazon EBS seleccionados:

   a. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
   b. Elija Elastic Block Store, Volumes.
   c. Seleccione Tags (Etiquetas).
   d. Elija Administrar etiquetas.
   e. Añada la siguiente etiqueta:

      - Clave: Modo de ejecución TR- DAv U99Dc4C
      - Valor: Inactivo

      El siguiente es un ejemplo de la sección Etiquetas que muestra los campos Clave y Valor:

f. Repita los pasos 2 a 5 para todos los volúmenes de Amazon EBS que desee excluir de la corrección.

## Corrija los recursos etiquetados automáticamente

Este ejemplo configura la corrección automática para todos los volúmenes de Amazon EBS con la etiqueta `Stage=NonProd` con el identificador de Trusted Advisor comprobación DAv U99Dc4C (volúmenes de Amazon EBS subutilizados). Los demás recursos sin esta etiqueta no se corrigen.

Configure la corrección automática para los volúmenes de Amazon EBS con la etiqueta **`Stage=NonProd`** para el ID de comprobación U99Dc4C DAv

1. Abra la consola en appconfig. AWS AppConfig https://console.aws.amazon.com/systems-manager/

   Asegúrese de iniciar sesión con la cuenta de administrador delegado.
2. Seleccione Trusted Remediator en la lista de aplicaciones.
3. Elija el perfil de configuración de optimización de costes.
4. Seleccione el indicador de volúmenes de Amazon EBS infrautilizados.
5. Para el modo de ejecución, seleccione Condicional.
6. Configure el automated-for-tagged-only en `Stage=NonProd`. Este atributo anula el valor predeterminado `execution-mode` para los recursos con etiquetas coincidentes. Asegúrese de que los manual-for-tagged-onlyatributos estén en blanco.

   A continuación, se muestra un ejemplo de la sección de atributos automated-for-tagged-onlyconfigurada en Stage= NonProd y Conditional en el modo de ejecución:

7. Si lo desea, defina los parámetros preconfigurados en uno de los siguientes valores:

   - `CreateSnapshot=false`para no crear una instantánea del volumen de Amazon EBS antes de eliminarlo
   - `MinimumUnattachedDays=10`establecer un mínimo de 10 días sin adjuntar del volumen de Amazon EBS que se va a eliminar
   - `CreateSnapshot=false`, `MinimumUnattachedDays=10` para los dos casos anteriores

8. Seleccione Guardar para actualizar el valor y, a continuación, seleccione Guardar nueva versión para aplicar los cambios. Debe seleccionar Guardar nueva versión para que Trusted Remediator reconozca el cambio.
9. Asegúrese de que sus volúmenes de Amazon EBS no tengan una etiqueta con la claveTR-DAvU99Dc4C-Execution-Mode. Esta clave de etiqueta anula el modo de ejecución predeterminado para ese volumen de EBS.

# Trabaje con las soluciones en Trusted Remediator

## Realice un seguimiento de las correcciones en Trusted Remediator

Para realizar un seguimiento de OpsItems las correcciones, siga estos pasos:

1. Abra la AWS Systems Manager consola en. https://console.aws.amazon.com/systems-manager/
2. Elija Administración de operaciones, OpsCenter.
3. (Opcional) Filtre la lista por Source=Trusted Remediator para incluir solo Trusted Remediator OpsItems en la lista.

   A continuación se muestra un ejemplo de la OpsCenter pantalla filtrada por Source=Trusted Remediator:

> **Note**
>
> Además OpsItems de verlos desde OpsCenter, puede ver los registros de corrección del bucket AMS S3. Para obtener más información, consulte Registros de remediación en Trusted Remediator.

## Ejecute las correcciones manuales en Trusted Remediator

Trusted Remediator crea comprobaciones configuradas OpsItems para la corrección manual. Debe revisar estas comprobaciones e iniciar el proceso de corrección manualmente.

Para solucionarlo manualmente OpsItem, complete los siguientes pasos:

1. Abra la AWS Systems Manager consola en. https://console.aws.amazon.com/systems-manager/

2. Elija Administración de operaciones, OpsCenter.
3. (Opcional) Filtre la lista por Source=Trusted Remediator para incluir solo Trusted Remediator OpsItems en la lista.
4. Elija lo OpsItem que desee revisar.
5. Revise los datos operativos del OpsItem. Los datos operativos incluyen los siguientes elementos:

   - trustedAdvisorCheckCategoría: la categoría del identificador del Trusted Advisor cheque. Por ejemplo, tolerancia a errores
   - trustedAdvisorCheckID: el identificador de Trusted Advisor verificación único.
   - trustedAdvisorCheckMetadatos: los metadatos del recurso, incluido el ID del recurso.
   - trustedAdvisorCheckNombre: el nombre de la Trusted Advisor comprobación.
   - trustedAdvisorCheckEstado: el estado de la Trusted Advisor comprobación detectada para el recurso.

6. Para solucionarlo manualmente OpsItem, complete los siguientes pasos:

   a. En Runbooks, elija uno de los runbooks asociados (documentos SSM).
   b. Elija Ejecutar.
   c. En AutomationAssumeRole , elija `arn:aws:iam::`*`Cuenta de AWS ID`*`:role/ams_ssm_automation_role`. Sustituya el Cuenta de AWS ID por el ID de la cuenta en la que se ejecuta la corrección. Para ver otros valores de parámetros, consulte los datos de la operación.

      Para corregir los recursos manualmente, el rol o el usuario utilizado para autenticarse Cuenta de AWS debe tener los `iam:PassRole` permisos para el rol de IAM. `ams-ssm-automation-role` Para obtener más información, consulte Otorgar permisos a un usuario para transferir un rol a un arquitecto de nube Servicio de AWS o ponerse en contacto con él.
   d. Elija Ejecutar.
   e. Supervisa el progreso de la ejecución del documento SSM en la columna Últimos estados y resultados.
   f. Cuando se complete el documento, seleccione Establecer estado, resuelto para resolver manualmente el OpsItem. Si el documento ha fallado, revise los detalles y vuelva a ejecutar el SSMdocument. Para obtener asistencia adicional para la solución de problemas, cree una solicitud de servicio.

Para resolver un problema OpsItem sin remediarlo, selecciona Establecer el estado como Resuelto.

7. Repita los pasos 3 y 4 para todas las demás correcciones OpsItems manuales.

## Solucione los problemas de las correcciones en Trusted Remediator

Para obtener ayuda con las correcciones manuales y los errores de corrección, póngase en contacto con AMS.

Para ver el estado y los resultados de la reparación, complete los siguientes pasos:

1. Abra la AWS Systems Manager consola en. https://console.aws.amazon.com/systems-manager/
2. Elija Administración de operaciones, OpsCenter.
3. (Opcional) Filtre la lista por Source=Trusted Remediator para incluir solo Trusted Remediator OpsItems en la lista.
4. Elija lo OpsItem que desee revisar.
5. En la sección Ejecuciones automatizadas, revise el nombre y el estado del documento y los resultados.
6. Revise los siguientes errores comunes de automatización. Si sus problemas no aparecen aquí, póngase en contacto con su CSDM para obtener ayuda.

### Errores de corrección comunes

#### No aparece ninguna ejecución en Automation Executions

Si no hay ninguna ejecución asociada a ella, OpsItem podría indicar que la ejecución no se pudo iniciar debido a valores de parámetros incorrectos.

#### Pasos para la solución de problemas

1. En los datos operativos, revise el valor de la `trustedAdvisorCheckAutoRemediation` propiedad.
2. Compruebe que los valores DocumentNamey los parámetros sean correctos. Para obtener los valores correctos, consulte Configurar la corrección de Trusted Advisor comprobaciones en Trusted Remediator los detalles sobre cómo configurar los parámetros del SSM. Para revisar los

parámetros de comprobación admitidos, consulte Trusted Advisor comprobaciones compatibles con Trusted Remediator

3. Compruebe que los valores del documento SSM coincidan con los patrones permitidos. Para ver los detalles de los parámetros del contenido del documento, seleccione el nombre del documento en la sección Runbooks.
4. Tras revisar y corregir los parámetros, vuelva a ejecutar manualmente el documento SSM.
5. Para evitar que se repita este error, asegúrese de configurar la corrección con los valores de parámetros correctos en su configuración. Para obtener más información, consulte Configurar la corrección de Trusted Advisor comprobaciones en Trusted Remediator

Ejecuciones fallidas en Automation Executions

Los documentos de remediación contienen varios pasos que interactúan con la Servicios de AWS realización de diversas acciones. APIs Para identificar la causa específica del error, complete los siguientes pasos:

Pasos para la solución de problemas

1. Para ver los pasos de ejecución individuales, selecciona el enlace del identificador de ejecución que se encuentra en la sección Ejecuciones automatizadas. A continuación, se muestra un ejemplo de la consola de Systems Manager que muestra los pasos de ejecución de una automatización seleccionada:



2. Elija el paso con el estado Fallido. Los siguientes son ejemplos de mensajes de error:

   - `NoSuchBucket - An error occurred (NoSuchBucket) when calling the GetPublicAccessBlock operation: The specified bucket does not exist`

     Este error indica que se especificó un nombre de depósito incorrecto en los parámetros preconfigurados de la configuración de corrección.

     Para resolver este error, ejecute la automatización manualmente con el nombre de bucket correcto. Para evitar que este problema vuelva a producirse, actualice la configuración de corrección con el nombre de bucket correcto.

   - `DB instance my-db-instance-1 is not in available status for modification.`

Este error indica que la automatización no pudo realizar los cambios esperados porque la instancia de base de datos estaba en un estado no válido.

Para resolver este error, ejecute la automatización manualmente.

## Registros de remediación en Trusted Remediator

Trusted Remediator crea registros en formato JSON y los carga en Amazon Simple Storage Service. Los archivos de registro se cargan en un bucket de S3 creado por AMS y denominado. `ams-trusted-remediator-{your-account-id}-logs` AMS crea el bucket de S3 en la cuenta de administrador delegado. Puede importar los archivos de registro a Quick para generar informes de corrección personalizados.

Para obtener más información, consulte Integración de Trusted Remediator con Quick.

### Registro de elementos de remediación

Trusted Remediator crea el `Remediation item log` cuando se crea una remediación OpsItem . Este registro contiene la remediación manual OpsItem y la remediación automática. OpsItem Puede utilizarlo `Remediation item log` para realizar un seguimiento de la visión general de todas las correcciones.

Ubicación del registro de elementos de corrección para las recomendaciones de Compute Optimizer

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs/compute_optimizer_remediation_items/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Compute Optimizer check ID`*`-`*`Resource ID`*`.json`

Ubicación del registro de elementos de corrección para las comprobaciones Trusted Advisor

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs/remediation_items/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Trusted Advisor check ID`*`- `*`Resource ID`*`.json`

Ubicación del registro de elementos de corrección para las recomendaciones de Security Hub (CSPM)

`s3://ams-trusted-remediator-`*`delegated-administrator-account`*`-id-logs/security_hub_remediation_items/`*`remediation creation time in yyyy-mm-dd`*

*format*/*10 digits epoch time or unix timestamp-Security Hub CSPM check ID-Resource ID*.json

URL del archivo de ejemplo del registro de elementos de remediación

s3:///ams-trusted-remediator-*111122223333*-logs/remediation_items/*2023-02-06*/*1675660464-DAvU99Dc4C-vol-00bd8965660b4c16d.json*

Formato de registro de elementos de Compute Optimizer Remediation

```
{
  "AccountID": "Account_ID",
  "ComputeOptimizerCheckID": "Compute Optimizer check ID",
  "ComputeOptimizerCheckName": "Compute Optimizer check name",
  "ResourceID": "Resource ID",
  "RemediationTime": Remediation creation time,
  "ExecutionMode": "Automated or Manual",
  "OpsItemID": "OpsItem ID"
}
```

Trusted Advisor Formato de registro de elementos de corrección

```
{
   "TrustedAdvisorCheckID": Trusted Advisor check ID,
   "TrustedAdvisorCheckName": Trusted Advisor check name,
   "TrustedAdvisorCheckResultTime": 10 digits epoch time or unix timestamp,
   "ResourceID": Resource ID,
   "RemediationTime": Remediation creation time,
   "ExecutionMode": Automated or Manual,
   "OpsItemID": OpsItem ID
}
```

Formato de registro de elementos de remediación CSPM de Security Hub

```
{
 "AccountID": "Account_ID",
 "SecurityHubCheckID": "Security Hub check ID",
 "SecurityHubCheckName": "Security Hub check name",
 "ResourceID": "Resource ID",
 "RemediationTime": Remediation creation time,
```

```
 "ExecutionMode": "Automated or Manual",
 "OpsItemID": "OpsItem ID"
}
```

Contenido de muestra en formato de registro de elementos de Compute Optimizer Remediation

```
{
  "AccountID": "123456789012",
  "ComputeOptimizerCheckID": "compute-optimizer-ebs",
  "ComputeOptimizerCheckName": "EBS volumes",
  "ResourceID": "vol-1235589366f77aca7",
  "RemediationTime": 1755044783,
  "ExecutionMode": "Manual",
  "OpsItemID": "oi-b8888b38fe78"
}
```

Trusted Advisor Contenido de muestra en formato de registro de elementos de remediación

```
{
    "TrustedAdvisorCheckID": "DAvU99Dc4C",
    "TrustedAdvisorCheckName": "Underutilized Amazon EBS Volumes",
    "TrustedAdvisorCheckResultTime": 1675614749,
    "ResourceID": "vol-00bd8965660b4c16d",
    "RemediationTime": 1675660464,
    "OpsItemID": "oi-cca5df7af718"
}
```

Contenido de muestra en formato de registro de elementos de remediación CSPM de Security Hub

```
{
    "AccountID": "012345678901",
    "SecurityHubControlID": "security-hub-lambda-7",
    "SecurityHubControlName": "Lambda functions should have AWS X-Ray active tracing
 enabled",
    "SecurityHubControlResultTime": 1764580147,
    "ResourceID": "test-lambda-7-xray-disabled",
    "RemediationTime": 1764900171,
    "ExecutionMode": "Manual",
    "OpsItemID": "oi-ea12c3456d7f"
}
```

## Registro automatizado de ejecución de correcciones, Compute Optimizer, Security Hub CSPM y Trusted Advisor

Trusted Remediator lo crea `Automated remediation execution log` cuando se completa la ejecución automática de un documento SSM. Este registro contiene detalles de ejecución de SSM únicamente para la corrección automática. OpsItem Puede utilizar este archivo de registro para realizar un seguimiento de las correcciones automatizadas.

Ubicación del registro de correcciones automatizadas de Compute Optimizer

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs//remediation_executions/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Compute Optimizer recommendation ID`*`.json`

Ubicación del registro de correcciones automatizadas de Security Hub CSPM

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs//remediation_executions/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Security Hub CSPM recommendation ID`*`.json`

Trusted Advisor Ubicación del registro de correcciones automatizado

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs//remediation_executions/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Trusted Advisor check ID`*`-`*`Resource ID`*`.json`

Ejemplo de ubicación del registro de correcciones automatizadas de Compute Optimizer

`s3://ams-trusted-remediator-`*`111122223333`*`-logs/remediation_executions/2025-06-26/1750908858-123456789012-compute-optimizer-ec2-i-1235173471d2cd789.json`

Ejemplo de ubicación del registro de correcciones automatizadas de Security Hub (CSPM)

`s3://ams-trusted-remediator-`*`111122223333`*`-logs/remediation_executions/2025-06-26/763247655-066028476520-security-hub-rds-8-miz-tr-sh-test-rds-instance-1.json`

Trusted Advisor Ejemplo de ubicación del registro de correcciones automatizadas

`s3://ams-trusted-remediator-111122223333-logs/remediation_executions/2023-02-06/1675660573-DAvU99Dc4C-vol-00bd8965660b4c16d.json`

Contenido de muestra en formato de registro de correcciones automatizado

```
{
    "OpsItemID": "oi-767c77e05301",
    "SSMExecutionID": "93d091b2-778a-4cbc-b672-006954d76b86",
    "SSMExecutionStatus": "Success"
}
```

## Registro de cuentas de miembros

Trusted Remediator las crea `Member accounts log` cuando su cuenta está incorporada o desactivada. Puede utilizarla `Member accounts log` para encontrar el ID de cuenta, la incorporación y el tiempo de ejecución de cada cuenta de Regiones de AWS miembro.

Ubicación del registro de las cuentas de los miembros

`s3://ams-trusted-remediator-delegated-administrator-account-id-logs/configuration_logs/member_accounts.json`

URL del archivo de ejemplo de registro de las cuentas de los miembros

`s3://ams-trusted-remediator-111122223333-logs/configuration_logs/member_accounts.json`

Formato de registro de cuentas de miembros

```
{
    "delegated_administrator_account_id": Delegated Administrator account id,
    "appconfig_configuration_region": Trusted Remediator AppConfig Region,
    "member_accounts": [
        {
            "account_id": Member account id
            "account_partition": Member account partition (for example, aws),
            "regions": [
                {
```

```
                    "execution_time": Remediation execution time in cron schedule
 expression,
                    "execution_timezone": Timezone for the remediation execution time,
                    "region_name": Región de AWS name
                }
                ...
            ]
        }
        ...
    ],
    "updated_at": Log update time,
}
```

Contenido de muestra en formato de registro de cuentas de miembros

```
{
    "delegated_administrator_account_id": "111122223333",
    "appconfig_configuration_region": "ap-southeast-2",
    "member_accounts": [
        {
            "account_id": "222233334444",
            "account_partition": "aws",
            "regions": [
                {
                    "execution_time": "0 9 * * 6",
                    "execution_timezone": "Australia/Sydney",
                    "region_name": "ap-southeast-2"
                },
                {
                    "execution_time": "0 5 * * 7",
                    "execution_timezone": "UTC",
                    "region_name": "us-east-1"
                }
            ]
        },
        {
            "account_id": "333344445555",
            "account_partition": "aws",
            "regions": [
                {
                    "execution_time": "0 1 * * 5",
                    "execution_timezone": "Asia/Seoul",
                    "region_name": "ap-northeast-2"
```

```
                }
            ]
        }
    ],
    "updated_at": "1730869607"
}
```

## Integración de Trusted Remediator con Quick

Puede integrar los registros de Trusted Remediator almacenados en Amazon S3 con Quick para crear un informe de remediación personalizado. La integración rápida es opcional. Esta función le permite usar los registros para crear paneles de informes personalizados. Para obtener informes a pedido para Trusted Remediator, póngase en contacto con su CSDM. Para obtener más información sobre los informes de Trusted Remediator disponibles, consulte. Informes de Trusted Remediator

Para obtener más información sobre la visualización de datos en Quick, consulte Visualización de datos en Quick.

### Agregue un conjunto de datos a Quick para el registro de elementos de remediación

Para añadir un conjunto de datos al registro de elementos de Quick for the Remediation, siga estos pasos:

1. Inicie sesión en la consola rápida. Puede crear el informe rápido en cualquier Región de AWS dispositivo compatible con Quick. Sin embargo, para mejorar el rendimiento y reducir los costes, se recomienda crear el informe en la región en la que se encuentra el depósito de registro de Trusted Remediator.
2. Elija Conjuntos de datos.
3. Elija S3.
4. En la nueva fuente de datos de S3, introduzca los siguientes valores:

   - Nombre de la fuente de datos: `trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-items`.
   - Cargar un archivo de manifiesto: Crea un archivo JSON con el siguiente contenido y úsalo. Al crear el archivo, sustituya `logging_bucket_name` la URIPrefixes clave.

     ```
     {
     ```

```
    "fileLocations": [
        {
            "URIPrefixes": [
                "s3://{logging_bucket_name}/remediation_items/"
            ]
        }
    ],
    "globalUploadSettings": {
        "format": "JSON",
        "delimiter": ",",
        "textqualifier": "'",
        "containsHeader": "true"
    }
}
```

- Elija Conectar.
- En la ventana Finalizar la creación del conjunto de datos, elija Visualizar.
- Quick abre la nueva página de la hoja de análisis. Ahora está listo para crear un nuevo análisis utilizando el registro de elementos de remediación.

El siguiente es un ejemplo de análisis:

## Agregue un conjunto de datos a Quick para el registro de ejecución de correcciones automatizadas

1. Inicie sesión en la consola Quick. Puede crear el informe rápido en cualquier Región de AWS dispositivo compatible con Quick. Sin embargo, para mejorar el rendimiento y reducir los costes, se recomienda crear el informe en la región en la que se encuentra el depósito de registro de Trusted Remediator.
2. Elija Conjuntos de datos.
3. Elija S3.
4. En la nueva fuente de datos de S3, introduzca los siguientes valores:
   - Nombre de la fuente de datos:`trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-executions`.

- Cargar un archivo de manifiesto: cree un archivo JSON con el siguiente contenido y, a continuación, utilice este archivo. Al crear el archivo, sustituya `logging_bucket_name` la URIPrefixes clave.

```
{
    "fileLocations": [
        {
            "URIPrefixes": [
                "s3://{logging_bucket_name}/remediation_executions/"
            ]
        }
    ],
    "globalUploadSettings": {
        "format": "JSON",
        "delimiter": ",",
        "textqualifier": "'",
        "containsHeader": "true"
    }
}
```

- Elija Conectar.
- En la ventana Finalizar la creación del conjunto de datos, elija Visualizar.
- Quick abre la nueva página de la hoja de análisis. Ahora está listo para crear un nuevo análisis utilizando el registro de elementos de remediación.

El siguiente es un ejemplo de análisis:

## Mejores prácticas en Trusted Remediator

Las siguientes son las mejores prácticas para ayudarle a utilizar Trusted Remediator:

- Si no está seguro de los resultados de la reparación, comience con el modo de ejecución manual. A veces, aplicar la ejecución automática para las correcciones desde el principio puede provocar resultados inesperados.
- Realice una revisión semanal de las correcciones OpsItems para obtener información sobre los resultados de Trusted Remediator.
- Las cuentas de los miembros heredan las configuraciones de la cuenta de administrador delegado. Por lo tanto, es importante estructurar las cuentas de manera que te ayuden a administrar

varias cuentas con las mismas configuraciones. Puede eximir los recursos de la configuración predeterminada mediante etiquetas.

## Remediador confiable FAQs

Las siguientes son preguntas frecuentes sobre Trusted Remediator:

¿Qué es Trusted Remediator y en qué me beneficia?

Cuando Compute Optimizer Trusted Advisor o Security Hub CSPM identifican un incumplimiento o emiten una recomendación, Trusted Remediator responde de acuerdo con sus preferencias especificadas, ya sea aplicando medidas correctivas, solicitando la aprobación mediante correcciones manuales o informando de las correcciones en su próxima revisión empresarial mensual (MBR). La subsanación se lleva a cabo en el momento o el cronograma de remediación que prefieras. Trusted Remediator le ofrece la posibilidad de autogestionar las Trusted Advisor comprobaciones y actuar en función de ellas, con la flexibilidad de configurar y corregir las comprobaciones de forma individual o masiva. Con una biblioteca de documentos de remediación comprobados, AMS aumenta constantemente sus cuentas aplicando controles de seguridad y siguiendo las mejores prácticas. AWS Solo recibirá una notificación si así lo especifica en su configuración. Los usuarios de AMS pueden suscribirse a Trusted Remediator sin coste adicional.

¿Cómo se relaciona Trusted Remediator con otros y trabaja con ellos? Servicios de AWS

Tienes acceso a las Trusted Advisor comprobaciones, a las recomendaciones de Compute Optimizer y a los controles CSPM de Security Hub como parte de tu plan Enterprise Support actual. Trusted Remediator se integra con Trusted Advisor Compute Optimizer y Security Hub CSPM para aprovechar las capacidades de automatización de AMS existentes. En concreto, AMS utiliza documentos de AWS Systems Manager automatización (manuales de ejecución) para las correcciones automatizadas. AWS AppConfig se utiliza para configurar los flujos de trabajo de corrección. Puede ver todas las correcciones actuales y pasadas a través del Systems Manager OpsCenter. Los registros de corrección se almacenan en un bucket de Amazon S3. Puede usar los registros para importar y crear paneles de informes personalizados en Quick.

¿Quién configura las correcciones?

Eres el propietario de las configuraciones de tu cuenta. Administrar las configuraciones es su responsabilidad. Puede ponerse en contacto con su CA o CDSM para que le ayude a gestionar sus configuraciones. También puede ponerse en contacto con AMS mediante una solicitud de servicio

para obtener asistencia en materia de configuración, correcciones manuales y solución de problemas relacionados con las correcciones.

¿Cómo instalo los documentos de automatización de SSM?

Los documentos de automatización de SSM se comparten automáticamente con las cuentas AMS integradas.

¿También se remediarán los recursos propiedad de AMS?

Trusted Remediator no marca los recursos propiedad de AMS. Trusted Remediator se centra únicamente en sus recursos.

¿En qué Regiones de AWS está disponible Trusted Remediator y quién puede usarlo?

Trusted Remediator está disponible para los clientes de AMS Accelerate. Para ver una lista actualizada de las regiones de soporte, consulte Servicios de AWS por región.

¿Trusted Remediator provocará la pérdida de recursos?

Dado que los documentos de automatización de SSM actualizan directamente los recursos a través de la AWS API, es posible que se produzcan desviaciones de recursos. Puedes usar etiquetas para segregar los recursos creados a través de tus paquetes existentes CI/CD . Puede configurar Trusted Remediator para que ignore los recursos etiquetados y, al mismo tiempo, corrija los demás recursos.

¿Cómo puedo pausar o detener Trusted Remediator?

Puede desactivar Trusted Remediator a través de la AWS AppConfig aplicación. Para pausar o detener Trusted Remediator, siga estos pasos:

1. Abra la AWS AppConfig consola en https://console.aws.amazon.com/systems-manager/appconfig.
2. Seleccione Trusted Remediator.
3. Seleccione Parámetros en el perfil de configuración.
4. Seleccione el indicador Suspender Trusted Remediator.
5. Defina el valor del atributo en `suspended`. `true`

> **Note**
>
> Tenga cuidado al utilizar este procedimiento, ya que detendrá Trusted Remediator en todas las cuentas vinculadas a la cuenta de administrador delegado.

¿Cómo puedo corregir las comprobaciones que no son compatibles con Trusted Remediator?

Puede seguir comunicándose con AMS a través de Operations On Demand (OOD) en caso de comprobaciones no admitidas. AMS le ayuda a corregir estas comprobaciones. Para obtener más información, consulte Operations On Demand.

¿En qué se diferencia Trusted Remediator de la AWS Config remediación?

AWS Config La remediación es otra solución que le ayuda a optimizar los recursos de la nube y a mantener el cumplimiento de las mejores prácticas. Las siguientes son algunas de las diferencias operativas entre las dos soluciones:

- Trusted Remediator utiliza Trusted Advisor Compute Optimizer y Security Hub CSPM como mecanismos de detección. AWS Config La remediación utiliza AWS Config reglas como mecanismo de detección.
- En el caso de Trusted Remediator, la remediación se realiza según el programa de remediación predefinido. En AWS Config, la remediación se produce en tiempo real.
- Los parámetros de cada remediación de Trusted Remediator se pueden personalizar fácilmente en función de su caso de uso, y la remediación puede automatizarse o hacerse de forma manual añadiendo etiquetas a los recursos.
- Trusted Remediator proporciona la funcionalidad de generación de informes.
- Trusted Remediator le envía una notificación por correo electrónico con la lista de las correcciones y el estado de las mismas.

Es posible que algunas Trusted Advisor comprobaciones, así como las recomendaciones de Compute Optimizer y Security Hub (CSPM), incluyan la misma regla. AWS Config Se recomienda habilitar solo una corrección si hay una regla y una comprobación coincidentes AWS Config . Trusted Advisor Para obtener información sobre AWS Config las reglas de cada Trusted Advisor comprobación, consulteTrusted Advisor comprobaciones compatibles con Trusted Remediator.

¿Qué recursos utiliza Trusted Remediator en sus cuentas?

Trusted Remediator implementa los siguientes recursos en la cuenta de administrador delegado de Trusted Remediator:

- Un bucket de Amazon S3 denominado `ams-trusted-remediator-{your-account-id}-logs`. Trusted Remediator crea la solución `Remediation item log` en formato JSON cuando se crea una solución y OpsItem carga los archivos de registro en este depósito.
- Una AWS AppConfig aplicación para almacenar las configuraciones de corrección para las Trusted Advisor comprobaciones compatibles, las recomendaciones de Compute Optimizer y Security Hub CSPM.

Trusted Remediator no despliega recursos en la cuenta de miembro de Trusted Remediator.

# Supervisión y gestión de incidentes para Amazon EKS en AMS Accelerate

Monitoring and Incident Management for Amazon EKS supervisa los recursos de Amazon EKS para detectar errores, degradación del rendimiento y problemas de seguridad. AMS Accelerate configura e implementa las reglas del administrador de alertas de Amazon Managed Service para Prometheus, supervisa las alertas y, a continuación, gestiona los incidentes cuando se activan estas alertas. La supervisión y la gestión de incidentes de Amazon EKS se basan en AMS Alarm Manager y utilizan AWS servicios nativos, como Amazon Managed Service for Prometheus, Amazon Managed Grafana, Amazon y. GuardDuty AWS LambdaAWS Config

> **Important**
>
> La supervisión y la administración de incidentes de Amazon EKS no son compatibles con la región de Asia Pacífico (Malasia) AWS GovCloud (US), los nodos de Windows ni los contenedores de Windows.

## ¿Qué es la supervisión y la gestión de incidentes para Amazon EKS en AMS Accelerate?

La supervisión y la administración de incidentes de Amazon EKS proporcionan lo siguiente:

- Una configuración predeterminada que crea, administra e implementa monitores y políticas en su cuenta gestionada para los clústeres de Amazon EKS que seleccione.
- Una línea base de monitoreo para permitir que sus cargas de trabajo de Amazon EKS tengan una mayor disponibilidad, incluso si no configura ningún otro monitoreo para sus clústeres de Amazon EKS. Para obtener más información, consulte Alertas de referencia en la supervisión y la gestión de incidentes para Amazon EKS en AMS Accelerate.
- Notificaciones generadas por la supervisión de referencia configurada para su clúster de Amazon EKS. Estas notificaciones se conocen como alertas. Las alertas se generan cuando hay fallos inminentes, continuos, inminentes o potenciales, una degradación del rendimiento o problemas de seguridad. Algunos ejemplos de alertas incluyen una alerta de Prometheus, un evento o un hallazgo de AWS un servicio, como Amazon. GuardDuty

- Realiza una investigación de alertas con orientación sobre las medidas correctivas adecuadas que puedes tomar. Para obtener más información, consulte los informes de incidentes y las solicitudes de servicio en AMS Accelerate.
- Las operaciones de AMS corrigen las alertas e incidentes, siempre que sea posible y con su aprobación, para evitar o reducir el impacto en sus aplicaciones. Para obtener más información, consulte los informes de incidentes y las solicitudes de servicio en AMS Accelerate.
- Paneles opcionales de Amazon Managed Grafana predefinidos que proporcionan visibilidad de la utilización de los recursos, el rendimiento, el estado de CoredNS, las alertas activas y las alertas previamente resueltas. Si configura Amazon Managed Grafana con la plantilla proporcionada por AMS, puede abrir la consola de Amazon Managed Grafana para ver las métricas y alertas de su clúster de Amazon EKS.

# Cómo funcionan la supervisión y la gestión de incidentes para Amazon EKS en AMS Accelerate

Generación: Como parte de la supervisión de incorporación y la gestión de incidentes para EKS, AMS configura la supervisión de referencia para los clústeres de Amazon EKS que ha seleccionado en su cuenta gestionada. AMS utiliza una combinación de las reglas del administrador de alertas de Amazon Managed Service for Prometheus y las reglas de eventos de CloudWatch Amazon para configurar la supervisión de referencia. Un servidor Prometheus configurado por AMS en su clúster recopila y escribe de forma remota sus métricas de Prometheus en un servicio gestionado de Amazon para un punto final de Prometheus de la misma región. La configuración de supervisión básica genera una alerta cuando se activa una regla del administrador de alertas de Prometheus o se genera CloudWatch un evento.

Agregación: AMS envía todas las alertas que generan sus recursos al sistema de supervisión de AMS dirigiéndolas a un tema de Amazon Simple Notification Service gestionado por AMS.

Procesamiento y análisis de impacto: AMS analiza las alertas y, a continuación, las procesa en función de su posible impacto. AMS clasifica las alertas de la siguiente manera:

- Alertas con un impacto conocido en los clientes: para estas alertas, AMS crea un nuevo informe de incidentes mediante el proceso de gestión de incidentes.
- Alertas con un impacto incierto en los clientes: para estas alertas, AMS envía un informe de incidente. En muchos casos, estas alertas le piden que verifique el impacto antes de que AMS pueda tomar medidas. En el caso de dichas alertas, AMS envía una notificación de alerta con los

detalles y comprueba si la alerta necesita una acción atenuante. AMS proporciona opciones para mitigar las acciones en la notificación. Si su respuesta confirma que la alerta es un incidente, AMS activa entonces la creación de un nuevo informe de incidente e inicia el proceso de gestión de incidentes. Cualquier notificación de servicio que reciba una respuesta que indique que «no ha afectado al cliente» o que no haya recibido respuesta alguna durante tres días se marcará como resuelta. Además, la alerta correspondiente se marca como resuelta.

- Alertas que no afectan a los clientes: si, tras una evaluación, AMS determina que la alerta no afecta a los clientes, se cierra.

## Matriz de responsabilidad de AMS (RACI)

La matriz responsable, responsable, consultada e informada de AMS, o RACI, asigna la responsabilidad principal al cliente o a AMS en lo que respecta a una variedad de actividades. La siguiente tabla proporciona un resumen de las responsabilidades del cliente y de AMS en relación con las actividades de una aplicación que utiliza la supervisión y la gestión de incidentes para Amazon EKS.

- R significa la parte responsable que hace el trabajo para lograr la tarea.
- A representa a la parte responsable.
- C significa consultado; la parte cuya opinión se solicita, por lo general como expertos en la materia; y con la que existe comunicación bilateral.
- I significa informado; la parte que recibe información sobre el progreso, a menudo solo una vez finalizada la tarea o el producto final.

| Actividad | Cliente | AMS |
|---|---|---|
| Descubrimiento de los requisitos de AMS | I | R |
| Habilite los permisos AMS (RBAC) para el acceso al clúster | R | C |
| Instale el agente de Amazon EC2 Systems Manager en los | R | C |

| Actividad | Cliente | AMS |
| --- | --- | --- |
| nodos de trabajo si aún no está presente | | |
| Implemente componentes de AMS en el clúster, como Prometheus, Prometheu s Node Exporter y en un espacio de nombres de AMS, según sea necesario kube-stat e-metrics. | C | R |
| Aprovisione Amazon Managed Service para Prometheus en el plano de control de AMS | I | R |
| Configurar el administrador de alertas de Prometheus en el plano de control AMS | I | R |
| Proporcione la plantilla de Grafana gestionada por Amazon y ayude con la configuración | C | R |
| Habilite la supervisión del registro de auditoría de GuardDuty EKS | C | R |
| Habilitar el registro del plano de control de Amazon EKS | I | R |
| Supervise el estado y el rendimiento del plano de control Amazon EKS | I | R |

| Actividad | Cliente | AMS |
| --- | --- | --- |
| Supervise el estado y el rendimiento de su clúster de Amazon EKS (clúster, nodo, carga de trabajo, pod, servidor de API y CoredNS) | I | R |
| Clasifique las alertas y proporcione respuesta a incidentes para Amazon EKS | I | R |
| Ejecute comandos de diagnóstico durante los incidentes | I | R |
| Analice los registros durante los incidentes (registros del plano de control y del módulo) | I | R |
| Respuesta a incidentes relacionados con problemas AWS de red | I | R |
| Responda a los hallazgos de GuardDuty EKS Audit Log Monitoring | I | R |
| Siempre que sea posible, proporcione orientación al cliente sobre las medidas que deben adoptarse para subsanar los incidentes | I | R |

# Alertas de referencia en la supervisión y la gestión de incidentes para Amazon EKS en AMS Accelerate

Tras verificar las alertas, AMS habilita las siguientes alertas para Amazon EKS y, a continuación, se encarga de la supervisión y la gestión de incidentes de los clústeres de Amazon EKS seleccionados. El tiempo de respuesta, los acuerdos de nivel de servicio (SLAs) y los objetivos de nivel de servicio (SLOs) dependen del nivel de servicio (Plus, Premium) de la cuenta que haya seleccionado. Para obtener más información, consulte los informes de incidentes y las solicitudes de servicio en AMS Accelerate.

## Alertas y acciones

En la siguiente tabla se enumeran las alertas de Amazon EKS y las acciones respectivas que lleva a cabo AMS:

| Alerta | Umbrales | Acción |
|---|---|---|
| Container OOM ha muerto | El número total de contenedores reiniciados en los últimos 10 minutos es de al menos 1 y un contenedor de Kubernetes de un pod se ha cerrado por el motivo «OOMKilled» en los últimos 10 minutos. | AMS investiga si la causa del cierre de OOM se debe a que se ha alcanzado el límite de contenedores o a que se ha sobrepasado el límite de memoria y, a continuación, te aconseja qué medidas correctivas tomar. |
| Error en Pod Job | No se puede completar un trabajo de Kubernetes. El error se indica mediante la presencia de al menos un estado de trabajo fallido. | AMS investiga los motivos por los que el trabajo de Kubernetes o el trabajo cron correspondiente está fallando y, a continuación, le asesora sobre las medidas correctivas. |
| StatefulSet Abajo | La cantidad de réplicas listas para atender el tráfico no coincide con la cantidad actual de réplicas existentes | AMS determina por qué los pods no están preparados revisando los mensajes de error de los eventos de los |

| Alerta | Umbrales | Acción |
| --- | --- | --- |
| | StatefulSet durante al menos 1 minuto. | pods y los fragmentos del registro de errores de los registros de los pods y, a continuación, le recomienda las medidas correctivas. |
| Capacidad de escalado de HPA | El escalador automático de cápsulas horizontales (HPA) no puede escalar debido a que la condición de estado «AbleToScale» es falsa durante al menos 2 minutos. | AMS determina qué escalador automático de pods horizonta les (HPA) de Kubernetes no puede escalar los pods para su recurso de carga de trabajo posterior, como una implementación o. StatefulSet |
| Disponibilidad métrica de HPA | El escalador automático de cápsulas horizontales (HPA) no puede recopilar métricas debido a que la condición de estado «ScalingActive» es falsa durante al menos 2 minutos. | AMS determina por qué HPA no puede recopilar métricas, como las relacionadas con problemas de configuración del servidor o problemas de autorización del RBAC. |
| El pod no está listo | Un pod de Kubernetes permanece en estado inactivo (como pendiente, desconocido o fallido) durante más de 15 minutos. | AMS investiga los módulos afectados para obtener más información, revisa los registros de los módulos para detectar errores y eventos relacionados y, a continuac ión, le aconseja sobre las medidas correctivas. |

| Alerta | Umbrales | Acción |
| --- | --- | --- |
| Pod Crash Looping | Un contenedor de cápsulas se reinicia al menos una vez cada 15 minutos durante un período de 1 hora. | AMS investiga los motivos por los que el pod no se inicia, como recursos insuficientes, un archivo bloqueado por otro contenedor, una base de datos bloqueada por otro contenedor, fallos en las dependencias de los servicios , problemas de DNS en los servicios externos y errores de configuración. |
| Daemonset está mal programado | Hay al menos un pod de Daemonset de Kubernetes mal programado durante un período de 10 minutos. | AMS determina por qué un Daemonset está programad o en un nodo en el que no debería ejecutarse. Esto puede ocurrir si se ha aplicado un pod incorrecto a nodeSelec tor/taints/affinities los pods de Daemonset o cuando los nodos (grupos de nodos) están contaminados y no se ha programado el desalojo de los pods existentes. |

| Alerta | Umbrales | Acción |
| --- | --- | --- |
| Errores de la API de Kubernetes | La tasa de errores del servidor de la API de Kubernetes supera el 3% en un período de 2 minutos. | AMS analiza los registros del plano de control para determinar el volumen y los tipos de errores que están causando esta alerta e identifica cualquier problema de contención de recursos en el nodo maestro o en los grupos de escalado automátic o, etc.d. Si el servidor de API no se recupera, AMS contacta con el equipo de servicio de Amazon EKS. |
| Latencia de la API de Kubernetes | La latencia del percentil 99 de las solicitudes al servidor de la API de Kubernetes supera 1 segundo en un período de 2 minutos. | AMS analiza los registros del plano de control para determinar el volumen y los tipos de errores que causan la latencia e identifica cualquier problema de contención de recursos para el nodo maestro o los grupos de autoescalado, etcd. Si el servidor de API no se recupera, AMS contacta con el equipo de servicio de Amazon EKS. |
| El certificado de cliente de Kubernetes está caducando | El certificado de cliente utilizado para autenticarse en el servidor API de Kubernetes vence en menos de 24 horas. | AMS envía esta notificación para informarle de que su certificado de clúster caducará en 24 horas. |

| Alerta | Umbrales | Acción |
| --- | --- | --- |
| El nodo no está listo | El estado de condición del nodo «Listo» es falso durante al menos 10 minutos. | AMS investiga las condiciones y los eventos del nodo, como los problemas de red, que impiden el acceso de Kubelet al servidor API. |
| CPU con un nivel alto de nodos | La carga de la CPU supera el 80% en un período de 5 minutos. | El AMS determina si uno o más módulos consumen una cantidad de CPU inusualmente alta. A continuación, AMS comprueba contigo que tus solicitudes, límites y actividad de los pods son los esperados. |
| Se ha detectado una interrupción del OOM del nodo | El nodo ha informado de al menos una interrupción de la función OOM de un host en un período de 4 minutos. | AMS determina si la interrupción de la OOM se debe a que se ha alcanzado el límite de contenedores o a que los nodos se han sobrecomprometido. Si la actividad de la aplicación es normal, AMS le asesora sobre las solicitudes y los límites de sobreasignación y sobre la revisión de los límites de los módulos. |

| Alerta | Umbrales | Acción |
| --- | --- | --- |
| Límite de seguimiento de nodos | La relación entre el número actual de entradas de seguimiento de conexione s y el límite máximo supera el 80% en un período de 5 minutos. | AMS le asesora sobre el valor de seguimiento de conexiones recomendado por núcleo. Los nodos de Kubernetes establecen el valor máximo de conntrack de forma proporcional a la capacidad total de memoria del nodo. Las aplicaciones de alta carga, especialmente en los nodos más pequeños, pueden superar fácilmente el valor máximo de conntrack, lo que provoca que la conexión se restablezca y se agoten los tiempos de espera. |
| El reloj del nodo no está sincronizado | El estado de sincronización mínimo durante un período de 2 minutos es 0 y el error máximo en segundos es 16 o superior. | El AMS determina si el Protocolo de tiempo de red (NTP) está instalado y funciona correctamente. |
| CPU Pod High | El uso de la CPU de un contenedor supera el 80% en una velocidad de 3 minutos durante un período mínimo de 2 minutos. | AMS investiga los registros de los módulos para determina r las tareas del módulo que consumen una gran cantidad de CPU. |
| Memoria alta del pod | El uso de memoria de un contenedor supera el 80% del límite de memoria especific ado durante un período de 2 minutos. | AMS investiga los registros de los módulos para determina r las tareas del módulo que consumen una gran cantidad de memoria. |

| Alerta | Umbrales | Acción |
| --- | --- | --- |
| CoredNS inactivo | CoredNS ha desaparecido del descubrimiento de objetivos de Prometheus durante más de 15 minutos. | Se trata de una alerta crítica que indica que se ha interrumpido la resolució n de nombres de dominio para los servicios de clúster internos o externos. AMS comprueba el estado de los pods de CoreDNS, verifica la configuración de CoreDNS, verifica los puntos de enlace de DNS que apuntan a los pods de CoreDNS, verifica los límites de CoreDNS y, con su aprobación, habilita el registro de depuración de CoreDNS. |
| Errores de CoredNS | CoredNS devuelve errores SERVFAIL para más del 3% de las solicitudes de DNS en un período de 10 minutos. | Esta alerta puede indicar un problema con una aplicación o una configuración incorrecta. AMS comprueba el estado de los pods de CoreDNS, verifica la configuración de CoreDNS, verifica los puntos de enlace de DNS que apuntan a los pods de CoreDNS, verifica los límites de CoreDNS y, con su aprobación, habilita el registro de depuración de CoreDNS. |

| Alerta | Umbrales | Acción |
| --- | --- | --- |
| Latencia de CoredNS | El percentil 99 de las duraciones de las solicitud es de DNS supera los 4 segundos durante 10 minutos. | Esta alerta indica que CoredNS podría estar sobrecargado. AMS comprueba el estado de los pods de CoreDNS, verifica la configuración de CoreDNS, verifica los puntos de enlace de DNS que apuntan a los pods de CoreDNS, verifica los límites de CoreDNS y, con su aprobación, habilita el registro de depuración de CoreDNS. |
| Latencia de reenvío de CoredNS | El percentil 99 del tiempo de respuesta de las solicitudes de reenvío de CoredNS a kube-dns supera los 4 segundos en un período de 10 minutos. | Cuando CoreDNS no es el servidor autorizado o no tiene una entrada de caché para un nombre de dominio, CoreDNS reenvía la solicitud de DNS a un servidor DNS ascendente. Esta alerta indica que CoredNS podría estar sobrecargado o que podría haber un problema con un servidor DNS ascendente. AMS comprueba el estado de los pods de CoreDNS, verifica la configuración de CoreDNS, verifica los puntos de enlace de DNS que apuntan a los pods de CoreDNS, verifica los límites de CoreDNS y, con su aprobación, habilita el registro de depuración de CoreDNS. |

| Alerta | Umbrales | Acción |
| --- | --- | --- |
| Error de reenvío de CoredNS | Más del 3% de las consultas de DNS fallan en un período de 5 minutos. | Cuando CoreDNS no es el servidor autorizado o no tiene una entrada de caché para un nombre de dominio, CoreDNS reenvía la solicitud de DNS a un servidor DNS ascendente. Esta alerta indica un posible error de configura ción o un problema con un servidor DNS ascendente. AMS comprueba el estado de los pods de CoreDNS, verifica la configuración de CoreDNS, verifica los puntos de enlace de DNS que apuntan a los pods de CoreDNS, verifica los límites de CoreDNS y, con su aprobación, habilita el registro de depuración de CoreDNS. |

# Requisitos de supervisión y gestión de incidentes para Amazon EKS en AMS Accelerate

Estos son los recursos and/or necesarios y compatibles para la supervisión y la gestión de incidentes de Amazon EKS for AMS Accelerate

- Versiones de Kubernetes compatibles: consulte las versiones de Amazon EKS Kubernetes en la Guía del usuario de Amazon EKS.
- Tipos de nodos: se admiten los nodos gestionados por Amazon EKS. No se admiten los nodos y contenedores de Windows.
- Acceso al clúster de Kubernetes: AMS requiere el rol de clúster RBAC de system:masters y el usuario del clúster.

- SSM Agent en los nodos de Amazon EC2: tanto las AMI Bottle Rocket como las Amazon EKS tienen SSM Agent preinstalado. Asegúrese de que el agente SSM esté instalado en las AMI personalizadas y en los nodos de Amazon EC2.
- Para obtener más información, consulta las cuotas de servicio de Amazon Managed Service for Prometheus y Amazon Managed Grafana.
- Regiones compatibles: AWS

| Nombre de la región | Region | Región de almacenamiento de métricas |
|---|---|---|
| Este de EE. UU. (Ohio) | us-east-2 | us-east-2 |
| Este de EE. UU. (Norte de Virginia) | us-east-1 | us-east-1 |
| Oeste de EE. UU. (Oregón) | us-west-2 | us-west-2 |
| Asia Pacífico (Tokio) | ap-northeast-1 | ap-northeast-1 |
| Asia-Pacífico (Seúl) | ap-northeast-2 | ap-northeast-2 |
| Asia-Pacífico (Singapur) | ap-southeast-1 | ap-southeast-1 |
| Asia-Pacífico (Sídney) | ap-southeast-2 | ap-southeast-2 |
| Europa (Fráncfort) | eu-central-1 | eu-central-1 |
| Europa (Irlanda) | eu-west-1 | eu-west-1 |
| Europa (Londres) | eu-west-2 | eu-west-2 |
| África (Ciudad del Cabo) | af-south-1 | eu-west-1<br>eu-west-2 |
| Asia-Pacífico (Hong Kong) | ap-east-1 | ap-northeast-1<br>ap-northeast-2 |

> **Note**
>
> Las métricas de los clústeres de Amazon EKS en af-south-1, África (Ciudad del Cabo) y ap-east-1, Asia Pacífico (Hong Kong) se exportan al servicio de monitoreo AMS en el mismo lugar, respectivamente. Región de AWS Luego, las métricas correspondientes Regiones de AWS se transportan dentro del servicio de monitoreo AMS a diferentes regiones, donde se procesan y almacenan. Consulte la tabla anterior para ver las regiones que el servicio de supervisión de AMS utiliza para almacenar las métricas.

# Integre la supervisión y la gestión de incidentes de Amazon EKS en AMS Accelerate

Realice los siguientes pasos para incorporarse a la supervisión y la gestión de incidentes de Amazon EKS.

1. Habilite las etiquetas de optimización de costos de Amazon EKS: consulte Etiquetar sus recursos para la facturación en la Guía del usuario de Amazon EKS.
2. Inicie la incorporación de la supervisión y la gestión de incidentes a EKS: póngase en contacto con su administrador de prestación de servicios en la nube (CSDM) e indique los nombres de las cuentas IDs y los clústeres para incorporarlo.
3. Valide los requisitos: su arquitecto de nube (CA) valida el cumplimiento de todos los requisitos antes de que comience la incorporación.
4. Actualice el control de acceso basado en roles (RBAC) de Kubernetes: AMS comparte los comandos para implementar estos cambios. `eksctl` Puede revisar estos cambios y luego implementarlos. Debe implementar las actualizaciones del RBAC para que AMS tenga permisos para ejecutar comandos en su nombre. Estas actualizaciones incluyen asignar la función de IAM de AMS a un usuario de Kubernetes, crear una nueva función de clúster de Kubernetes para AMS y vincular la función de clúster de AMS Kubernetes al usuario.
5. Implemente los componentes del clúster: AMS implementa los siguientes componentes en un espacio de nombres de su clúster administrado por AMS:
   - Servidor Prometheus
   - Exportador de nodos Prometheus (no aplicable para) AWS Fargate
   - kube-state-metrics

6. Realizar actualizaciones de configuración de Prometheus: AMS configura Prometheus para permitir la escritura remota de métricas.
7. (Opcional) Configurar paneles: su CA le ayuda a configurar los paneles de Amazon Managed Grafana en su cuenta.

> **Note**
>
> Una vez incorporado el clúster de Amazon EKS, AMS analiza las señales de alerta y realiza una evaluación de referencia para identificar los problemas existentes en el clúster. Una vez finalizada la evaluación de referencia, AMS comparte las conclusiones y las recomendaciones de corrección a través de Trusted Advisor y una solicitud de servicio que puede utilizar para abordar los problemas de su clúster. A partir de la evaluación, AMS crea una línea base de monitoreo de Amazon EKS específica para sus clústeres de EKS ajustando nuestros umbrales de alarma a nivel de cuenta. Para evitar la duplicación de las respuestas de AMS en función de estos resultados, ajustamos nuestra supervisión para excluir esas señales de alerta. Reajustamos nuestra supervisión para incluir las señales cuando su CSDM nos informa de que se han solucionado los problemas subyacentes.

## Olvídese de la supervisión y la gestión de incidentes para Amazon EKS en AMS Accelerate

Notifique a su administrador de prestación de servicios en la nube (CSDM) los nombres de las cuentas IDs y los clústeres para iniciar el proceso de exclusión. Una vez que te des de baja, se suspenden el procesamiento de alertas, el almacenamiento de métricas y las consultas de métricas y las métricas se eliminan de acuerdo con las políticas de retención de datos predeterminadas de Amazon Managed Service for Prometheus.

AMS lleva a cabo los siguientes pasos de desvinculación:

1. AMS desactiva las alertas que se le envían a usted y a AMS Operations.
2. AMS elimina la instancia de Prometheus del clúster de Amazon EKS.
3. AMS elimina otros AWS recursos que están instalados en su cuenta, como las funciones y las reglas de IAM. AWS Config

Una vez completados estos pasos, debe completar los siguientes pasos de desconexión:

1. Úselo `eksctl` para eliminar los permisos RBAC de Kubernetes del. `aws-auth` `ConfigMap`
2. Si la instaló anteriormente, elimine la instancia de Grafana gestionada por Amazon que configuró para conectarse a AMS.

# Gestión de la continuidad en AMS Accelerate

AMS aprovecha AWS Backup para centralizar y automatizar el respaldo de sus datos en todos AWS los servicios. Los planes de respaldo de AMS proporcionan las mejores prácticas para varios casos de uso; sin embargo, le invitamos a seguir utilizando sus planes de respaldo actuales. Una vez que te hayas incorporado a la gestión de copias de seguridad de AMS, AMS te proporcionará informes de copias de seguridad y los expertos de AMS supervisarán continuamente tus tareas de copia de seguridad para garantizar que dispongas de una solución de copia de seguridad fiable.

Para obtener más información, consulte AWS Backup: Cómo funciona y AWS recursos compatibles y aplicaciones de terceros.

AMS Accelerate ofrece una gama de servicios operativos para ayudarlo a alcanzar la excelencia operativa en AWS. Para comprender rápidamente cómo AMS ayuda a sus equipos a alcanzar la excelencia operativa general Nube de AWS con algunas de nuestras capacidades operativas clave, como el servicio de asistencia las 24 horas del día, los 7 días de la semana, la supervisión proactiva, la seguridad, la aplicación de parches, el registro y la copia de seguridad, consulte los diagramas de arquitectura de referencia de AMS.

Vea el vídeo de Carl para obtener más información (9:29)

Temas

- Cómo funciona la gestión de la continuidad en AMS
- Seleccione un plan de respaldo de AMS
- Etiquete sus recursos para aplicar los planes de respaldo de AMS
- Ver copias de seguridad en bóvedas de AMS
- Monitorización e informes de copias de seguridad de AMS

## Cómo funciona la gestión de la continuidad en AMS

Los planes de respaldo de AMS definen la frecuencia con la que se hacen copias de seguridad de sus datos y la política de retención de las copias de seguridad. Las bóvedas de respaldo de AMS mantienen sus datos de respaldo organizados. Una vez que un recurso está asociado a un plan de respaldo, los recursos compatibles se respaldan de forma incremental. La primera copia de seguridad es una copia completa y las copias de seguridad posteriores capturan los cambios

incrementales. Según el recurso y el plan de copia de seguridad de AMS seleccionados, la Point-in-time restauración (PITR) le permite recuperar los recursos seleccionando un momento para la recuperación. Para empezar a utilizar AMS Backup Management, solo tiene que seleccionar un plan de backup de AMS y etiquetar sus recursos.

> **Note**
>
> Asegúrese de que AWS Backup esté habilitado para cada cuenta y tipo de recurso siguiendo los pasos que se indican a continuación: Primeros pasos 1: suscripción al servicio. Región de AWS
> No necesita continuar con la sección Primeros pasos 2: Crear copias de seguridad bajo demanda.

Temas relacionados de AWS Backup

- Trabajar con copias de seguridad (crear, editar, copiar, restaurar, eliminar)
- Creación de una copia de seguridad bajo demanda
- Crear copias de seguridad en Regiones de AWS
- AWS Backup Servicios admitidos
- Point-in-time restaurar
- AWS Backup Características

## Seleccione un plan de respaldo de AMS

AMS ofrece tres planes de respaldo diferentes y un cuarto plan de respaldo para minimizar los costos durante la incorporación. Para seleccionar un plan de respaldo de AMS para cada recurso compatible, etiquete el recurso con la etiqueta asociada al plan. Cuando se incorpore a Accelerate, AMS trabajará con usted para identificar el plan de respaldo que mejor se adapte a sus necesidades.

> **Important**
>
> No edite los planes de respaldo predeterminados de AMS, ya que los cambios podrían perderse. En su lugar, cree nuevos planes para sus configuraciones personalizadas. Para obtener más información, consulte Crear un plan de respaldo.

## Plan de respaldo de AMS predeterminado

AWS Backup La copia de seguridad continua no está habilitada para este plan de copia de seguridad; para obtener más información, consulte Restaurar a una hora específica mediante la point-in-time restauración (PITR).

Clave de etiqueta: `ams:rt:backup-orchestrator`

Valor TAG: `true`

| Plan de respaldo de AMS predeterminado | Start Time | Retención |
|---|---|---|
| copia de seguridad por hora | N/A | N/A |
| copia de seguridad diaria | todos los días a las 4:00 UTC | 7 días |
| copia de seguridad semanal | sábado, 2:00 UTC | 4 semanas |
| copia de seguridad mensual | El 1 de cada mes, a las 2:00 UTC | 26 semanas |
| respaldo anual | 1 de enero a las 2:00 UTC | 2 años |

## Plan de respaldo mejorado

AWS Backup El respaldo continuo está habilitado con una retención máxima (31 días) en los recursos compatibles; para obtener más información, consulte Restaurar a un tiempo específico mediante la point-in-time restauración (PITR) y Servicios y aplicaciones de point-in-time restauración compatibles (PITR).

Clave de etiqueta: `ams:rt:backup-orchestrator-enhanced`

Valor TAG: `true`

| Plan de respaldo mejorado | Start Time | Retención |
|---|---|---|
| respaldo por hora | N/A | N/A |
| copia de seguridad diaria | todos los días a las 4:00 UTC | 31 días |

| Plan de respaldo mejorado | Start Time | Retención |
|---|---|---|
| copia de seguridad semanal | sábado, 2:00 UTC | 6 semanas |
| copia de seguridad mensual | El 1 de cada mes, a las 2:00 UTC | 26 semanas |
| respaldo anual | 1 de enero a las 2:00 UTC | 2 años |

## Plan de respaldo para datos sensibles

AWS Backup La copia de seguridad continua está habilitada con una retención máxima (31 días) de los recursos compatibles; para obtener más información, consulte point-in-timeRestaurar a un tiempo específico mediante la restauración (PITR) y Servicios y aplicaciones de point-in-time restauración compatibles (PITR).

Clave de etiqueta: `ams:rt:backup-orchestrator-data-sensitive`

Valor TAG: `true`

| Plan de respaldo para datos confidenciales | Start Time | Retención |
|---|---|---|
| copia de seguridad por hora | cada hora | 7 días |
| copia de seguridad diaria | todos los días a las 4:00 UTC | 31 días |
| copia de seguridad semanal | sábado, 2:00 UTC | 6 semanas |
| copia de seguridad mensual | El 1 de cada mes, a las 2:00 UTC | 26 semanas |
| respaldo anual | 1 de enero a las 2:00 UTC | 2 años |

## Plan de respaldo para la incorporación de AMS Accelerate

AWS Backup La copia de seguridad continua no está habilitada para este plan de copia de seguridad; para obtener más información, consulte Restaurar a una hora específica mediante la point-in-time restauración (PITR).

Clave de etiqueta: `ams:rt:backup-orchestrator-onboarding`

Valor TAG: `true`

| Plan de respaldo de incorporación de AMS Accelerate | Start Time | Retención |
|---|---|---|
| respaldo por hora | cada hora | 2 semanas |
| copia de seguridad diaria | N/A | N/A |
| copia de seguridad semanal | N/A | N/A |
| copia de seguridad mensual | N/A | N/A |
| copia de seguridad anual | N/A | N/A |

AWS Backup Temas relacionados

- Crear un plan de respaldo
- Point-in-time La restauración (PITR) permite realizar copias de seguridad continuas de los recursos compatibles y le permite seleccionar un momento específico para la recuperación. Para obtener una lista de los recursos compatibles, consulte Disponibilidad de funciones por recurso.

## Etiquete sus recursos para aplicar los planes de respaldo de AMS

Para asignar recursos a un plan de respaldo de AMS, etiquete el recurso con el par clave-valor del plan. Puede usar el etiquetador de recursos de AMS para aplicar los planes de respaldo de AMS a un subconjunto de sus recursos o a todos los recursos compatibles de su cuenta. Si quieres usar un método alternativo para aplicar etiquetas a tus recursos, como AWS CloudFormation o Terraform, desactiva Resource Tagger para que no compita con el método de etiquetado que hayas elegido. Para obtener más información, consulte Impedir que Resource Tagger modifique los recursos.

El siguiente ejemplo demuestra cómo puede usar Resource Tagger para aplicar el plan de respaldo de AMS predeterminado en las instancias de Amazon Elastic Compute Cloud de su cuenta. Para este plan de respaldo, aplique la clave `ams:rt:backup-orchestrator` y el valor `true` de la etiqueta. Para usar un plan de respaldo diferente, cambie la clave para que coincida con la clave de etiqueta del plan de respaldo que desee. Para obtener más información sobre AMS Resource Tagger

y comprender cómo integrar el siguiente perfil de referencia con el perfil actual (ya configurado) de su cuenta de Accelerate, consulteAcelere el etiquetador de recursos.

1. Abra la AWS AppConfig consola en https://console.aws.amazon.com/systems-manager/appconfig.
2. Elija la aplicación de ResourceTagger.
3. Seleccione la pestaña Perfiles de configuración y, a continuación, elija CustomerManagedTags
4. Seleccione Crear para crear una nueva versión.
5. Selecciona JSON y, a continuación, copia y pega el siguiente objeto JSON:

```
{
    "AWS::EC2::Instance": {
        "AccelerateBackupPlan": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "*"
                    }
                ]
            },
            "Tags": [
                {
                    "Key": "ams:rt:backup-orchestrator",
                    "Value": "true"
                }
            ]
        }
    }
}
```

6. Seleccione Crear versión de configuración alojada.
7. Elija Iniciar la implementación.
8. Defina los siguientes detalles de implementación:

```
Environment: AMSInfrastructure
Hosted configuration version: Select the version that you have just created.
Deployment Strategy: AMSNoBakeDeployment
```

9. Elija Iniciar la implementación. Resource Tagger etiqueta las instancias `ams:rt:backup-orchestrator: true` para garantizar que las copias de seguridad de las mismas se realicen de acuerdo con el plan de copias de seguridad predeterminado de AMS.

## Ver copias de seguridad en bóvedas de AMS

Puede controlar las notificaciones del almacén de copias de seguridad a nivel de almacén individual mediante etiquetas. Puede inhabilitar las notificaciones de un almacén específico añadiendo la etiqueta `AMSNotificationOptOut` y configurando el valor `True` en un almacén específico. Para volver a recibir notificaciones del almacén, elimina la etiqueta.

Para ver una lista de las copias de seguridad de AMS, abra la AWS Backup consola. En el panel de navegación, elija Backup Vaults y seleccione uno de los almacenes de respaldo AMS de las siguientes tablas. En la sección Copias de seguridad, consulte la lista de todas las copias de seguridad del almacén de copias de seguridad. Seleccione una copia de seguridad para editarla, eliminarla o restaurarla.

Bóvedas para planes de backup de AMS

| Nombre de la bóveda de AMS | Clave de etiqueta del Plan de Backup de AMS |
|---|---|
| ams-automated-backups | ams:rt:backup-orchestrator |
| ams-automated-enhanced-backups | ams:rt: backup-orchestrator-enhanced |
| ams-automated-data-sensitive- copias de seguridad | ams: rt: backup-orchestrator-data-sensitive |
| ams-onboarding-backups | ams:rt: backup-orchestrator-onboarding |

Otras bóvedas de AMS

| Nombre de la bóveda de AMS | Descripción |
|---|---|
| ams-manual-backups | Este almacén contiene copias de seguridad iniciadas manualmente creadas en el documento de automatización de `AWSManagedServices-StartBackupJob` SSM y |

| Nombre de la bóveda de AMS | Descripción |
| --- | --- |
| | copias de seguridad previas a los parches creadas por las automatizaciones de parches de AMS antes de aplicar los parches. |
| ams-custom-backups | Este es el almacén recomendado para las copias de seguridad creadas fuera de los planes de copias de seguridad de AMS. |

AWS Backup Temas relacionados

- Ver copias de seguridad por recurso
- Trabajando con copias de seguridad

## Monitorización e informes de copias de seguridad de AMS

> **Important**
>
> La supervisión y los informes de las copias de seguridad de AMS solo están disponibles en las regiones compatibles con AMS. Estos son EE.UU. Este (Virginia), EE.UU. Oeste (Norte de California), EE.UU. Oeste (Oregón), EE.UU. Este (Ohio), Canadá (Centro), Sudamérica (São Paulo), UE (Irlanda), UE (Fráncfort), UE (Londres), UE (París), Asia Pacífico (Bombay), Asia Pacífico (Seúl), Asia Pacífico (Singapur), Asia Pacífico (Sídney), Asia Pacífico (Tokio).

AMS genera informes de autoservicio diarios, así como informes mensuales sobre la cobertura de los recursos y el estado de las tareas de respaldo. Los informes mensuales se comparten en Monthly Business Reviews (MBRs). Para obtener más información sobre los informes de respaldo diarios, consulte Informe de respaldo diario Informe .

Los expertos de AMS supervisan todas las tareas de copia de seguridad configuradas mediante AWS Backup. En caso de que se produzcan errores en la copia de seguridad, AMS la investigará y le notificará la causa raíz y las opciones de reparación, si están disponibles. Para evitar el ruido de las alertas, durante los eventos que provocan un gran número de fallos en las copias de seguridad de sus cuentas, AMS hace una recomendación colectiva, a través de su CSDM, en lugar de notificarle cada fallo individual.

Tenga en cuenta que AMS no supervisa ninguna copia de seguridad configurada mediante la función de copia de seguridad independiente de un AWS servicio.

# Comprenda la administración de parches en AMS Accelerate

**Important**

Accelerate Patch Reporting implementa periódicamente una política basada en AWS Glue los recursos. Tenga en cuenta que las actualizaciones de AMS en el sistema de parches sobrescriben las políticas basadas en recursos existentes. AWS Glue

**Important**

Puede especificar repositorios de parches alternativos para los nodos gestionados. Mientras AMS implementa las configuraciones de parches solicitadas, usted es responsable de seleccionar y validar la seguridad de los repositorios elegidos. También debe aceptar cualquier riesgo derivado del uso de estos repositorios, como los riesgos de la cadena de suministro.
Las siguientes son las prácticas recomendadas para la seguridad del proceso de administración de parches:

- Utilice únicamente fuentes de repositorio confiables y verificadas
- Utilice de forma predeterminada los repositorios de los proveedores de sistemas operativos estándar cuando sea posible
- Audite periódicamente las configuraciones de los repositorios personalizados

Puede usar el sistema de parches AMS Accelerate, Patch Add-On, para parchear sus instancias con actualizaciones relacionadas con la seguridad y de otro tipo. Accelerate Patch Add-On es una función que proporciona parches basados en etiquetas para las instancias de AMS. Aprovecha la funcionalidad AWS Systems Manager (SSM) para etiquetar instancias y parchearlas mediante una línea base y una ventana que usted configure. El parche AMS Accelerate Add-On es una opción de integración. Si no lo obtuvo al incorporar su cuenta de Accelerate, póngase en contacto con su administrador de prestación de servicios en la nube (CSDM) para obtenerlo.

La administración de parches de AMS Accelerate utiliza la funcionalidad básica de parches de Systems Manager para controlar la definición de los parches que se aplican a una instancia. La

línea base de parches contiene la lista de parches que están aprobados previamente; por ejemplo, todos los parches de seguridad. La conformidad de la instancia se mide con respecto a la línea base del parche asociada a ella. De forma predeterminada, AMS Accelerate instala todos los parches disponibles para mantener la instancia actualizada.

> **Note**
>
> AMS Accelerate aplica únicamente los parches del sistema operativo (SO). Por ejemplo, para Windows, solo se aplican las actualizaciones de Windows, no las de Microsoft.

Para obtener información sobre los informes, consulteInformes de gestión de hosts de AMS.

AMS Accelerate ofrece una gama de servicios operativos para ayudarlo a alcanzar la excelencia operativa en AWS. Para comprender rápidamente cómo AMS ayuda a sus equipos a alcanzar la excelencia operativa general Nube de AWS con algunas de nuestras capacidades operativas clave, como el servicio de asistencia las 24 horas del día, los 7 días de la semana, la supervisión proactiva, la seguridad, la aplicación de parches, el registro y la copia de seguridad, consulte los diagramas de arquitectura de referencia de AMS.

Temas

- Recomendaciones de aplicación de parches
- Cree una ventana de mantenimiento de parches en AMS
- Parche con ganchos
- Línea base del parche AMS Accelerate
- Creación de una función de IAM para la aplicación de parches bajo demanda a AMS Accelerate
- Comprenda las notificaciones de parches y los fallos de los parches en AMS Accelerate

## Recomendaciones de aplicación de parches

Si se dedica a operaciones de aplicaciones o infraestructuras, entiende la importancia de una solución de revisión del sistema operativo (SO) que sea lo suficientemente flexible y escalable como para cumplir con los diversos requisitos de sus equipos de aplicaciones. En una organización típica, algunos equipos de aplicaciones utilizan una arquitectura que incluye instancias inmutables, mientras que otros implementan sus aplicaciones en instancias mutables.

Para obtener más información sobre AWS las directrices prescriptivas para la aplicación de parches, consulte Aplicación automática de parches para instancias mutables en la nube híbrida mediante el uso de parches. AWS Systems Manager

> **Note**
>
> Accelerate Patch Add-On es una función que proporciona parches basados en etiquetas para las instancias de AMS. Aprovecha la funcionalidad AWS Systems Manager (SSM) para etiquetar instancias y parchearlas mediante una línea base y una ventana que usted configure. El parche AMS Accelerate Add-On es una opción de integración. Si no lo obtuvo al incorporar su cuenta de Accelerate, póngase en contacto con su administrador de prestación de servicios en la nube (CSDM) para obtenerlo.

## Recomendaciones sobre la responsabilidad del parche

El proceso de aplicación de parches para las instancias persistentes debe incluir los siguientes equipos y acciones:

- Los equipos de aplicaciones definen los grupos de parches para sus servidores en función del entorno de la aplicación, el tipo de sistema operativo u otros criterios. DevOps También definen los períodos de mantenimiento específicos de cada grupo de revisiones. Esta información debe almacenarse en las etiquetas adjuntas a las instancias. Los nombres de etiqueta recomendados son «Grupo de parches» y «Ventana de mantenimiento». Durante cada ciclo de revisiones, los equipos de aplicaciones se preparan para aplicar las revisiones, prueban la aplicación después de aplicarlos y solucionan cualquier problema con sus aplicaciones y su sistema operativo durante la aplicación de las revisiones.
- El equipo de operaciones de seguridad define las líneas base de los parches para los distintos tipos de sistemas operativos que utilizan los equipos de aplicaciones y hace que los parches estén disponibles a través de Systems Manager Patch Manager.
- La solución de parches automatizada se ejecuta de forma regular e implementa los parches definidos en las líneas base de parches, en función de los grupos de parches definidos por el usuario y los períodos de mantenimiento.
- Los equipos de gobierno y cumplimiento definen las directrices de aplicación de parches y los procesos y mecanismos de excepción.

Para obtener más información, consulte Diseño de soluciones de parches para instancias EC2 mutables.

## Guía para los equipos de aplicaciones

- Revise y familiarícese con la creación y administración de ventanas de mantenimiento; consulte Ventanas de AWS Systems Manager mantenimiento y Creación de una ventana de mantenimiento de SSM para la aplicación de parches para obtener más información. Comprender la estructura general y el uso de las ventanas de mantenimiento le ayuda a comprender qué información debe proporcionar si no es usted quien las ha creado.
- Para las configuraciones de alta disponibilidad (HA), planifique tener una ventana de mantenimiento por zona de disponibilidad y por entorno (Dev/Test/Prod). Esto garantizará la disponibilidad continua durante la aplicación de parches.
- La duración recomendada del período de mantenimiento es de 4 horas con un límite de 1 hora, más 1 hora adicional por cada 50 instancias
- Parchee las versiones de desarrollo y prueba con suficiente tiempo entre cada una para que pueda identificar cualquier posible problema antes de aplicar los parches de producción.
- Automatice las tareas habituales previas y posteriores a la aplicación de parches mediante la automatización de SSM y ejecútelas como tareas de mantenimiento. Tenga en cuenta que, para las tareas posteriores a la aplicación de parches, debe asegurarse de que hay suficiente tiempo asignado, ya que las tareas no se iniciarán una vez que se alcance el límite.
- Familiarícese con las líneas base de los parches y sus características, especialmente en lo que respecta a los retrasos en la aprobación automática de los tipos de gravedad de los parches, que se pueden utilizar para garantizar que solo los parches que se aplicaron en producción Dev/Test se apliquen posteriormente. Consulte Acerca de las bases de referencia de los parches para obtener más información.

## Guía para los equipos de operaciones de seguridad

- Revise las bases de referencia de los parches y familiarícese con ellas. La aprobación de los parches se gestiona de forma automática y tiene diferentes opciones de reglas. Consulte Acerca de las líneas base de los parches para obtener más información.
- Analice las necesidades relacionadas con la aplicación de parches Dev/Test/Prod con los equipos de aplicaciones y desarrolle varias líneas de base para adaptarlas a estas necesidades.

## Guía para los equipos de gobierno y cumplimiento

- La aplicación de parches debe ser una función de «exclusión voluntaria». Debe haber un período de mantenimiento predeterminado y un etiquetado automático para garantizar que nada quede sin corregir. AMS Resource Tagger puede ayudarle en este sentido; consulte esta opción con su arquitecto de nube (CA) o administrador de prestación de servicios en la nube (CSDM) para obtener orientación sobre la implementación.
- Las solicitudes de exención de la aplicación de parches deben requerir documentación que justifique la exención. Un director de seguridad de la información (CISO) u otro oficial de aprobación debe aprobar o denegar la solicitud.
- El cumplimiento de los parches debe revisarse periódicamente a través de la consola de Patch Manager, Security Hub o un escáner de vulnerabilidades.

## Ejemplo de diseño para una aplicación Windows de alta disponibilidad

Información general:

- Una ventana de mantenimiento por zona de disponibilidad.
- Un conjunto de ventanas de mantenimiento por entorno.
- Un parche de referencia por entorno:
  - Desarrollador: apruebe toda la gravedad y la clasificación después de 0 días.
  - Prueba: apruebe los parches de actualización de seguridad críticos después de 0 días y todas las demás clasificaciones y grados de gravedad después de 7 días.
  - Producto: Apruebe las actualizaciones de seguridad críticas después de 0 días y todas las demás clasificaciones y niveles de gravedad después de 14 días.

CloudFormation Guiones:

Estos scripts se configuran para crear los períodos de mantenimiento, las líneas base y las tareas de aplicación de parches para una aplicación EC2 de Windows HA con dos zonas de disponibilidad utilizando la configuración de aprobación básica descrita anteriormente.

- Ejemplo de la pila CFN para desarrolladores de Windows: HA-Patching-Dev-Stack.json
- Ejemplo de Windows Test CFN Stack: HA-Patching-Test-Stack.json

- Ejemplo de pila de CFN de Windows Prod: HA-Patching-Prod-Stack.json

## Preguntas frecuentes sobre recomendaciones de parches

P: ¿Cómo puedo gestionar los parches no programados para las vulnerabilidades de «0» días?

R: SSM admite la función Patch Now que utiliza la línea base predeterminada actual para el sistema operativo de la instancia. AMS implementa un conjunto predeterminado de líneas base de parches que aprueba todos los parches después de 0 días. Sin embargo, cuando se utiliza la función Patch Now, no se toma una instantánea previa al parche, ya que este comando ejecuta el documento SSM. AWS-RunPatchBaseline Se recomienda realizar una copia de seguridad manual antes de aplicar el parche.

P: ¿AMS admite la aplicación de parches para instancias en Auto-Scaling grupos (ASG)?

R: No. En este momento, los clientes de Accelerate no admiten los parches de ASG.

P: ¿Hay alguna limitación que debas tener en cuenta para Maintenance Windows?

R: Sí, hay algunas limitaciones que debe tener en cuenta.

- Windows de mantenimiento por cuenta: 50
- Tareas por período de mantenimiento: 20
- Número máximo de automatizaciones simultáneas por ventana de mantenimiento: 20
- Número máximo de ventanas de mantenimiento simultáneas: 5

Para obtener una lista completa de los límites de SSM predeterminados, consulte AWS Systems Manager puntos finales y cuotas.

# Cree una ventana de mantenimiento de parches en AMS

Un período de mantenimiento de parches ejecuta las automatizaciones de parches de AMS según un cronograma establecido para las EC2 instancias de Amazon específicas. Los objetivos se definen mediante una o varias etiquetas para un grupo de instancias. Puedes establecer horarios en función de los días y las horas en torno a Patch Tuesday, o puedes definir un horario mediante una expresión cron. Para obtener más información, consulte Referencia: expresiones cron y rate para Systems Manager en la Guía del usuario de AWS Systems Manager . Antes de aplicar los parches,

AMS crea una instantánea del volumen raíz de cada instancia. Si AMS detecta que la aplicación de parches afecta al estado de la instancia o si usted notifica a AMS el impacto de la aplicación a causa de la aplicación de parches, AMS utilizará esta instantánea para restaurar el volumen raíz al estado anterior al parche.

## AMS Accelerate: límites del período de mantenimiento de los parches

Usos de parcheo AMS AWS Systems Manager (Systems Manager). Además de los límites de servicio de Systems Manager, la aplicación de parches de AMS tiene un límite de 300 instancias de destino por período de mantenimiento de parches. Dado que el tiempo general de finalización de los parches es de 30 minutos por instancia, en la siguiente tabla se proporcionan ejemplos del número de intervalos y la duración del mantenimiento.

| Instancias para parchear | Duración de los períodos de mantenimiento (horas) | Se necesitan períodos de mantenimiento simultáneos |
|---|---|---|
| 100 | 1 | 1 |
| 200 | 1 | 1 |
| 300 | 2. | 1 |
| 600 | 3 | 2 |
| 800 | 4 | 3 |
| 1200 | 6 | 4 |
| 1500 | 8 | 5 |

> **Important**
>
> En estos ejemplos se supone que no hay otras ventanas de mantenimiento de Systems Manager activas ni se están ejecutando otras automatizaciones.

Para obtener más información sobre los límites, consulte AWS Systems Manager puntos finales y cuotas.

Temas


- Cree una ventana de mantenimiento periódica «Patch Tuesday» desde la consola AMS (recomendado)
- Cree una ventana de mantenimiento de parches con CloudFormation AMS Accelerate
- Cree una ventana de mantenimiento desde la consola de Systems Manager para AMS Accelerate
- Cree una ventana de mantenimiento con la interfaz de línea de comandos (CLI) de Systems Manager para AMS Accelerate


## Cree una ventana de mantenimiento periódica «Patch Tuesday» desde la consola AMS (recomendado)

Microsoft lanza parches para sus sistemas operativos el segundo martes de cada mes, también conocido como Patch Tuesday. Es habitual programar la aplicación de parches para las instancias de Windows y Linux en relación con el Patch Tuesday. Para programar períodos de mantenimiento periódicos de los parches el primer o segundo fin de semana después del martes de parches, visita la consola AMS y sigue estos pasos:

1. Introduce un nombre para la ventana de mantenimiento de los parches.
2. [opcional] Proporcione una descripción del período de mantenimiento del parche.
3. Selecciona un día relacionado con el martes de parches.
4. Introduzca una hora para que comience el período de mantenimiento del parche en hh:mm. Por ejemplo, medianoche son las 00:00 y las 23:00 horas. A continuación, selecciona una zona horaria.
5. [opcional] Cambia la duración para adaptarla a tus necesidades. AMS recomienda una duración mínima de cuatro horas.
6. Introduzca la clave y el valor de una etiqueta de parche para el objetivo. Para obtener más información, consulte ¿Qué son las etiquetas? .
7. [opcional] Amplíe los parámetros opcionales para ajustar la simultaneidad, la tasa de errores y el límite de la ventana de mantenimiento.

    1. La simultaneidad controla el número de instancias de destino que se están aplicando parches al mismo tiempo. Por ejemplo, una simultaneidad del 50% para 10 instancias de destino no parcheará más de 5 instancias a la vez, mientras que una simultaneidad del 100% parcheará las 10 a la vez.

2. La tasa de errores controla la tolerancia a los errores antes de que se suspenda la aplicación de parches. Por ejemplo, una tasa de error del 100% para 10 instancias de destino parcheará todas las instancias sin importar cuántas fallen, mientras que una tasa de error del 50% suspenderá la aplicación de parches una vez que 5 instancias no hayan podido parchear. AMS recomienda una tasa de error del 100%.
3. El cierre del período de mantenimiento de los parches evita que se rompa el período de mantenimiento de los parches al suspender el inicio de nuevas actividades de aplicación de parches las horas especificadas antes de que finalice el período de mantenimiento de los parches. Por ejemplo, un límite de 1 hora (recomendado) interrumpe las actividades de los nuevos parches 1 hora antes de que finalice el período de mantenimiento del parche.

> **Important**
>
> Compruebe la hora de la próxima ejecución.
> Visite la consola de la ventana de mantenimiento de SSM, busque la ventana de mantenimiento del parche recién creada y compruebe la hora de la próxima ejecución. Si tiene alguna duda o necesita editar el período de mantenimiento de los parches, cree una solicitud de servicio para hablar con un experto en parches de AMS

Para programar un período de mantenimiento de parches basado en CRON utilizando CloudFormation, consulte. Cree una ventana de mantenimiento de parches con CloudFormation AMS Accelerate

## Cree una ventana de mantenimiento de parches con CloudFormation AMS Accelerate

Para crear una ventana de mantenimiento de parches de AMS Accelerate utilizando AWS CloudFormation, primero inicie sesión en su cuenta de Accelerate y seleccione la ubicación en la Región de AWS que se encuentran las instancias de destino. A continuación, siga estos pasos en https://console.aws.amazon.com/cloudformation:

1. Seleccione una de las dos plantillas de parches CloudFormation personalizadas de Accelerate.
   - Programación del martes de parches: Microsoft publica parches para sus sistemas operativos el segundo martes de cada mes, también conocido como martes de parches, para programar los períodos de mantenimiento de parches el primer o segundo fin de semana después del

martes de parches: una vez que haya iniciado sesión en la consola de Accelerate, utilice esta PatchTuesdayScheduling CloudFormation plantilla de enlaces.

- Programación de CRON: para crear ventanas de mantenimiento de parches utilizando CRON para definir el día de inicio, utilice esta plantilla de enlaces CRONScheduling CloudFormation . Recuerde que los CRON de Systems Manager numeran los días del 1 al 7 (para obtener más información sobre el CRON de Systems Manager, consulte Referencia: Cron y expresiones de velocidad para Systems Manager).

Al elegir uno de estos enlaces, la plantilla se carga automáticamente en la consola. CloudFormation Haga clic en Next (Siguiente).

2. En la página Especificar los detalles de la pila (paso 2 de las páginas Crear pila), introduzca el nombre de la pila y los parámetros de la plantilla (los parámetros predeterminados que se muestran son los valores predeterminados recomendados por AMS; seleccione el día y la hora para su caso de uso). Cuando haya terminado, haga clic en Next (Siguiente).
3. Configure las opciones de pila (opcional). Para obtener información sobre las opciones, consulte Configuración de las opciones de CloudFormation pila de AWS. Cuando haya terminado, haga clic en Next (Siguiente).
4. Revise los valores de su pila (opcional). Para obtener información sobre cómo revisar los detalles de la pila para estimar los costos, consulta Cómo revisar la pila y estimar el costo de la pila. Cuando estés listo, haz clic en Crear pila.

   La creación de la pila puede tardar hasta un minuto. Una vez que la pila se haya creado correctamente, el período de mantenimiento de los parches se ejecutará a la hora especificada. Puede realizar cambios en la ventana de mantenimiento de parches creando y ejecutando un conjunto de CloudFormation cambios (recomendado) (para obtener más información sobre cómo hacerlo, consulte Creación de pilas mediante conjuntos de cambios) o actualizando la ventana de mantenimiento de parches en la consola de la ventana de mantenimiento de Systems Manager (). https://console.aws.amazon.com/systems-manager/maintenance-windows

Vea el vídeo de Namrata para obtener más información (5:41)

## Cree una ventana de mantenimiento desde la consola de Systems Manager para AMS Accelerate

Para crear una ventana de mantenimiento de AMS Accelerate desde la consola de Systems Manager, siga estos pasos:

1. En la barra de navegación izquierda del área de administración de cambios, haga clic en Windows de mantenimiento y, a continuación, en Crear ventana de mantenimiento en la parte superior derecha de la pantalla. Rellene el formulario. Para obtener más información sobre cualquiera de las opciones, consulte Crear una ventana de mantenimiento (consola). Cuando haya terminado, haga clic en Crear ventana de mantenimiento.

   Se abre la página de lista de ventanas de mantenimiento.
2. Seleccione la ventana de mantenimiento recién creada.

   Se abre la página de detalles de la ventana de mantenimiento.
3. Vaya a la pestaña Objetivos y elija Registrar objetivo.

   Se abre la página de destino de Registrar.
4. Añada su objetivo de Accelerate. Para obtener información sobre los objetivos, consulte Asignar objetivos a una ventana de mantenimiento (consola). Cuando haya terminado, haga clic en Registrar destino. Anote el objetivo, ya que lo necesitará más adelante.

   La página de detalles de la ventana de mantenimiento se vuelve a abrir en la pestaña Objetivos con una lista que incluye el nuevo objetivo.
5. En la pestaña Tareas de la página de detalles de la ventana de mantenimiento, seleccione Registrar tarea y, a continuación, seleccione Registrar tarea de automatización en la lista desplegable. Rellene el formulario. Acelera las notas:

   - Proporcione un nombre de tarea significativo. Por ejemplo: AcceleratePatch.
   - En el área de documentos de automatización, haga clic en el cuadro de búsqueda, seleccione Propietario y, a continuación, Documentos compartidos.
   - Seleccione el documento de automatización haciendo clic en el cuadro de búsqueda y seleccionando Prefijo del nombre del documento --> Igual y, a continuación, escribiendo: AWSManagedServices-PatchInstance. A continuación, seleccione el AWSManagedServices-PatchInstancedocumento pulsando su botón de radio.
   - En Versión del documento, elija Versión predeterminada en tiempo de ejecución.
   - En la sección Objetivos:
     - Defina el objetivo de la siguiente manera: para seleccionar los grupos objetivo registrados.
     - En la lista de objetivos, seleccione el objetivo que registró en la pestaña Objetivos.
   - En la sección Parámetros de entrada, rellene el formulario.
     - InstanceId: {{*TARGET_ID*}}

- StartInactiveInstances: `True` para iniciar las instancias si se detienen durante el período de mantenimiento del parche.

> **Note**
>
> El valor del InstanceIdparámetro distingue entre mayúsculas y minúsculas y puede ser verdadero o falso. StartInactiveInstances
> Las instancias detenidas no se pueden iniciar cuando están segmentadas por etiquetas. Para obtener más información, consulte No hay invocaciones que ejecutar.

- En la sección Control de tasas, selecciona porcentajes. AMS Accelerate recomienda el 100% para la simultaneidad y el 100% para el umbral de error para intentar parchear todas las instancias simultáneamente, independientemente de los errores de automatización. Si desea aplicar parches a la mitad de sus objetivos a la vez, por ejemplo, para mantener en funcionamiento la mitad de las instancias de destino que están detrás de un equilibrio de carga, defina la simultaneidad en el 50%.
- En la sección Función de servicio de IAM, selecciona Usar una función de servicio personalizada y, a continuación, selecciona ams_ssm_automation_role.

Haga clic en Registrar tarea de automatización.

Se crea la ventana de mantenimiento de los parches. En la pestaña Descripción, puede ver la próxima hora de ejecución.

## Cree una ventana de mantenimiento con la interfaz de línea de comandos (CLI) de Systems Manager para AMS Accelerate

Para crear una ventana de mantenimiento de AMS Accelerate con la interfaz de línea de comandos:

1. Siga el tutorial de SSM: Creación y configuración de una ventana de mantenimiento (AWS CLI). Para cada paso del tutorial, aquí hay ejemplos de comandos CLI para aplicar parches.

> **Note**
>
> Estos ejemplos son específicos de Linux o macOS. Los comandos también se pueden ejecutar desde allí AWS CloudShell , lo que puede resultar más sencillo que `awscli`

configurarlos en una máquina local. Para obtener más información, consulte Trabajar con AWS CloudShell.

a. En el paso 1 del tutorial, para crear una ventana de mantenimiento:

```
aws ssm create-maintenance-window \
                --name Sample-Maintenance-Window \
                --schedule "cron(0 30 23 ? * TUE#2 *)" \
                --duration 4 \
                --cutoff 1 \
                --allow-unassociated-targets \
                --tags "Key=Environment,Value=Production"
```

Al finalizar satisfactoriamente, `window-id` se devuelve.

b. En el paso 2 del tutorial, para registrar un nodo de destino:

```
aws ssm register-target-with-maintenance-window \
                --window-id "mw-xxxxxxxxx" \
                --resource-type "INSTANCE" \
                --target "Key=tag:Environment,Values=Prod"
```

Si se completa correctamente, `WindowTargetID` se devuelven.

c. En el paso 3 del tutorial, para registrar una tarea:

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-xxxxxx" \
    --targets "Key=WindowTargetIds,Values=63d4f63c-xxxxxx-9b1d-xxxxxfff" \
    --task-arn "AWSManagedServices-PatchInstance" \
    --service-role-arn "arn:aws:iam::AWS-Account-ID:role/ams_ssm_automation_role"
 \
    --task-invocation-parameters "{\"Automation\":{\"DocumentVersion\":\"\$DEFAULT
\",\"Parameters\":{\"InstanceId\":[\"{{TARGET_ID}}\"],\"StartInactiveInstances\":
[\"True\"]}}}" \
    --max-concurrency 50 \
    --max-errors 50 \
    --name "AutomationExample" \
    --description "Sample Description" \
    --task-type=AUTOMATION
```

# Parche con ganchos

Puede configurar los parches de AMS para que ejecuten comandos a nivel del sistema operativo (SO) antes y después de aplicar los parches mediante los patch hooks de AMS. Utilice los patch hooks de AMS para ejecutar los documentos de comandos SSM con el fin de detener un servicio antes de aplicar los parches e iniciarlo después de aplicarlos, o bien para ejecutar comandos que confirmen que la aplicación está en buen estado después de aplicarlos.

Para utilizar los patch hooks de AMS, debe hacer lo siguiente:

1. Cree documentos de comandos SSM para usarlos como enlaces de parches.
2. Cree una ventana de mantenimiento de parches de AMS o utilice una ventana de mantenimiento de parches de AMS existente. Para obtener más información, consulte la ventana de mantenimiento de los parches de AMS.
3. Configure una ventana de mantenimiento de los parches de AMS para utilizar los documentos de comandos de SSM para los patch hooks de AMS.

## Los enganches de conexión AMS RACI

La matriz responsable, responsable, consultada e informada (RACI, por sus siglas en inglés) asigna la responsabilidad principal al cliente o a AMS en relación con una variedad de actividades. En la siguiente tabla se ofrece un resumen de las responsabilidades del cliente y de AMS en relación con las actividades de una aplicación que utiliza los patch hooks de AMS.

- R significa la parte responsable que hace el trabajo para lograr la tarea
- A representa a la parte responsable
- C significa consultada; la parte cuya opinión se solicita, normalmente como experta en la materia; y con la que existe comunicación bilateral
- I significa informado; la parte que recibe información sobre el progreso, a menudo solo una vez finalizada la tarea o el producto

| Actividad | Cliente | AMS |
|---|---|---|
| Cree un pre/post parche para el documento SSM Command y documente el contenido | R | C |
| Configure los parámetros del patch hook para la aplicación de parches a AMS | R | C |
| Ejecute el pre/post documento de comandos SSM del parche | I | R |
| Clasifique y responda a las fallas del patch hook | I | R |
| Notifique al cliente si se produce un fallo en el enganche | I | R |
| Si el cliente lo solicita, vuelva a un estado anterior al parche | C | R |

## Cree documentos SSM para los patch hooks

Los patch hooks de AMS utilizan documentos de Amazon EC2 Systems Manager (SSM) durante la aplicación de parches. Cree un documento de comandos SSM o comparta un documento de comandos SSM existente con la cuenta en la que se realiza la aplicación de parches. Para obtener información sobre los documentos SSM, incluidas las limitaciones, consulte Compartir documentos SSM.

Para crear un documento de comandos SSM, sigue estos pasos:

1. Cree un documento SSM con el tipo de documento = «Comando».
2. Introduzca sus comandos en la sección de contenido. Para obtener más información, consulte Creación del contenido de un documento SSM.

> **Note**
>
> Los documentos SSM para los patch hooks de AMS también se pueden crear con AWS CLI o. CloudFormation Si necesita ayuda para crear documentos SSM para sus patch hooks de AMS, póngase en contacto con su arquitecto de nube.

## Configure la ventana de mantenimiento de parches de AMS para utilizar sus documentos de comandos de SSM como enlaces de parches de AMS

Una ventana de mantenimiento de parches de AMS es una ventana de mantenimiento de Systems Manager que ejecuta la automatización de parches de AMS configurada.

Para editar una ventana de mantenimiento de parches de AMS para utilizar los patch hooks, siga estos pasos:

1. En la sección Herramientas de gestión de cambios https://console.aws.amazon.com/systems-manager/, en el panel de navegación izquierdo, selecciona Maintenance Windows.

   Se abre una página con una lista de las ventanas de mantenimiento existentes.
2. Seleccione un identificador de ventana que empiece por mw-.

   Se abre la página de detalles de esa ventana de mantenimiento.
3. Seleccione la pestaña Tareas y el ID de tarea de la ventana con el ARN de la tarea de AMS-PatchInstancey haga clic en Editar.

4. Desplácese hacia abajo hasta la sección Parámetros y actualice los siguientes parámetros.

Parámetros del patch hook de AMS:

- PrePatchHook: El nombre del documento SSM del tipo «Comando» que desea ejecutar antes de aplicar el parche. Déjelo en blanco o escriba "AWS-Noop" (distingue entre mayúsculas y minúsculas) si no está ejecutando un comando antes de aplicar el parche.
- PostPatchHook: el nombre del documento SSM con el tipo «Comando» que desea ejecutar después de aplicar el parche. Déjelo en blanco o escriba "AWS-Noop" (distingue entre mayúsculas y minúsculas) si no está ejecutando un comando después de aplicar el parche.

- ExecutePatchBasedOnPreHookStatus: Ejecute el parche en función del éxito o el fracaso de la PrePatchHook ejecución, elija una de las siguientes opciones:
  - OnPreHookSuccess: Ejecute la automatización de parches de AMS únicamente cuando PrePatchHook se haya realizado correctamente.
  - Siempre: ejecute la automatización de parches de AMS cuando PrePatchHook la aplicación tenga éxito y cuando falle.
  - OnPreHookFailure- Ejecute la automatización de parches de AMS solo cuando PrePatchHook falle.
  - Nunca: no ejecute la automatización de parches de AMS. Esto puede resultar útil a la hora de probar su PrePatchHook.
- ExecutePostHookBasedOnPatchStatus: Ejecute el enlace posterior al parche en función del éxito o el fracaso de la automatización de parches de AMS, elija una de las siguientes opciones:
  - OnPatchSuccess: Solo ejecútelo PostPatchHook cuando la automatización de parches de AMS se ejecute correctamente.
  - Siempre: ejecútelo PostPatchHook cuando la automatización de parches de AMS se realice correctamente y cuando falle.
  - OnPatchFailure- Ejecútelo PostPatchHook solo cuando falle la automatización de los parches de AMS.

> **Note**
>
> Si a alguna de estas variables le falta su cuadro de texto, corrija el problema desplazándose hacia arriba hasta la sección de documentos de automatización de la misma página, seleccionando un documento diferente y, a continuación, volviendo a seleccionar el documento original. Esto actualiza los parámetros de entrada para que pueda editarlos.

# Línea base del parche AMS Accelerate

Una base de referencia de parches define los parches aprobados para instalación en las instancias. Puede especificar revisiones aprobadas o rechazadas de forma de uno en uno. También puede crear reglas de aprobación automática para especificar que determinados tipos de actualizaciones (por ejemplo, las actualizaciones críticas) se deben aprobar automáticamente. La lista de rechazados anula las reglas y la lista de aprobados.

## Línea base predeterminada del parche

Al incorporar los parches de AMS Accelerate, las líneas base de parches predeterminadas se sustituyen por las líneas base de parches predeterminadas de AMS Accelerate para los siguientes sistemas operativos.

- Windows
- Amazon Linux 1
- Amazon Linux 2
- CentOS
- Suse
- Rhel
- Ubuntu

> **Important**
>
> AMS administra las líneas base de los parches predeterminadas. No edite las líneas base de los parches predeterminadas, ya que es posible que se pierdan los cambios. En su lugar, cree una línea base de parche personalizada. Consulte Línea base de parches personalizada con AMS Accelerate

> **Note**
>
> Las líneas base de los parches de AMS Accelerate definidas como product = * significan que todos los parches se aplican a la instancia de todos los tipos de seguridad y clasificaciones.

## Línea base de parches personalizada con AMS Accelerate

Para usar una línea base de parches personalizada con AMS Accelerate, primero asegúrese de tener un grupo de parches y, a continuación, cree la línea base personalizada.

Para obtener más información, consulte los siguientes recursos:

- Trabaje con grupos de parches

- Crear una línea base de parches personalizada (Windows)
- Crear una línea base de parche personalizada (Linux)
- Actualizar o eliminar una línea base de parches personalizada (consola)

# Creación de una función de IAM para la aplicación de parches bajo demanda a AMS Accelerate

Una vez que su cuenta está incorporada a AMS Accelerate Patching, AMS Accelerate implementa una política gestionada, amspatchmanagedpolicy. Esta política contiene los permisos necesarios para la aplicación de parches bajo demanda mediante el documento de automatización de AMS. `AWSManagedServices-PatchInstance` Para usar este documento de automatización, el administrador de la cuenta crea un rol de IAM para los usuarios. Siga estos pasos:

Cree un rol mediante: Consola de administración de AWS

1. Inicie sesión en la consola de IAM Consola de administración de AWS y ábrala.
2. En el panel de navegación de la consola, selecciona Funciones y, a continuación, Crear función.
3. Elija Otro tipo de Cuenta de AWS rol.
4. En el campo ID de AWS cuenta, introduce el ID de cuenta al que deseas conceder acceso a tus recursos.

   El administrador de la cuenta especificada puede conceder permiso para asumir este rol a cualquier usuario de IAM en esa cuenta. Para ello, el administrador adjunta una política al usuario, o grupo, que concede el permiso para la AssumeRole acción sts:. Esa política debe especificar el nombre de recurso de Amazon (ARN) del rol como recurso. Tenga en cuenta lo siguiente:

   - Si vas a conceder permisos a los usuarios desde una cuenta que no controlas y los usuarios asumirán esta función mediante programación, selecciona Requerir un ID externo. El ID externo puede ser cualquier palabra o número acordados entre usted y el administrador de la cuenta de terceros. Esta opción añade automáticamente una condición a la política de confianza que permite al usuario asumir el rol solo si la solicitud incluye el STS:ExternalID correcto. Para obtener más información, consulte Cómo utilizar un identificador externo al conceder acceso a sus AWS recursos a un tercero.
   - Si desea restringir la función a los usuarios que inician sesión con autenticación multifactor (MFA), elija Requerir MFA. De esta forma se agrega una condición a la política de confianza del rol que comprueba si se produce un inicio de sesión con MFA. Un usuario que desee asumir

el rol debe iniciar sesión con una contraseña temporal de uso único desde un dispositivo MFA configurado. Los usuarios sin autenticación MFA no pueden asumir la función. Para obtener más información acerca de la MFA, consulte Uso de la autenticación multifactor (MFA) en. AWS

5. Elija Siguiente: permisos.

   IAM incluye una lista de políticas en la cuenta. En Añadir permisos, introduce amspatchmanagedpolicy en el cuadro de filtro y selecciona la casilla de verificación de esta política de permisos. Haga clic en Next (Siguiente).

6. En Detalles del rol, introduzca un nombre para el rol, por ejemplo PatchRole, añada una descripción del rol (recomendado) y añada también etiquetas que le ayuden a identificar este rol. Los nombres de los roles no distinguen entre mayúsculas y minúsculas, pero deben ser únicos dentro del Cuenta de AWS. Cuando haya terminado, haga clic en Crear rol.

> **Note**
>
> Los nombres de los roles no se pueden editar una vez creados.

# Comprenda las notificaciones de parches y los fallos de los parches en AMS Accelerate

> **Important**
>
> A partir del 1 de febrero de 2025, los clientes de AMS dejarán de recibir notificaciones sobre las ventanas de mantenimiento de parches vacías en sus cuentas gestionadas.

## Solicitudes de servicios de parches y notificaciones por correo electrónico

AMS crea una nueva solicitud de servicio cuatro días antes del siguiente período de mantenimiento de parches. Por ejemplo, cuatro días antes de que se ejecute una ventana de mantenimiento de parches denominada App1 PROD, AMS crea una solicitud de servicio denominada Ventana de mantenimiento de parches de abril para App1 Prod para la cuenta [id de cuenta]. Utilice la solicitud de servicio de parches para comunicarse con AMS si necesita realizar ajustes en el parche programado o si desea omitir un parche próximo. Cuando se crea una solicitud de servicio, se envía

un correo electrónico a su dirección de notificación del parche con un enlace a la solicitud de servicio. Recibirá un correo electrónico adicional cada vez que AMS actualice la solicitud de servicio.

> **Note**
>
> AMS crea una nueva solicitud de servicio, incluso si el período de mantenimiento del parche se crea menos de cuatro días antes de la fecha prevista para su ejecución.
> La ventana de mantenimiento de parches debe estar «habilitada» para recibir las notificaciones de solicitud de servicio.

Una hora antes de que comience la aplicación de parches, AMS le notificará mediante la solicitud del servicio de parches. Una vez finalizada la aplicación de parches, AMS actualiza la solicitud de servicio de parches con un enlace a la consola de Patch Manager. Utilice el enlace para ver el cumplimiento de los parches en las instancias a las que se dirige la ventana de mantenimiento de parches.

> **Note**
>
> Los enlaces de la consola de Patch Manager muestran el cumplimiento actual de las instancias. El administrador de parches muestra una instancia como no compatible si se publican nuevos parches entre el momento en que AMS termina de aplicar los parches y el momento en que se accede al enlace.

## Notificaciones de parches a través de eventos CloudWatch

AMS envía CloudWatch eventos tres veces durante el proceso de revisión, incluidos los siguientes:

- Cuatro días antes de que se ejecute el período de mantenimiento del parche.
- Una hora antes de que se ejecute el período de mantenimiento del parche.
- Cuando finalice el período de mantenimiento del parche.

A continuación se muestra el esquema de eventos de notificación avanzada de la ventana de mantenimiento de parches:

```
{
    "version": "0",
```

```
    "id": "37004d81-458d-2cef-fe1c-8afa8af30406",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "145917996532",
    "time": "2021-05-20T02:00:00Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {
        "State": "PREEMPTIVE",
        "StartTime": "2021-05-24T02:00:00.000000",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\"}, {\"instanceId\":
 \"i-0000000aaaaaaaaab\"}]"
    }
}
```

En la siguiente tabla se describe el esquema de eventos de notificación previa de la ventana de mantenimiento de parches:

Detalles de la notificación del parche

| Nombre de la propiedad | Descripción | Valores de muestra |
|---|---|---|
| Estado | El estado del período de mantenimiento de los parches | PREVENTIVO: está previsto que el período de aplicación de parches comience pronto |
| Estado | El estado del período de mantenimiento de los parches | CORRECTO: todas las instancias fueron parcheadas sin errores<br><br>ERROR: no se pudo aplicar el parche al menos a una instancia |
| StartTime | La hora de inicio, en formato ISO, del período de mantenimi | 2021-02-03T 22:14:05.814 308 |

| Nombre de la propiedad | Descripción | Valores de muestra |
| --- | --- | --- |
| | ento de la aplicación de parches | |
| WindowArn | El identificador único de la ventana de mantenimiento de los parches | arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235 |
| Resultados | La lista de instancias a las que apunta la ventana de parches | InstanceId — el ID de instancia de la instancia de destino |

El siguiente es el esquema de eventos de fin de la ventana de mantenimiento de parches:

```
{"version": "0",
    "id": "0f25add5-44a9-0702-d2bc-bd2102affefe",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "123456789012",
    "time": "2021-02-03T22:14:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {"State": "[COMPLETED]",
        "Status": "SUCCESS",
        "StartTime": "2021-02-03T22:12:00.814308",
        "EndTime": "2021-02-03T22:14:05.814309",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "WindowExecutionId": "e32088eb-c05f-4c63-b766-6866e163c818",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\", \"status\":
 \"Success\", \"missing_critical_patch_count\": 0, \"missing_total_patch_count
\": 0} }, {\"instanceId\": \"i-0000000aaaaaaaaab\", \"status\": Success},
 \"missing_critical_patch_count\": 0, \"missing_total_patch_count\": 0}]"
    }
}
```

En la siguiente tabla se describe el esquema de eventos de fin de la ventana de mantenimiento de parches:

Detalles del final de la ventana de parches

| Nombre de la propiedad | Descripción | Valores de muestra |
|---|---|---|
| Estado | El estado del período de mantenimiento de los parches | COMPLETADO: la ventana de aplicación de parches ha finalizado |
| Estado | El estado del período de mantenimiento de los parches | CORRECTO: todas las instancias fueron parcheadas sin errores<br><br>ERROR: no se pudo aplicar el parche al menos a una instancia |
| StartTime | La hora de inicio, en formato ISO, del período de mantenimiento de la aplicación de parches | 2021-02-03T 22:14:05.814 308 |
| EndTime | La hora de finalización, en formato ISO, del período de mantenimiento de los parches | 2021-02-03T 23:14:05.814 308 |
| WindowArn | El identificador único del período de mantenimiento de los parches. | arn:aws:ssm:us-east-1:12345 6789012:maintenance window/mw-00000001235 |
| WindowExecutionId | El identificador de ejecución de la ventana, que se puede ver en la consola de SSM Maintenance Window | e32088eb-c05f-4c63-b766-6866e163c818 |
| Resultados | La lista de instancias a las que se dirigirá la ventana de parches | InstanceId — el ID de instancia objetivo |

| Nombre de la propiedad | Descripción | Valores de muestra |
| --- | --- | --- |
| | | status: el estado del parche de la instancia<br><br>missing_critical_patch_count: el recuento de parches críticos que faltan en la instancia<br><br>missing_total_patch_count: el recuento total de parches que faltan en la instancia |

Puede usar el evento CloudWatch Events para activar una CloudWatch regla que le notifique cuando se envíe un aviso previo sobre el período de mantenimiento de parches. Para ello, configure la CloudWatch regla con la siguiente configuración:

```
{
    "source": [
        "aws.managedservices"
    ],
    "detail-type": [
        "AMS Patch Window Execution State Change"
    ],
    "detail": {
        "State": ["PREEMPTIVE"]
    }
}
```

> **Note**
>
> Las alertas de error de los parches no se crean para las instancias que tienen sistemas operativos no compatibles o que se detienen durante el período de mantenimiento.

## Investigación de errores de parches en AMS

AWS Managed Services (AMS) administra la aplicación de parches e incluye la corrección de errores de los parches. Cuando se produce un error al aplicar los parches, AMS Operations recibe una

alerta e intenta solucionarlo siguiendo las AWS prácticas recomendadas por AMS para solucionar el problema.

<instance-id>Si se produce un error en un parche, AMS crea un SSM OpsItem en la cuenta con el siguiente título: AWS Managed Services — Patch Instance failure, por ejemplo.

A continuación, AMS investiga el. OpsItem Si AMS puede corregir la falla sin su intervención, AMS resuelve la OpsItem. Si su intervención es necesaria, AMS se lo notifica mediante una solicitud de servicio que contiene los resultados de la investigación y las medidas correctivas recomendadas. Si no tomas ninguna medida para resolver el problema, AMS intentará parchear la instancia durante el siguiente período de mantenimiento de parches programado.

> **Note**
>
> Los parches OpsItems no fallan en las instancias que tienen sistemas operativos no compatibles o que se encuentran en estado de parada durante el período de mantenimiento de los parches.

# Optimización de costes con AMS Resource Scheduler

La AWS solución AMS Resource Scheduler le ayuda a reducir sus costes AWS y los de AMS, ya que detiene los recursos que no se utilizan e inicia los recursos cuando se necesita capacidad. Por ejemplo, puede utilizar el programador de recursos de AMS AWS en un entorno de desarrollo para detener automáticamente las instancias fuera del horario laboral todos los días. Si deja todas las instancias ejecutándose a pleno rendimiento, esta solución puede reducir la utilización de las instancias, lo que reduce el costo total en función de los programas que configure.

Utilice el programador de recursos de AWS Managed Services (AMS) para programar el inicio y la parada automáticos de los grupos de Auto Scaling, EC2 las instancias de Amazon y las instancias de Amazon RDS en su cuenta. Esto ayuda a reducir los costos de infraestructura cuando los recursos no están diseñados para funcionar las 24 horas del día, los 7 días de la semana. La solución se basa en AWS Instance Scheduler, pero contiene funciones y personalizaciones adicionales específicas para las necesidades de los clientes de AMS. La personalización incluye soporte para programar grupos de Auto Scaling, supresor de CloudWatch alarmas para alarmas de Elastic Load Balancing, soporte para múltiples ventanas de AWS Systems Manager mantenimiento para Amazon EC2, un estimador de ahorro de costos y soporte operativo de AMS.

El programador de recursos de AMS utiliza períodos y programas. Los períodos definen las horas en que debe ejecutarse el recurso, como la hora de inicio, la hora de finalización y los días del mes. Los programas contienen los períodos definidos, junto con configuraciones adicionales (ventana de mantenimiento del SSM, zona horaria, hibernación, etc.) y especifican cuándo deben ejecutarse los recursos. Puede configurar estos períodos y programas mediante los manuales de automatización proporcionados por AMS. AWS Systems Manager Cada programación debe contener al menos un período que defina las horas en las que debe ejecutarse la instancia. Una programación puede contener más de un período. Cuando se utiliza más de un período en una programación, el programador de instancias aplica la acción de inicio adecuada cuando se cumple al menos una de las reglas del período. Para obtener más información sobre el cronograma y los períodos, consulte Componentes de soluciones de AWS Instance Scheduler.

El programador de recursos de AMS utiliza etiquetas de AWS recursos para asociar una programación a uno o más recursos con el fin de orientarlos a las acciones programadas de inicio y finalización. Los recursos se etiquetan con la clave de etiqueta (por defecto`Schedule`) configurada en el programador con el nombre del programa como valor. Debe configurar la misma clave de etiqueta que la etiqueta de asignación de costos AWS Cost Explorer para que la función de

estimación de costos del Scheduler haga un seguimiento de los ahorros de costos e informe sobre ellos.

El programador de recursos de AMS es una función opcional que puede habilitar por cuenta.

## Uso de recursos con AMS Resource Scheduler

Amazon EC2

- Las EC2 instancias de Amazon que forman parte de un grupo de Auto Scaling no se procesan individualmente y AMS Resource Scheduler las omite, incluso si están etiquetadas.
- Si el volumen raíz de la instancia de destino está cifrado con una clave maestra AWS KMS del cliente (CMK), tendrás que añadir un `kms:CreateGrant` permiso adicional a tu función de IAM del programador de recursos para que el programador pueda iniciar dichas instancias. Este permiso no se agrega a la función de forma predeterminada para mejorar la seguridad. Si necesita este permiso, puede añadirlo actualizando la CloudFormation pila`ams-resource-scheduler`, con una lista de CMK como valor del `UseCMK` parámetro (utilice una o más claves CMK ARNs en el formato en `arn:`*`partition`*`:kms:`*`region`*`:`*`account-id`*`:key/`*`key-id`* lugar de un alias de KMS).
- Si tus EC2 instancias de Amazon están configuradas con un software específico o con licencias de proveedores gestionadas por él AWS License Manager, Resource Scheduler necesita permisos para AWS License Manager esas licencias específicas para poder iniciar la instancia. Puede conceder a Resource Scheduler los permisos necesarios añadiendo la lista de ARN (s) de las licencias a la licencia AWS License Manager del administrador de licencias, EC2 por ejemplo, el parámetro de CloudFormation la pila (). `ams-resource-scheduler`

Amazon EC2 Auto Scaling

- El programador de recursos de AMS inicia o detiene el escalado automático de los grupos de Auto Scaling, no de las instancias individuales del grupo. Es decir, el planificador restaura el tamaño del grupo de Auto Scaling (inicio) o establece el tamaño en 0 (parada).
- Etiquete el grupo de Auto Scaling con la etiqueta especificada y no con las instancias del grupo.
- Durante la parada, el programador de recursos AMS almacena los valores de capacidad mínima, deseada y máxima del grupo Auto Scaling y establece la capacidad mínima y deseada en 0. Durante el inicio, el planificador restaura el tamaño del grupo de Auto Scaling tal como estaba durante la parada. Por lo tanto, las instancias de grupo de Auto Scaling deben usar una

configuración de capacidad adecuada para que la finalización y el relanzamiento de las instancias no afecten a ninguna aplicación que se ejecute en el grupo Auto Scaling.

- Si se modifica el grupo de Auto Scaling (la capacidad mínima o máxima) durante un período de ejecución, el planificador almacena el nuevo tamaño del grupo de Auto Scaling y lo usa para restaurar el grupo al final de una programación de paradas.

Amazon RDS

- El programador puede tomar una instantánea antes de detener las instancias de RDS (no se aplica al clúster de base de datos Aurora). Esta función está activada de forma predeterminada con el parámetro de CloudFormation plantilla AWS Create RDS Instance Snapshot establecido en true. La instantánea se conserva hasta la próxima vez que se detenga la instancia de Amazon RDS y se cree una nueva instantánea.
- El programador puede ser una instancia de start/stop Amazon RDS que forme parte de un clúster o una base de datos Aurora de Amazon RDS o que se encuentre en una configuración de zona de disponibilidad múltiple (Multi-AZ). Sin embargo, compruebe las limitaciones de Amazon RDS cuando el programador no pueda detener la instancia de Amazon RDS, especialmente las instancias Multi-AZ.
- Para programar el inicio o la parada del Clúster de Aurora, utilice el parámetro de plantilla Programar cúmulos de Aurora (el valor predeterminado es true). El clúster de Aurora (no las instancias individuales del clúster) debe etiquetarse con la clave de etiqueta definida durante la configuración inicial y el nombre del programa como valor de etiqueta para programar ese clúster.

> **Note**
>
> El programador de recursos no valida que un recurso esté iniciado o detenido. Hace que la API solicite el servicio correspondiente y continúa. Si la llamada a la API falla, registra el error para su investigación.
> El programador de recursos de AMS no admite AWS Backup la ventana. Si asigna una instancia de RDS AWS Backup habilitada con la programación del Programador de recursos, para que la copia de seguridad funcione según lo previsto, la ventana de copia de seguridad debe estar dentro de la ventana de ejecución de la programación.

# Incorporación del programador de recursos AMS

Su cuenta no se incorpora automáticamente al AMS Resource Scheduler cuando se incorpora al plan de operaciones AMS Accelerate. Sin embargo, como parte de la incorporación de la cuenta al plan operativo AMS Accelerate, o en cualquier momento posterior, puede solicitar a su administrador de prestación de servicios en la nube (CSDM) que incorpore la cuenta al AMS Resource Scheduler. Una vez que su CSDM se incorpora a la cuenta, se aprovisiona automáticamente en su cuenta una CloudFormation pila que contiene los recursos del AMS Resource Scheduler con la configuración predeterminada.

Una vez aprovisionado el programador de recursos de AMS en su cuenta, le recomendamos que revise la configuración predeterminada y, si es necesario, que personalice las configuraciones, como la clave de etiqueta, la zona horaria, los servicios programados, etc., en función de sus preferencias. Para obtener más información sobre las personalizaciones recomendadas, consulte a continuación. Personalización del programador de recursos AMS

# Personalización del programador de recursos AMS

Una vez incorporado, el programador de recursos de AMS se implementa como una CloudFormation pila, con su nombre`ams-resource-scheduler`, en la región de AWS principal de su cuenta de AMS Accelerate. Puede configurar las propiedades del programador de recursos de AMS en función de sus preferencias mediante los parámetros de la CloudFormation pila y realizando una actualización de la pila. Para obtener información sobre la actualización CloudFormation de pilas, consulte Actualización directa de pilas.

Le recomendamos que personalice las siguientes propiedades y deje el resto como predeterminado para obtener una funcionalidad óptima.

- Nombre de etiqueta: el nombre de la etiqueta que utilizará Resource Scheduler para asociar las programaciones de instancias con los recursos. El valor predeterminado es `Schedule`.
- Servicios a programar: lista de servicios separados por comas que Resource Scheduler puede administrar. El valor predeterminado es "`ec2,rds,autoscaling`". Los valores válidos son «ec2", «rds» y «autoscaling».
- Zona horaria predeterminada: especifique la zona horaria predeterminada que utilizará el programador de recursos. El valor predeterminado es `UTC`.

- CMK para volúmenes de EBS cifrados: lista separada por comas de la clave gestionada por el cliente (CMK) de Amazon KMS a la ARNs que se le pueden conceder permisos a Resource Scheduler.
- Licencia de administrador de licencias EC2 , por ejemplo: se pueden conceder permisos a ese programador de recursos ARNs a una lista separada por comas de AWS Licence Manager para ese programador de recursos.

> **Note**
>
> En ocasiones, AMS publica funciones y correcciones para mantener el Programador de recursos de AMS actualizado en su cuenta. Cuando esto ocurre, se conserva cualquier personalización que realice en la pila del Programador de recursos de AMS mediante los parámetros de la pila.
> Recomendamos encarecidamente no realizar ninguna personalización directamente en ninguno de los recursos componentes del AMS Resource Scheduler. Hacerlo afectará a la funcionalidad del Programador de recursos y a la capacidad de AMS de mantenerlo actualizado.

## Uso del programador de recursos AMS

Cómo utilizar los períodos del programador de recursos de AMS en las cuentas de AMS Accelerate.

Utilice el siguiente conjunto de manuales de AWS Systems Manager automatización para administrar el cronograma y el período necesarios en AMS Resource Scheduler.

> **Note**
>
> Estos manuales de automatización de SSM están disponibles en la región de AWS principal de su cuenta.

- `AWSManagedServices-AddOrUpdatePeriod`
- `AWSManagedServices-AddOrUpdateSchedule`
- `AWSManagedServices-DeleteScheduleOrPeriod`
- `AWSManagedServices-DescribeScheduleOrPeriods`

- `AWSManagedServices-EnableOrDisableAMSResourceScheduler`

Además, AMS proporciona una AWS Identity and Access Management función que `ams_resource_scheduler_ssm_automation_role` se AWS Systems Manager requiere y asume para poder utilizar los manuales. La función de IAM se basa en una política integrada de privilegios mínimos que concede los permisos de SSM necesarios para el funcionamiento de los manuales.

Requisitos previos

Realice los siguientes pasos antes de empezar a utilizar el manual de automatización de SSM y el programador de recursos de AMS.

Adjunte la siguiente política a la entidad de IAM correspondiente (usuario, grupo o rol) a la que desee permitir que utilice los manuales de automatización para administrar la programación y el período en el Programador de recursos de AMS. La política no es obligatoria si su entidad de IAM tiene un administrador o un PowerUser permiso en su cuenta.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPassingResourceSchedulerRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/
ams_resource_scheduler_ssm_automation_role",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
            "Sid": "ListAndDescribeAutomationExecutions",
            "Effect": "Allow",
            "Action": [
                "ssm:GetAutomationExecution",
                "ssm:DescribeAutomationStepExecutions"
```

```
            ],
            "Resource": "arn:aws:ssm:*:111122223333:automation-execution/*"
        },
        {
            "Sid": "ListAndDescribeResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:ListDocumentVersions",
                "ssm:DescribeDocument",
                "ssm:ListDocumentMetadataHistory",
                "ssm:DescribeDocumentParameters",
                "ssm:GetDocument",
                "ssm:DescribeDocumentPermission"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdatePeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdateSchedule",
                "arn:aws:ssm:*::document/AWSManagedServices-
DeleteScheduleOrPeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-
DescribeScheduleOrPeriods",
                "arn:aws:ssm:*::document/AWSManagedServices-
EnableOrDisableAMSResourceScheduler"
            ]
        },
        {
            "Sid": "AllowExecutionOfResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdatePeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdateSchedule",
                "arn:aws:ssm:*::document/AWSManagedServices-
DeleteScheduleOrPeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-
DescribeScheduleOrPeriods",
                "arn:aws:ssm:*::document/AWSManagedServices-
EnableOrDisableAMSResourceScheduler",
                "arn:aws:ssm:*:111122223333:automation-execution/*"
            ]
        },
        {
```

```
            "Sid": "AllowListingAllDocuments",
            "Effect": "Allow",
            "Action": "ssm:ListDocuments",
            "Resource": "*"
        },
        {
            "Sid": "AllowListingAllSSMExecutions",
            "Effect": "Allow",
            "Action": "ssm:DescribeAutomationExecutions",
            "Resource": "*"
        },
        {
            "Sid": "AllowListingIAMRolesForStartingExecutionViaConsole",
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        }
    ]
}
```

Puede ejecutar la automatización desde la AWS Systems Manager consola o mediante la AWS CLI. Si usa la AWS CLI, es posible que necesite instalarla y configurarla o las AWS herramientas para PowerShell, si aún no lo ha hecho. Para obtener más información, consulte Instalar o actualizar las herramientas de línea de AWS comandos.

Vea el vídeo de Navish para obtener más información (4:52)

## Trabajar con períodos y cronogramas en AWS Managed Services Resource Scheduler

Puede utilizar el programador de recursos de AMS para añadir, actualizar o eliminar programas o períodos en las cuentas de AMS Accelerate.

### Añadir o actualizar períodos en el Programador de recursos de AMS

Agregue o actualice un período del Programador de recursos en sus cuentas de AMS.

Datos que necesitará:

- Acción: el tipo de operación que se va a realizar. Use «agregar» si desea agregar un período o «actualizar» si desea actualizar un período existente.

- Nombre: el nombre del período. Debe especificar un valor único si va a añadir un período nuevo.
- AutomationAssumeRole: El ARN del rol AWS Identity and Access Management (IAM) que permite al runbook añadir o actualizar el período en tu nombre. Especifique el rol como. `ams_resource_scheduler_ssm_automation_role`
- Descripción (opcional): una descripción significativa del período.
- BeginTime(Opcional): la hora en formato HH:MM en la que desea iniciar los recursos.
- EndTime(Opcional): la hora en formato HH:MM en la que desea detener los recursos.
- Meses (opcional): una lista de meses delimitados por comas o un rango de meses separados por guiones durante los cuales deben ejecutarse los recursos.
- MonthDays(Opcional): una lista delimitada por comas de los días del mes o un intervalo de días separados por guiones durante los que deben ejecutarse los recursos.
- WeekDays(Opcional): una lista delimitada por comas de los días de la semana o un rango de días de la semana durante los que deben ejecutarse los recursos.

Cómo hacerlo:

- Consulta el documento en AWSManagedServices-AddOrUpdatePeriod(puede que tengas que elegir tu región de incorporación).

  Especifique los requisitos en la sección de parámetros de entrada y, a continuación, seleccione Ejecutar. Una vez completada la operación, consulte los resultados en la pestaña Salida.
- AWS CLI:

  Ejecute el siguiente comando para iniciar una automatización. Reemplácelo *`placeholders`* con su propia información.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdatePeriod" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"],
    "Description":["DESCRIPTION"],"BeginTime":["TIME"], "EndTime":["TIME"],
    "Months":["MONTH"],"MonthDays":["DAY"], "WeekDays":["DAY"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

Ejemplo:

En el siguiente ejemplo, se muestra cómo añadir un nuevo período mediante la AWS Systems Manager consola. Hemos asignado al período el nombre del período y lo hemos configurado para que abarque de lunes a viernes de 9:00 a 18:00 horas durante los primeros 15 días de cada mes.

1. Consulta el documento de AWS Systems Manager automatización en AWSManagedServices-AddOrUpdatePeriod(puede que tengas que elegir tu región de inicio).

2. Proporcione valores para los parámetros.

3. Haga clic en Ejecutar y espere a que se complete la automatización.

## Añadir o actualizar programas en el programador de recursos de AMS

Agregue o actualice un cronograma del programador de recursos en las cuentas de AMS Accelerate.

Datos que necesitará:

- Acción: el tipo de operación que se va a realizar. Utilice «añadir» si desea añadir una programación o «actualizar» si quiere actualizar una programación existente.
- Nombre: el nombre de la programación. Debe especificar un valor único si va a añadir una nueva programación.
- AutomationAssumeRole: El ARN del rol AWS Identity and Access Management (IAM) que permite al runbook añadir o actualizar la programación en tu nombre. Especifique el rol. `ams_resource_scheduler_ssm_automation_role`
- Descripción (opcional): una descripción significativa del programa.
- Períodos (opcional): especifique una lista delimitada por comas de los períodos que se van a utilizar con este programa. Cada período debe haberse creado ya.
- RetainRunning(Opcional): especifique «true» para evitar que el Programador de recursos detenga un recurso en ejecución al final de un período de ejecución si el recurso se inició manualmente antes del comienzo del período de ejecución. De forma predeterminada, el Programador de recursos detiene el recurso.
- StopNewInstances(Opcional): especifique «false» para evitar que el Programador de recursos detenga un recurso la primera vez que se etiqueta si se está ejecutando fuera del período de ejecución. De forma predeterminada, el Programador de recursos detiene el recurso.
- SSMMaintenanceVentana (opcional): especifique una lista delimitada por comas de las ventanas de mantenimiento de AWS Systems Manager (SSM) que desee añadir como períodos de

ejecución del programa. También debe especificar la propiedad "UseMaintenanceWindow" como «true».

- TimeZone(Opcional): especifique la zona horaria que desea que utilice Resource Scheduler. De forma predeterminada, el Programador de recursos usa UTC.
- UseMaintenanceWindow(Opcional): especifique «true» si desea que Resource Scheduler considere el período de mantenimiento de Amazon Relational Database Service (RDS) como un período de ejecución de un programa de instancias de Amazon RDS o que añada los períodos de mantenimiento de AWS Systems Manager (SSM) como período de ejecución a un programa de instancias de Amazon EC2.
- UseMetrics(Opcional): especifique «true» para habilitar CloudWatch las métricas a nivel de programación y «false» para inhabilitarlas. CloudWatch Al especificar esta propiedad, se anula la configuración de CloudWatch métricas establecida en el nivel de pila.

Cómo hacerlo:

- Consulta el documento en AWSManagedServices-AddOrUpdateSchedule(puede que tengas que elegir tu región de incorporación).

  Especifique los requisitos en la sección de parámetros de entrada y, a continuación, seleccione Ejecutar. Una vez finalizada la operación, consulte los resultados en la pestaña Salida.
- AWS CLI:

  Ejecute el siguiente comando para iniciar una automatización. Reemplácelo *placeholders* con su propia información.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdateSchedule" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"], "Description":
["DESCRIPTION"],
    "Hibernate":["true or false"],"Enforced":["true or false"],
    "OverrideStatus":["running or stopped"],"Periods":["PERIOD-A, PERIOD-B"],
    "RetainRunning":["true or false"],"StopNewInstances":["true or false"],
    "SSMMaintenanceWindow":["WINDOW-NAME"],"TimeZone":["TIMEZONE"],
    "UseMaintenanceWindow":["true or false"],"UseMetrics":["true or false"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

Ejemplo:

El siguiente ejemplo muestra cómo agregar una programación para el Programador de recursos de AMS. En este ejemplo, se agrega un horario denominado como. CustomSchedule CustomPeriod

1. Consulta el documento de AWS Systems Manager automatización en AWSManagedServices-AddOrUpdateSchedule(puede que tengas que elegir la región en la que estás embarcada).

2. Proporcione valores para los parámetros.

3. Haga clic en Ejecutar y espere a que se complete la automatización.

## Eliminar períodos o programas en el programador de recursos de AMS

Para eliminar los períodos o programas del Resource Scheduler en las cuentas de AMS Accelerate, necesita los siguientes datos:

- ConfigurationType: El tipo de configuración que desea eliminar. Utilice «período» si desea eliminar períodos o «programar» si desea eliminar horarios.
- Nombre: el nombre del programa o período que desea eliminar.
- AutomationAssumeRole: El ARN del rol AWS Identity and Access Management (IAM) que permite que el runbook elimine horarios o períodos en su nombre. Especifique el rol. `ams_resource_scheduler_ssm_automation_role`

Cómo hacerlo:

- Consulta el documento en AWSManagedServices-DeleteScheduleOrPeriod(es posible que tengas que elegir tu región de destino).

  Especifique los requisitos en la sección de parámetros de entrada y, a continuación, seleccione Ejecutar. Una vez completada la operación, consulte los resultados en la pestaña Salida.
- AWS CLI:

  Ejecute el siguiente comando para iniciar una automatización. Reemplácelo *`placeholders`* con su propia información.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DeleteScheduleOrPeriod" --document-version "\$DEFAULT"
```

```
--parameters '{"ConfigurationType":["period" or "schedule"],"Name":["NAME"],
    "AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}' --region ONBOARDED_REGION
```

Ejemplo:

En el siguiente ejemplo, se muestra cómo se puede eliminar un período mediante la AWS Systems Manager consola.

1. Consulta el documento de AWS Systems Manager automatización en AWSManagedServices-DeleteScheduleOrPeriod(puede que tengas que elegir tu región de inicio).

2. Proporcione valores para los parámetros.

3. Haga clic en Ejecutar y espere a que se complete la automatización.

## Describir períodos o programas en el programador de recursos de AMS

Para describir (ver detalles sobre) un período o programa del Resource Scheduler en las cuentas de AMS Accelerate, necesita los siguientes datos:

- ConfigurationType: el tipo de configuración que desea describir. Utilice «períodos» si desea describir todos los períodos o «programas» si quiere describir todos los horarios.
- AutomationAssumeRole: El ARN de la función AWS Identity and Access Management (IAM) que permite que el manual describa los horarios o períodos en su nombre. Especifique el rol. `ams_resource_scheduler_ssm_automation_role`

Cómo hacerlo:

- Consulta el documento en AWSManagedServices-DescribeScheduleOrPeriods(puede que tengas que elegir tu región de incorporación):
  1. Especifique los requisitos en la sección de parámetros de entrada y, a continuación, seleccione Ejecutar.
  2. Una vez completada la operación, consulte los resultados en la pestaña Salida.
- AWS CLI:

1. Ejecute el siguiente comando para iniciar una automatización. Reemplácelo *placeholders* con su propia información.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DescribeScheduleOrPeriods" --document-version "\$DEFAULT"
                --parameters '{"ConfigurationType":["period" or
 "schedule"],"AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}'
                --region ONBOARDED_REGION
```

Ejemplo:

El siguiente ejemplo muestra cómo se puede describir un período con la AWS Systems Manager consola.

1. Consulta el documento de AWS Systems Manager automatización en AWSManagedServices-DescribeScheduleOrPeriods(puede que tengas que elegir tu región de incorporación).

2. Proporcione valores para los parámetros.

3. Haga clic en Ejecutar y espere a que se complete la automatización.

## Recursos de etiquetado para AMS Resource Scheduler

Recursos de etiquetado para AMS Resource Scheduler.

Una vez que añada los programas y períodos al programa de recursos de AMS, tendrá que etiquetar sus recursos con el nombre de la etiqueta del programador de recursos como clave de etiqueta, o el personalizado, y el nombre del programa como valor de etiqueta. Para obtener más información sobre cómo etiquetar los recursos en su cuenta de AMS Accelerate, consulteEtiquetado en AMS Accelerate.

> **Note**
>
> Si se utiliza el etiquetador de recursos para etiquetar los recursos, la clave de etiqueta predeterminada del Programador de recursos debe personalizarse para que tenga el prefijo '`ams:rt:`', ya que todas las etiquetas aplicadas por el etiquetador de recursos

tienen el prefijo clave ". `ams:rt:` De lo contrario, Resource Scheduler no administrará los recursos etiquetados con el etiquetador de recursos. Para obtener más información sobre la personalización de la clave de etiqueta predeterminada del Programador de recursos, consulte. Personalización del programador de recursos AMS

## Estimador de costos en AMS Resource Scheduler

Para hacer un seguimiento del ahorro de costes, el programador de recursos de AMS incluye un componente que calcula cada hora el ahorro de costes estimado para los recursos de Amazon EC2 y Amazon RDS que gestiona el programador. Estos datos de ahorro de costes se publican luego como una CloudWatch métrica (`AMS/ResourceScheduler`) para ayudarle a realizar un seguimiento de los mismos. El estimador de ahorros de costos solo estima los ahorros en las horas de funcionamiento de una instancia. No tiene en cuenta ningún otro coste, como los costes de transferencia de datos asociados a un recurso.

El estimador de ahorro de costes está activado con Resource Scheduler. Funciona cada hora y recupera datos de costos y uso de. AWS Cost Explorer A partir de esos datos, calcula el costo promedio por hora para cada tipo de instancia y, a continuación, proyecta el costo de un día completo si se ejecutó sin programarse. El ahorro de costos es la diferencia entre el costo proyectado y el costo real informado por Cost Explorer para un día determinado.

Por ejemplo, si la instancia A está configurada con el programador de recursos para que se ejecute de 9 a. m. a 5 p. m., son ocho horas de un día determinado. Cost Explorer informa que el costo es de 1 dólar y el uso de 8. Por lo tanto, el costo promedio por hora es de 0,125 USD. Si la instancia no estaba programada con Resource Scheduler, se ejecutaría 24 horas ese día. En ese caso, el costo habría sido de 24 x 0,125 = 3$. Resource Scheduler le ayudó a ahorrar 2 dólares en costos.

Para que el estimador de ahorros de costos recupere el costo y el uso solo de los recursos administrados por Resource Scheduler desde Cost Explorer, la clave de etiqueta que el Programador de recursos utiliza para destinar los recursos debe activarse como etiqueta de asignación de costos en el panel de facturación. Si la cuenta pertenece a una organización, la clave de etiqueta debe estar activada en la cuenta de administración de la organización. Para obtener información sobre cómo hacerlo, consulte Activación de etiquetas de asignación de costes definidas por el usuario y etiquetas de asignación de costes definidas por el usuario

Una vez que la clave de etiqueta se activa como etiqueta de asignación de costos, la facturación de AWS comienza a rastrear el costo y el uso de los recursos administrados por Resource Scheduler y,

una vez que los datos estén disponibles, la calculadora de ahorros de costos comienza a calcular los ahorros de costos y a publicar los datos en el espacio de nombres de la `AMS/ResourceScheduler` métrica en. CloudWatch

Si la etiqueta de asignación de costos no está activada, el estimador no podrá calcular los ahorros ni publicar la métrica, aunque esté habilitada.

> **Note**
>
> Cost Savings Estimator no acepta descuentos como instancias reservadas, planes de ahorro, etc., para su cálculo. El estimador toma los costos de uso de Cost Explorer y calcula el costo promedio por hora de los recursos. Para obtener más información, consulte Cómo entender sus conjuntos de datos de AWS costos: una hoja de referencia.

## Supresor de alarmas en el programador de recursos AMS

El AMS Resource Scheduler incluye un supresor de CloudWatch alarmas, que se implementa como una función de Lambda independiente denominada `AMSAlarmSuppressor` que suprime las alarmas de las instancias que se encuentran detrás de un Elastic Load Balancing, Application Load Balancer o Network Load Balancer. La función se ejecuta cada 5 minutos, recupera todas las alarmas presentes en la cuenta y las agrupa según el espacio de nombres; por ejemplo,,,. `AWS/ELB` `AWS/ApplicationELB` `AWS/NetworkELB` Para cada grupo de alarmas, el supresor busca el nombre del balanceador de cargas, el grupo objetivo (para ALB/NLB) from alarm dimensions, finds the instances that are registered with the load balancer and/or el grupo and/or objetivo) y comprueba el estado de la instancia para descubrir si las instancias están programadas por AMS Resource Scheduler. Si Resource Scheduler programa las instancias y Resource Scheduler las detiene, el supresor marca las alarmas para inhabilitarlas. Si se está ejecutando al menos una instancia de la lista de instancias registradas, el supresor marca las alarmas correspondientes para activar las que están marcadas como activadas y deshabilita las que están marcadas como inhabilitadas. Los registros correspondientes se almacenan en el `/aws/lambda/AMSAlarmSuppressor` grupo de registros.

# Administración de registros en AMS Accelerate

AMS Accelerate configura los AWS servicios compatibles para recopilar registros. AMS Accelerate utiliza estos registros para garantizar el cumplimiento y la auditoría de los recursos de su cuenta.

AMS Accelerate ofrece una gama de servicios operativos para ayudarlo a alcanzar la excelencia operativa en AWS. Para comprender rápidamente cómo AMS ayuda a sus equipos a lograr la excelencia operativa general en la nube de AWS con algunas de nuestras capacidades operativas clave, como el servicio de asistencia las 24 horas, los 7 días de la semana, la supervisión proactiva, la seguridad, la aplicación de parches, el registro y la copia de seguridad, consulte los diagramas de arquitectura de referencia de AMS.

Temas


- Administración de registros: AWS CloudTrail
- Administración de registros — Amazon EC2
- Administración de registros: Amazon VPC Flow Logs


## Administración de registros: AWS CloudTrail

AWS CloudTrailes un servicio que se utiliza para el control de cuentas: cumplimiento, auditoría operativa y auditoría de riesgos. Con CloudTrail él, puede registrar, supervisar de forma continua y conservar la actividad de la cuenta relacionada con las acciones en toda su AWS infraestructura.

AMS Accelerate requiere el AWS CloudTrail registro para gestionar las auditorías y el cumplimiento de todos los recursos de su cuenta. Durante la incorporación, puede elegir una de las siguientes opciones:

- Ruta desplegada por AMS: si eliges esta opción, AMS crea, despliega y gestiona una ruta CloudTrail multirregional en tu AWS región principal, independientemente de las rutas existentes en tu cuenta.
- Crea tu propia ruta: si decides proporcionar tu propia cuenta u organización CloudTrail, tendrás que trabajar con tu Cloud Architect (CA) para asegurarte de que cumple con las configuraciones requeridas para Accelerate. Si elige esta opción pero no proporciona su propio registro, Accelerate implementará automáticamente su propio CloudTrail registro para mantener una cobertura continua de seguridad y auditoría. Si proporciona su propio registro más adelante, AMS eliminará el registro desplegado para evitar redundancias y costes adicionales. Este enfoque ayuda a

mantener un único registro activo en CloudTrail su cuenta y evita la duplicación de los costes de registro.

> **Note**
>
> Si su cuenta tiene un CloudTrail registro existente y no configuró ni solicitó específicamente un registro gestionado por AMS durante la incorporación, AMS Accelerate eliminará automáticamente el registro implementado por AMS de su cuenta. Esto evita la duplicación de registros, optimiza el uso de los recursos y ahorra costes adicionales.

AMS Accelerate crea un bucket de Amazon S3 para una CloudTrail ruta implementada por Accelerate como destino de entrega de eventos y utiliza el cifrado AWS Key Management Service (AWS KMS). Los operadores de AMS Accelerate acceden a los eventos de su ruta con fines de investigación y diagnóstico. Si la cuenta ya tiene habilitada una CloudTrail ruta existente, esta ruta se suma a la que usted eligió para que Accelerate desplegara una ruta gestionada por Accelerate durante la incorporación.

AMS Accelerate implementa AWS Config reglas para garantizar que los registros de su CloudTrail cuenta, incluido el CloudTrail registro implementado por Accelerate, estén configurados y cifrados correctamente. Para obtener más información, consulte AWS Config. Estas son las reglas utilizadas, presentadas como enlaces a la AWS documentación que las describe:

- multi-region-cloudtrail-enabled. Comprueba que AMS Accelerate CloudTrail esté correctamente configurado con las configuraciones correctas.
- cloud-trail-encryption-enabled. Comprueba si AWS CloudTrail está configurado para utilizar el cifrado del lado del servidor (SSE) con el cifrado de clave maestra AWS KMS del cliente (CMK).
- cloud-trail-log-file-habilitado para la validación. Cuando está habilitada, comprueba que se AWS CloudTrail cree un archivo de resumen firmado con registros. Le recomendamos encarecidamente que habilite la validación de archivos en todos los senderos.
- s3- bucket-default-lock-enabled. Cuando está habilitada, comprueba que el bucket de Amazon S3 tenga el bloqueo activado.
- s3- bucket-logging-enabled. Cuando está habilitada, comprueba si el registro está habilitado para los buckets de Amazon S3.

AMS Accelerate AWS KMS se utiliza para cifrar los eventos registrados para una CloudTrail ruta implementada por Accelerate en su cuenta. Los administradores de la cuenta, los operadores de AMS Accelerate y los operadores de AMS Accelerate y CloudTrail pueden acceder a esta clave. Para obtener más información sobre las AWS Key Management Service funciones AWS KMS, consulte la documentación del producto.

## Acceder a los CloudTrail registros y auditarlos

CloudTrail los registros de una CloudTrail ruta implementada por AMS Accelerate se almacenan en un bucket de Amazon S3 dentro de su cuenta. Los datos de seguimiento almacenados en el bucket de Amazon S3 se cifran mediante una clave de AWS KMS que se crea cuando se aprovisionan CloudTrail los recursos.

Los buckets de Amazon S3 utilizan un patrón de nomenclatura de ams-a ***aws account id*** -cloudtrail- (ejemplo: ams-a123456789- ***AWS Region*** cloudtrail-us-east -1a) y todos los eventos se almacenan con el prefijo AWS/. CloudTrail Todos los accesos al depósito principal se registran y los objetos de registro se cifran y se les asigna una versión con fines de auditoría.

Para obtener más información sobre el seguimiento de los cambios y la consulta de los registros, consulte. Seguimiento de los cambios en sus cuentas de AMS Accelerate

## Protección y conservación de los registros CloudTrail

AMS Accelerate permite el bloqueo de objetos de Amazon S3 con el modo Governance para un CloudTrail seguimiento implementado de Accelerate a fin de garantizar que los usuarios no puedan sobrescribir o eliminar una versión de un objeto ni modificar su configuración de bloqueo sin permisos especiales. Para obtener más información, consulte Bloqueo de objetos en Amazon S3.

De forma predeterminada, todos los registros de este depósito se guardan indefinidamente. Si desea cambiar el período de retención, puede enviar una solicitud de servicio a través del AWS Support Centro para configurar una política de retención diferente.

## Acceso a los registros de Amazon EC2

Puede acceder a los registros de instancias de Amazon EC2 mediante. Consola de administración de AWS Los registros generados por las instancias y AWS los servicios están disponibles en CloudWatch Logs, que está disponible en cada cuenta gestionada por AMS Accelerate. Para obtener información sobre cómo acceder a sus registros, consulte la documentación de CloudWatch registros.

## Conservación de los registros de Amazon EC2

De forma predeterminada, los registros de instancias de Amazon EC2 se guardan indefinidamente. Si desea cambiar el período de retención, puede enviar una solicitud de servicio a través del AWS Support Centro para configurar una política de retención diferente.

# Administración de registros — Amazon EC2

AMS Accelerate instala el CloudWatch agente en todas las instancias de Amazon EC2 que haya identificado como administradas por AMS Accelerate. Este agente envía registros de nivel de sistema a Amazon CloudWatch Logs. Para obtener más información, consulta ¿Qué son Amazon CloudWatch Logs?

Los siguientes archivos de registro se envían a CloudWatch Logs, a un grupo de registros con el mismo nombre que el registro. Dentro de cada grupo de registros, se crea un flujo de registros para cada instancia de Amazon EC2, cuyo nombre se denomina de acuerdo con el ID de la instancia de Amazon EC2.

Linux

- /-ssm-agent.log var/log/amazon/ssm/amazon
- /var/log/amazon/ssm/errors.log
- /.log var/log/audit/audit
- /.log var/log/auth
- /-init-output.log var/log/cloud
- /var/log/cron
- /var/log/dnf.log
- /.log var/log/dpkg
- /var/log/maillog
- /var/log/messages
- /var/log/secure
- /var/log/spooler
- /var/log/syslog
- /.log var/log/yum

- /.log var/log/zypper

Para obtener más información, consulte Crear o editar manualmente el archivo de configuración del CloudWatch agente.

Windows

- Amazon SSMAgent Log
- AmazonCloudWatchAgentLog
- Amazon SSMError Log
- AmazonCloudFormationLog
- ApplicationEventLog
- EC2ConfigServiceEventLog
- MicrosoftWindowsAppLockerEXEAndDLLEventRegistro
- MicrosoftWindowsAppLockerMSIAndScriptEventLog
- MicrosoftWindowsGroupPolicyOperationalEventLog
- SecurityEventLog
- SystemEventLog

Para obtener más información, consulte Inicio rápido: habilite sus instancias de Amazon EC2 que ejecutan Windows Server 2016 para enviar registros a CloudWatch registros mediante el agente de CloudWatch registros.

## Administración de registros: Amazon VPC Flow Logs

Los registros de flujo de la VPC son una función que captura información sobre el tráfico IP que entra y sale de las interfaces de red de la VPC. Los datos del registro de flujo se pueden publicar en Amazon CloudWatch Logs o Amazon S3. La recopilación de datos del registro de flujo no afecta al rendimiento ni a la latencia de la red. Puede crear o eliminar registros de flujo sin que ello afecte al rendimiento de la red.

Los logs de flujo pueden ayudarlo en una serie de tareas, tales como:

- Diagnosticar reglas de grupos de seguridad demasiado restrictivas
- Supervisar el tráfico que llega a su instancia

- Determinar la dirección del tráfico hacia y desde las interfaces de red

No tiene que habilitar los registros de flujo de VPC para cada VPC recién creada en las cuentas de Accelerate. AMS detectará automáticamente si una VPC tiene un registro de flujo mediante la regla - ams-nist-cis-vpcflow-logs-enabledConfig. Si los registros de flujo de VPC no están habilitados, AMS lo solucionará automáticamente mediante la creación de un registro de flujo de VPC con campos personalizados. Contar con estos campos adicionales permitirá a AMS y a los clientes monitorear mejor el tráfico de VPC, comprender las dependencias de la red, solucionar problemas de conectividad de la red e identificar las amenazas de la red.

Para obtener información sobre cómo ver y buscar registros de flujo, consulte Trabajar con registros de flujo.

# Seguimiento de los cambios en sus cuentas de AMS Accelerate

**Important**

El servicio Change Record dejará de estar disponible a partir del 1 de julio de 2025.
No se pueden incorporar cuentas nuevas al servicio Change Record.
Para consultar CloudTrail los datos de sus cuentas de AMS Accelerate, puede utilizar estos servicios:

- En AWS CloudTrail, elija Historial de eventos y filtre los eventos mediante los atributos de búsqueda. Puede usar el filtro de rango de tiempo y elegir filtrar el historial de eventos por fuente de eventos según lo `s3.amazon.aws.com` especificado, o filtrar el historial de eventos por nombre de usuario. Para obtener más información, consulta Cómo trabajar con el historial de CloudTrail eventos.
- Use AWS CloudTrail Lake para recopilar datos a través de consultas. En, AWS CloudTrail elija Lake y, a continuación, elija Query. Puede crear sus propias consultas, utilizar el generador de consultas o utilizar consultas de ejemplo para recopilar datos basados en eventos. Por ejemplo, puedes preguntar quién eliminó una EC2 instancia de Amazon la semana pasada. Para obtener más información, consulta Cómo crear un lago de datos a partir de una AWS CloudTrail fuente y CloudTrailLake consultas.
- Crea una tabla de Amazon Athena AWS CloudTrail y establece la ubicación de almacenamiento como el depósito de Amazon S3 asociado a tu ruta. Comprueba que la región de origen de tu ruta y la del bucket de Amazon S3 sean las mismas. En Amazon Athena, utilice el editor de consultas para ejecutar las consultas predeterminadas que Accelerate proporciona para su uso con la consola de Athena. Para obtener más información sobre cómo crear una tabla de Athena para consultar los CloudTrail registros, consulte Registros de consultas AWS CloudTrail.

Temas


- Ver tus registros de cambios
- Consultas predeterminadas
- Cambiar los permisos de registro

AWS Managed Services le ayuda a realizar un seguimiento de los cambios realizados por el equipo de AMS Accelerate Operations y la automatización de AMS Accelerate al proporcionar una interfaz consultable mediante la consola Amazon Athena (Athena) y la administración de registros de AMS Accelerate.

Athena es un servicio de consultas interactivo que puede utilizar para analizar datos en Amazon S3 mediante el lenguaje de consulta estructurado (SQL) estándar (consulte Referencia de SQL para Amazon Athena). Athena no requiere un servidor, por lo que no hay una infraestructura para administrar y solo pagará por las consultas que ejecute. AMS Accelerate crea tablas de Athena con particiones diarias sobre CloudTrail registros y proporciona consultas en su AWS región principal y dentro del ams-change-recordgrupo de trabajo. Puede elegir cualquiera de las consultas predeterminadas y ejecutarlas según sea necesario. Para obtener más información sobre los grupos de trabajo de Athena, consulte Cómo funcionan los grupos de trabajo.

> **Note**
>
> Solo Accelerate puede consultar CloudTrail los eventos de su cuenta de Accelerate mediante Athena cuando Accelerate está integrado en el registro de su CloudTrail organización, a menos que el administrador de su organización haya implementado un rol de IAM para usar Athena para consultar y analizar CloudTrail los eventos de su cuenta durante la incorporación.

Con el registro de cambios, puede responder fácilmente a preguntas como las siguientes:

- ¿Quién (AMS Accelerate Systems o AMS Accelerate Operators) ha accedido a su cuenta
- ¿Qué cambios ha realizado AMS Accelerate en su cuenta
- ¿Cuándo realizó AMS Accelerate cambios en su cuenta
- ¿Dónde ir para ver los cambios realizados en su cuenta
- ¿Por qué AMS Accelerate necesitaba realizar los cambios en su cuenta
- ¿Cómo modificar las consultas para obtener respuestas a todas esas preguntas también en el caso de cambios que no sean de AMS

## Ver tus registros de cambios

Para usar las consultas de Athena, inicia sesión en la consola de AWS administración y navega hasta la consola de Athena en tu región principal. AWS

> **Note**
>
> Si ve la página Primeros pasos de Amazon Athena mientras realiza alguno de los pasos, haga clic en Comenzar. Es posible que esto le aparezca incluso si su infraestructura de registro de cambios ya está instalada.

1. Seleccione Grupo de trabajo en el panel de navegación superior de la consola de Athena.
2. Elija el ams-change-recordgrupo de trabajo y, a continuación, haga clic en Cambiar grupo de trabajo.
3. Elija una opción ams-change-record-databasedel cuadro combinado de base de datos. ams-change-record-databaseIncluye la ams-change-record-tabletabla.
4. Seleccione Consultas guardadas en el panel de navegación superior.
5. La ventana Consultas guardadas muestra una lista de consultas que proporciona AMS Accelerate y que puede ejecutar. Elija la consulta que desee ejecutar en la lista de consultas guardadas. Por ejemplo, la consulta ams_session_accesses_v1.

   Para ver la lista completa de consultas predefinidas de AMS Accelerate, consulte. Consultas predeterminadas
6. Ajuste el filtro de fecha y hora en el cuadro del editor de consultas según sea necesario; de forma predeterminada, la consulta solo comprueba los cambios del último día.
7. Elija Ejecutar consulta.

## Consultas predeterminadas

AMS Accelerate proporciona varias consultas predeterminadas que puede utilizar en la consola de Athena. Las consultas predeterminadas se muestran en las siguientes tablas.

> **Note**
>
> - Todas las consultas aceptan el intervalo de fecha y hora como filtro opcional; de forma predeterminada, todas las consultas se ejecutan durante las últimas 24 horas. Para conocer los datos esperados, consulte la siguiente subsección,. Modificación del filtro de fecha y hora en las consultas

- Las entradas de parámetros que puede o necesita cambiar se muestran en la consulta como ocurre *<PARAMETER_NAME>* con las llaves angulares. Sustituya el marcador de posición y las llaves angulares por el valor del parámetro.
- Todos los filtros son opcionales. En las consultas, algunos filtros opcionales se comentan con un doble guión (--) al principio de la línea. Todas las consultas se ejecutarán sin ellos, con los parámetros predeterminados. Si desea especificar los valores de los parámetros para estos filtros opcionales, elimine el doble guión (--) situado al principio de la línea y sustituya el parámetro como desee.
- Todas las consultas retornan `IAM PincipalId` y `IAM SessionId` aparecen en los resultados
- El coste calculado de ejecutar una consulta depende del número de CloudTrail registros que se generen para la cuenta. Para calcular el costo, utilice la calculadora de precios de AWS Athena.

Consultas predefinidas

| Propósito/descripción | Entradas | Salidas |
|---|---|---|
| Nombre de la consulta: `ams_access_session_query_v1` | | |
| Seguimiento de las sesiones de acceso a AMS Accelerate<br><br>Proporciona información sobre una sesión de acceso específica a AMS Accelerate. La consulta acepta el ID principal de IAM como filtro opcional y devuelve la hora del evento, la necesidad empresarial de acceder a la cuenta, el solicitante, etc. | (Opcional)`IAM PrincipalId` : el identificador principal de IAM del recurso al que se intenta acceder. El formato es*UNIQUE_ID ENTIFIER* :*RESOURCE_NAME* . Para obtener más información, consulte identificadores únicos. Puede ejecutar la consulta sin este filtro para determinar el IAM exacto con PrincipalId el que desea filtrar. | • EventTime: Hora de obtener el acceso<br>• EventName: nombre del evento de AWS (AssumeRole)<br>• EventRegion: Región de AWS que recibe la solicitud<br>• EventId: ID CloudTrail del evento<br>• BusinessNeed Tipo: tipo de motivo comercial para acceder a la cuenta. Los valores permitidos son: SupportCase OpsItem, Issue, Text.<br>• BusinessNeed: Las empresas deben acceder a la cuenta. Por ejemplo, Support Case ID, Ops Item ID, etc. |

| Propósito/descripción | Entradas | Salidas |
| --- | --- | --- |
| Puede filtrar por un ID principal de IAM específico o quitando el comentario de la línea y sustituyendo el marcador de posición por un ID específico en el *IAM PrincipalId* editor de consultas.<br><br>También puede enumerar las sesiones de acceso que no sean de AMS quitando la línea de filtro useragent de la cláusula WHERE de la consulta. | | • Solicitante: ID de operador que accede a la cuenta o sistema de automatización que accede a la cuenta.<br>• RequestAccessType: Tipo de solicitante (System, OpsAPI OpsConsole, Unset) |
| Nombre de la consulta: ams_events_query_v1 | | |

| Propósito/descripción | Entradas | Salidas |
| --- | --- | --- |
| Realice un seguimiento de todas las acciones de mutación realizadas por AMS Accelerate<br><br>Devuelve todas las acciones de escritura realizadas en la cuenta utilizando ese filtro de roles de AMS Accelerate.<br><br>También puede realizar un seguimiento de las acciones de mutación realizadas por roles ajenos a AMS quitando las líneas del filtro useridentity.arn de la cláusula WHERE de la consulta. | (Opcional)<br><br>Solo rango de fecha y hora. Consulte Modificación del filtro de fecha y hora en las consultas. | • AccountId: ID de cuenta de AWS<br>• RoleArn: RoleArn para el solicitante<br>• EventTime: Hora de obtener el acceso<br>• EventName: nombre del evento de AWS (AssumeRole)<br>• EventRegion: Región de AWS que recibe la solicitud<br>• EventId: ID CloudTrail del evento<br>• RequestParameters : Parámetros de solicitud para la solicitud<br>• ResponseElements: Elementos de respuesta para la respuesta.<br>• UserAgent: Agente de CloudTrail usuario de AWS |
| Nombre de la consulta: `ams_instance_access_sessions_query_v1` | | |

| Propósito/descripción | Entradas | Salidas |
| --- | --- | --- |
| Realice un seguimiento de los accesos a las instancias mediante AMS Accelerate<br><br>Devuelve una lista de los accesos a las instancias de AMS Accelerate; cada registro incluye la hora del evento, la región del evento, el ID de instancia, el ID principal de IAM, el ID de sesión de IAM y el ID de sesión de SSM. Puede usar el ID principal de IAM para obtener más detalles sobre la necesidad empresarial de acceder a la instancia mediante la consulta `ams_access_sessions_query_v1` Athena. Puede usar el ID de sesión SSM para obtener más detalles sobre la sesión de acceso a la instancia, incluida la hora de inicio y finalización de la sesión, los detalles del registro y el uso de la consola del administrador de AWS sesiones en la región de la instancia. AWS | Solo `datetime range`. Consulte Modificación del filtro de fecha y hora en las consultas. | • InstanceId: ID de instancia<br>• SSMSession ID: ID de sesión de SSM<br>• RoleArn: RoleArn para el solicitante<br>• EventTime: Hora de obtener el acceso<br>• EventName: nombre del evento de AWS (AssumeRole)<br>• EventRegion: Región de AWS que recibe la solicitud<br>• EventId: ID CloudTrail del evento |

| Propósito/descripción | Entradas | Salidas |
| --- | --- | --- |
| Los usuarios también pueden enumerar los accesos a instancias ajenas a AMS quitando la línea del filtro de identidad de usuario de la cláusula WHERE de la consulta. | | |
| Nombre de la consulta: ams_privilege_escalation_events_query_v1 | | |

| Propósito/descripción | Entradas | Salidas |
| --- | --- | --- |
| Realice un seguimiento de los eventos de permisos (escalamiento) para usuarios de AMS y no usuarios de AMS<br><br>Proporciona una lista de eventos que pueden conducir directa o potencialmente a una escalada de privilegios. La consulta se acepta ActionedBy como filtro opcional y devuelve EventName EventId, EventTime, y así sucesivamente. También se devuelven todos los campos asociados al evento. Los campos están en blanco si no son aplicables a ese evento. El ActionedBy filtro está desactivado de forma predeterminada; para activarlo, elimine «--" de esa línea.<br><br>De forma predeterminada, el ActionedBy filtro está deshabilitado (mostrará los eventos de escalamiento de privilegios de todos los usuarios). Para mostrar | (Opcional)`ACTIONEDBY_PUT_USER_NAME` : nombre de usuario del usuario ActionedBy. Puede ser un rol o un usuario de IAM. Por ejemplo,. ams-access-admin<br><br>(Opcional)`datetime range`. Consulte Modificación del filtro de fecha y hora en las consultas. | • AccountId: ID de cuenta<br>• ActionedByNombre de usuario ActionedBy :<br>• EventTime: Hora de obtener el acceso<br>• EventName: Nombre del evento de AWS (AssumeRole).<br>• EventRegion: Región de AWS que recibe la solicitud<br>• EventId: ID CloudTrail del evento |

| Propósito/descripción | Entradas | Salidas |
| --- | --- | --- |
| los eventos de un usuario o rol en particular, elimine el doble guión (--) de la línea del filtro de identidad de usuario de la cláusula WHERE y sustituya el marcador *ACTIONEDBY_PUT_USER_NAME_HERE* de posición por el nombre de un usuario o rol de IAM. Puede ejecutar la consulta sin el filtro para determinar el usuario exacto con el que desea filtrar. | | |
| Nombre de la consulta: ams_resource_events_query_v1 | | |

| Propósito/descripción | Entradas | Salidas |
| --- | --- | --- |
| Realice un seguimiento de los eventos de escritura para recursos específicos (AMS o no AMS)<br><br>Proporciona una lista de los eventos realizados en un recurso específico. La consulta acepta el identificador del recurso como parte de los filtros (reemplaza el marcador de posición *RESOURCE_INFO* en la cláusula WHERE de la consulta) y devuelve todas las acciones de escritura realizadas en ese recurso. | (Obligatorio)`RESOURCE_INFO` : el identificador del recurso puede ser un ID de cualquier recurso de AWS de la cuenta. No hay que confundir esto con un recurso ARNs. Por ejemplo, un ID de instancia para una EC2 instancia, un nombre de tabla para una tabla de DynamoDB logGroupName , para CloudWatch un registro, etc.<br><br>(Opcional). `datetime range` Consulte Modificación del filtro de fecha y hora en las consultas. | • AccountId: ID de cuenta<br>• ActionedByNombre de usuario ActionedBy :<br>• EventTime: Hora de obtener el acceso<br>• EventName: Nombre del evento de AWS (AssumeRole).<br>• EventRegion: Región de AWS que recibe la solicitud<br>• EventId: ID CloudTrail del evento |
| Nombre de la consulta: `ams_session_events_query_v1` | | |

| Propósito/descripción | Entradas | Salidas |
| --- | --- | --- |
| Realice un seguimiento de las acciones de escritura realizadas por AMS Accelerate durante una sesión específica<br><br>Proporciona una lista de los eventos realizados en una sesión específica. La consulta acepta el ID principal de IAM como parte de los filtros (sustituya el marcador *PRINCIPAL_ID* de posición de la cláusula WHERE de la consulta) y devuelve todas las acciones de escritura realizadas en ese recurso. | (Obligatorio)`PRINCIPAL_ID` : ID principal de la sesión. El formato es*UNIQUE_ID ENTIFIER* :*RESOURCE_NAME* . Para obtener más información, consulte identificadores únicos. Puede ejecutar la consulta «ams_session_ids_by_requester_v1" para obtener la lista del principal de IAM de un solicitante. IDs También puede ejecutar la consulta sin este filtro para determinar el IAM exacto con el que desea filtrar. PrincipalId<br><br>(Opcional). `datetime range` Consulte Modificación del filtro de fecha y hora en las consultas. | • AccountId: ID de cuenta<br>• ActionedByNombre de usuario ActionedBy :<br>• EventTime: Hora de obtener el acceso<br>• EventName: nombre del evento de AWS (AssumeRole)<br>• EventRegion: Región de AWS que recibe la solicitud<br>• EventId: ID CloudTrail del evento |
| Nombre de la consulta: `ams_session_ids_by_requester_v1` | | |

| Propósito/descripción | Entradas | Salidas |
| --- | --- | --- |
| Realice un seguimiento del IAM Principal/Session IDs de un solicitante específico.<br><br>La consulta acepta la palabra «solicitante» (sustituya el marcador *Requester* de posición de la cláusula WHERE de la consulta) y devuelve todos los identificadores principales de IAM de ese solicitante durante el intervalo de tiempo especificado. | (Obligatorio)`Requester` : ID de operador que accede a la cuenta (por ejemplo: alias de un operador) o sistema de automatización que accede a la cuenta (por ejemplo: OsConfiguration,, AlarmManager etc.).<br><br>(Opcional). `datetime range` Consulte Modificación del filtro de fecha y hora en las consultas. | • IAM PrincipalId : ID principal de IAM de la sesión. El formato es*UNIQUE_IDENTIFIER* :. *RESOURCE_NAME* Para obtener más información, consulte identificadores únicos. Puede ejecutar la consulta sin este filtro para determinar el IAM exacto con el PrincipalId que desea filtrar.<br>• IAM SessionId : ID de sesión de IAM para la sesión de acceso<br>• EventTime: Hora de obtener el acceso |

## Modificación del filtro de fecha y hora en las consultas

Todas las consultas aceptan el rango de fecha y hora como filtro opcional. De forma predeterminada, todas las consultas se ejecutan durante el último día.

El formato utilizado para el campo de fecha y hora es yyyy/MM/dd (por ejemplo: 01/01/2021). Recuerde que solo almacena la fecha y no la marca de tiempo completa. Para toda la marca de tiempo, utilice el campo eventime, que almacena la marca de tiempo en el formato ISO 8601 yyyy-MM-dd T HH:mm:ss Z (por ejemplo: 2021-01-01T 23:59:59 Z). Sin embargo, dado que la tabla está dividida en el campo de fecha y hora, tendrás que pasar los filtros de fecha y hora a la consulta. Vea los siguientes ejemplos de .

> **Note**
>
> Para ver todas las formas aceptadas de modificar el rango, consulte la documentación más reciente de la función Presto, basada en la versión del motor Athena que se utiliza

actualmente para las funciones y operadores de fecha y hora, para ver todas las formas aceptadas de modificar el rango.

Nivel de fecha: último día o últimas 24 horas (predeterminado) Ejemplo: si CURRENT_DATE='2021/01/01', el filtro restará un día de la fecha actual y le dará el formato de datetime > '2020/12/31'

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
```

Nivel de fecha: ejemplo de los últimos 2 meses:

```
datetime > date_format(date_add('month', - 2, CURRENT_DATE), '%Y/%m/%d')
```

Nivel de fecha: ejemplo entre 2 fechas:

```
datetime > '2021/01/01'
      AND
      datetime < '2021/01/10'
```

Nivel de marca horaria: ejemplo de las últimas 12 horas:

Particione los datos escaneados para que duren 1 día y, a continuación, filtre todos los eventos de las últimas 12 horas

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND
      eventtime > date_format(date_add('hour', - 12, CURRENT_TIMESTAMP), '%Y-%m-%dT%H:
%i:%sZ')
```

Nivel de marca de tiempo: ejemplo de entre 2 marcas de tiempo:

Obtenga eventos entre el 1 de enero de 2021 a las 12:00 p. m. y el 10 de enero de 2021 a las 3:00 p. m.

```
datetime > '2021/01/01' AND datetime < '2021/01/10'
      AND
      eventtime > '2021-01-01T12:00:00Z' AND eventtime < '2021-01-10T15:00:00Z'
```

# Ejemplos de consultas por defecto

### ams_access_session_query_v1

```
Name: ams_access_session_query_v1

Description: >-
   The query provides more information on specific AMS access session.
   The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.
   By default; the query filter last day events only, the user can change the datetime
 filter to search for more wide time range.
   By default; the IAM PrincipalId filter is disabled. To enable it, remove "-- " from
 that line.

AthenaQueryString: |-
   /*
     The query provides list of AMS access sessions during specific time range.
     The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     By default; the IAM Principal ID filter is disabled (it shows access sessions for
 all IAM principals).
     If you want to only show access sessions for a particular IAM principal ID, remove
 the double-dash (--) from
     the "IAM Principal ID" filter line in the WHERE clause of the query, and replace
 the placeholder "<IAM PrincipalId>" with the specific ID that you want.
     You can run the query without the filter to determine the exact IAM PrincipalId
 you want to filter with.

     By default; the query only shows AMS access sessions. If you also want to show
 non-AMS access sessions,
     remove the "useragent" filter in the WHERE clause of the query.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
```

```
      json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
 PrincipalId",
      json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
 SessionId",
      eventtime AS "EventTime",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventid AS "EventId",
      json_extract_scalar(requestparameters, '$.tags[0].value') AS "BusinessNeed",
      json_extract_scalar(requestparameters, '$.tags[1].value') AS "BusinessNeedType",
      json_extract_scalar(requestparameters, '$.tags[2].value') AS "Requester",
      json_extract_scalar(requestparameters, '$.tags[3].value') AS "AccessRequestType"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND eventname = 'AssumeRole'
      AND useragent = 'access.managedservices.amazonaws.com'
      -- AND  json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId')
 = '<IAM PrincipalId>'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of AMS access sessions during specific time range.
   # The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.
   #
   # By default; the IAM Principal ID filter is disabled (it shows access sessions for
 all IAM principals).
   # If you want to only show access sessions for a particular IAM principal ID, remove
 the # (#) from
   # the "IAM Principal ID" filter of the query, and replace the placeholder "<IAM
 PrincipalId>" with the specific ID that you want.
   # You can run the query without the filter to determine the exact IAM PrincipalId
 you want to filter with.
   #
   # By default; the query only shows AMS access sessions. If you also want to show
 non-AMS access sessions,
   # remove the "useragent" filter from the query.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter eventName="AssumeRole" AND userAgent="access.managedservices.amazonaws.com"
```

```
   # | filter responseElements.assumedRoleUser.assumedRoleId= "<IAM PrincipalId>"
   | sort eventTime desc
   | fields
      responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
      responseElements.credentials.accessKeyId as IAMSessionId,
      eventTime as EventTime,
      eventName as EventName,
      awsRegion as EventRegion,
      eventID as EventId,
      requestParameters.tags.0.value as BusinessNeed,
      requestParameters.tags.1.value as BusinessNeedType,
      requestParameters.tags.2.value as Requester,
      requestParameters.tags.3.value as AccessRequestType
```

### ams_events_query_v1

```
ams_events_query_v1.yaml
/*
  The query provides list of events to track write actions for all AMS changes.
  The query returns all write actions done on the account using that AMS role filter.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  You can also track mutating actions done by non-AMS roles by removing the
 "useridentity.arn" filter lines from the WHERE clause of the query.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   useridentity.arn AS "RoleArn",
   eventid AS "EventId",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventsource AS "EventService",
   eventtime AS "EventTime",
   requestparameters As "RequestParameters",
```

```
   responseelements AS "ResponseElements",
   useragent AS "UserAgent"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   readonly <> 'true'
   AND
   (
      LOWER(useridentity.arn) LIKE '%/ams%'
      OR LOWER(useridentity.arn) LIKE '%/customer_ssm_automation_role%'
   )
ORDER BY eventtime
```

### ams_instance_access_sessions_query_v1

```
ams_instance_access_sessions_query_v1
/*
  The query provides list of AMS Instance accesses during specific time range.

  The query returns the list of AMS instance accesses; every record includes the event
 time, the event AWS Region, the instance ID, the IAM session ID, and the SSM session
 ID.
  You can use the IAM Principal ID to get more details on the business need for
 accessing the instance by using ams_access_session_query_v1 athena query.
  You can use the SSM session ID to get more details on the instance access session,
 including the start and end time of the session and log details, using the AWS Session
 Manager Console in the instance's AWS Region.

  You can also list non-AMS instance accesses by removing the "useridentity" filter
 line in the WHERE clause of the query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   json_extract_scalar(requestparameters, '$.target') AS "InstanceId",
   json_extract_scalar(responseelements, '$.sessionId') AS "SSM SessionId",
```

```
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventsource AS "EventService",
   eventtime AS "EventTime"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   useridentity.sessionContext.sessionIssuer.arn like '%/ams_%'
   AND eventname = 'StartSession'
ORDER BY eventtime
```

### ams_privilege_escalation_events_query_v1

```
ams_privilege_escalation_events_query_v1.yaml
/*
  The query provides list of events that can directly or potentially lead to a
 privilege escalation.

  The query accepts ActionedBy as an optional filter and returns EventName, EventId,
 EventTime, ... etc.
  All fields associated with the event are also returned. Some fields are blank if not
 applicable for that event.
  You can use the IAM Session ID to get more details about events happened in that
 session by using ams_session_events_query_v1 query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  By default, the ActionedBy filter is disabled (it shows privilege escalation events
 from all users).
  To show events for a particular user or role, remove the double-dash (--) from the
 useridentity filter line in the WHERE clause of the query
  and replace the placeholder "<ACTIONEDBY_PUT_USER_NAME_HERE>" with an IAM user or
 role name.
  You can run the query without the filter to determine the exact user you want to
 filter with.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
```

```
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventtime AS "EventTime",
   json_extract_scalar(requestparameters, '$.userName') AS "UserName",
   json_extract_scalar(requestparameters, '$.roleName') AS "RoleName",
   json_extract_scalar(requestparameters, '$.groupName') AS "GroupName",
   json_extract_scalar(requestparameters, '$.policyArn') AS "PolicyArn",
   json_extract_scalar(requestparameters, '$.policyName') AS "PolicyName",
   json_extract_scalar(requestparameters, '$.permissionsBoundary') AS
 "PermissionsBoundary",
   json_extract_scalar(requestparameters, '$.instanceProfileName') AS
 "InstanceProfileName",
   json_extract_scalar(requestparameters, '$.openIDConnectProviderArn') AS
 "OpenIDConnectProviderArn",
   json_extract_scalar(requestparameters, '$.serialNumber') AS "SerialNumber",
   json_extract_scalar(requestparameters, '$.serverCertificateName') AS
 "ServerCertificateName",
   json_extract_scalar(requestparameters, '$.accessKeyId') AS "AccessKeyId",
   json_extract_scalar(requestparameters, '$.certificateId') AS "CertificateId",
   json_extract_scalar(requestparameters, '$.newUserName') AS "NewUserName",
   json_extract_scalar(requestparameters, '$.newGroupName') AS "NewGroupName",
   json_extract_scalar(requestparameters, '$.newServerCertificateName') AS
 "NewServerCertificateName",
   json_extract_scalar(requestparameters, '$.name') AS "SAMLProviderName",
   json_extract_scalar(requestparameters, '$.sAMLProviderArn') AS "SAMLProviderArn",
   json_extract_scalar(requestparameters, '$.sSHPublicKeyId') AS "SSHPublicKeyId",
   json_extract_scalar(requestparameters, '$.virtualMFADeviceName') AS
 "VirtualMFADeviceName"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   (
     -- More event names can be found at https://docs.aws.amazon.com/IAM/latest/
UserGuide/list_identityandaccessmanagement.html
     eventname LIKE 'Add%' OR
     eventname LIKE 'Attach%' OR
     eventname LIKE 'Delete%' AND eventname != 'DeleteAccountAlias' OR
     eventname LIKE 'Detach%' OR
     eventname LIKE 'Create%' AND eventname != 'CreateAccountAlias' OR
```

```
     eventname LIKE 'Put%' OR
     eventname LIKE 'Remove%' OR
     eventname LIKE 'Update%' OR
     eventname LIKE 'Upload%' OR
     eventname = 'DeactivateMFADevice' OR
     eventname = 'EnableMFADevice' OR
     eventname = 'ResetServiceSpecificCredential' OR
     eventname = 'SetDefaultPolicyVersion'
   )
   AND eventsource = 'iam.amazonaws.com'
ORDER BY eventtime
```

### ams_resource_events_query_v1

```
Name: ams_resource_events_query_v1

Description: >-
   The query provides list of events done on specific resource.
   The query accepts resource id as part of the filters, and return all write actions
 done on that resource.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of events done on specific resource.

     The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the WHERE clause of the query),
     and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
     Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      useridentity.principalId AS "IAM PrincipalId",
```

```
      useridentity.accesskeyid AS "IAM SessionId",
      useridentity.accountid AS "AccountId",
      reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventid AS "EventId",
      eventsource AS "EventService",
      eventtime AS "EventTime"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
      AND
      (
         requestparameters LIKE '%<RESOURCE_INFO>%'
         OR responseelements LIKE '%<RESOURCE_INFO>%'
      )
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of events done on specific resource.
   #
   # The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the filter of the query),
   # and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
   # Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter readOnly=0
   | parse @message '"requestParameters":{*}' as RequestParameters
   | parse @message '"responseElements":{*}' as ResponseElements
   # | filter RequestParameters like "RESOURCE_INFO" or ResponseElements like
 "<RESOURCE_INFO>"
   | fields
      userIdentity.principalId as IAMPrincipalId,
      userIdentity.accessKeyId as IAMSessionId,
      userIdentity.accountId as AccountId,
      userIdentity.arn as ActionedBy,
      eventName as EventName,
```

```
      awsRegion as EventRegion,
      eventID as EventId,
      eventSource as EventService,
      eventTime as EventTime
   | display IAMPrincipalId, IAMSessionId, AccountId, ActionedBy, EventName,
 EventRegion, EventId, EventService, EventTime
   | sort eventTime desc
```

### ams_session_events_query_v1

```
Name: ams_session_events_query_v1

Description: >-
   The query provides list of events done on specific session.
   The query accepts IAM Principal Id as part of the filters, and return all write
 actions done on that resource.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides a list of events executed on a specific session.

     The query accepts the IAM principal ID as part of the filters (replace the
 placeholder "<PRINCIPAL_ID>" in the WHERE clause of the query),
     and returns all write actions done on that resource.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      useridentity.principalId AS "IAM PrincipalId",
      useridentity.accesskeyid AS "IAM SessionId",
      useridentity.accountid AS "AccountId",
      reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventsource AS "EventService",
      eventtime AS "EventTime",
```

```
      requestparameters As "RequestParameters",
      responseelements AS "ResponseElements",
      useragent AS "UserAgent"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate   WHERE
      useridentity.principalid = '<PRINCIPAL_ID>'
      AND datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides a list of events executed on a specific session.
   #
   # The query accepts the IAM principal ID as part of the filters (replace the
 placeholder "<PRINCIPAL_ID>" in the filter of the query),
   # and returns all write actions done on that resource.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter readOnly=0 AND userIdentity.principalId = "<IAM Principal>"
   | sort eventTime desc
   | fields
      userIdentity.accessKeyId as IAMSessionId,
      userIdentity.principalId as IAMPrincipalId,
      userIdentity.accountId as AccountId,
      userIdentity.arn as ActionedBy,
      eventName as EventName,
      awsRegion as EventRegion,
      eventSource as EventService,
      eventTime as EventTime,
      userAgent as UserAgent
   | parse @message '"requestParameters":{*}' as RequestParameters
   | parse @message '"responseElements":{*}' as ResponseElements
```

### ams_session_ids_by_requester_v1

```
Name: ams_session_ids_by_requester_v1

Description: >-
   The query provides list of IAM Principal/Session Ids for specific requester.
   The query accepts requester and return all IAM Principal/Session Ids by that
 requester during specific time range.
```

```
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of IAM Principal IDs for a specific requester.

     The query accepts the requester (replace placeholder "<Requester>" in the WHERE
 clause of the query),
     and returns all IAM Principal IDs by that requester during a specific time range.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
 PrincipalId",
      json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
 SessionIId",
      eventtime AS "EventTime"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND json_extract_scalar(requestparameters, '$.tags[2].value') = '<Requester>'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of IAM Principal IDs for a specific requester.
   #
   # The query accepts the requester (replace placeholder "<Requester>" in the filter
 of the query),
   # and returns all IAM Principal IDs by that requester during a specific time range.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   filter eventName="AssumeRole" AND requestParameters.tags.2.value="<Requester>"
   | sort eventTime desc
   | fields
      responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
```

```
    responseElements.credentials.accessKeyId as IAMSessionId,
    eventTime as EventTime
```

# Cambiar los permisos de registro

Se necesitan los siguientes permisos para ejecutar consultas de registro de cambios:

- Athena
  - Atenea: GetWorkGroup
  - atenea: StartQueryExecution
  - atenea: ListDataCatalogs
  - atenea: GetQueryExecution
  - atenea: GetQueryResults
  - atenea: BatchGetNamedQuery
  - atenea: ListWorkGroups
  - atenea: UpdateWorkGroup
  - atenea: GetNamedQuery
  - atenea: ListQueryExecutions
  - atenea: ListNamedQueries
- AWS KMS
  - kms:Decrypt
  - AWS KMS ID de clave de AMSCloudTrailLogManagement, o sus ID de AWS KMS clave, si Accelerate utiliza su almacén de datos de bucket Amazon S3 de CloudTrail Trail Events mediante el cifrado SSE-KMS.
- AWS Glue
  - pegamento: GetDatabase
  - pegamento: GetTables
  - pegamento: GetDatabases
  - pegamento: GetTable
- Acceso de lectura a Amazon S3
  - CloudTrail Almacén de datos de bucket de Amazon S3: ams-a *AccountId* -cloudtrail-, o el nombre de *primary region* su bucket de Amazon S3, trail events CloudTrail Amazon S3 data store.

- Acceso de escritura a Amazon S3
  - Resultados de consultas de eventos de Athena bucket de Amazon S3: *AccountId* ams-a athena-results- *primary region*

# AWS Systems Manager en Accelerate

Un AWS Systems Manager documento (documento SSM) define las acciones que Systems Manager realiza en sus AWS recursos. Systems Manager incluye más de una docena de documentos preconfigurados que puede utilizar especificando parámetros en tiempo de ejecución. Los documentos utilizan la notación de JavaScript objetos (JSON) o YAML e incluyen los pasos y parámetros que especifique.

AWS Managed Services (AMS) es un editor de confianza para documentos SSM. Los documentos SSM propiedad de AMS se comparten únicamente con las cuentas AMS integradas, siempre comienzan con un prefijo reservado (AWSManagedServicios-*) y aparecen en la consola de Systems Manager, propiedad de Amazon. El proceso de AMS para el desarrollo y la publicación de documentos SSM sigue las prácticas recomendadas de AWS y requiere varias revisiones por pares a lo largo del ciclo de vida del documento. Para obtener más información sobre las prácticas recomendadas de AWS para compartir documentos SSM, consulte Prácticas recomendadas para documentos SSM compartidos.

## Documentos disponibles sobre AMS Accelerate SSM

Los documentos SSM de AMS Accelerate están disponibles exclusivamente para los clientes de AMS Accelerate y se utilizan para automatizar el flujo de trabajo operativo para gestionar su cuenta.

Para ver los documentos SSM de AMS Accelerate disponibles en: Consola de administración de AWS

1. Abra la consola de Systems Manager en la consola.AWS Systems Manager
2. Seleccione Compartido conmigo.
3. En la barra de búsqueda, filtra por prefijo de nombre de documento, luego por igual y establece el valor en AWSManagedServicios-.

   Para AWS CLI obtener instrucciones, consulte Uso de documentos SSM compartidos.

## Versiones de documentos AMS Accelerate SSM

Los documentos SSM admiten el control de versiones. Los documentos SSM de AMS Accelerate no se pueden modificar desde la cuenta del cliente ni se pueden volver a compartir. AMS Accelerate los gestiona y mantiene de forma centralizada para gestionar la cuenta.

Los números de versión se incrementan con cada actualización del documento en una región de AWS específica. A medida que haya nuevas regiones disponibles, el mismo contenido del documento en dos regiones puede tener números de versión diferentes; esto es normal y no significa que su comportamiento vaya a ser diferente. Si quiere comparar dos documentos SSM de AMS Accelerate, le recomendamos que compare sus hashes con los siguientes: AWS CLI

```
aws ssm describe-document \
--name AWSManagedServices-DOCUMENTNAME \
--output text --query "Document.Hash"
```

Dos documentos SSM son idénticos si sus hashes coinciden.

## Precios de Systems Manager

El acceso a los documentos SSM de AMS Accelerate no conlleva ningún coste. El costo del tiempo de ejecución varía según el tipo de documento SSM, sus pasos y la duración del tiempo de ejecución. Para obtener más información, consulta los AWS Systems Manager precios.

# Historial de documentos de la Guía del usuario de AMS Accelerate

En la siguiente tabla se describen los cambios importantes de cada versión de la Guía del usuario de AMS Accelerate. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Documentación actualizada de Alarm Manager para actualizar el plano de control | Se actualizó la documentación de Alarm Manager para reflejar la migración del plano de control completada en febrero de 2026:<br>• Accelerate Alarm Manager: se eliminó el aviso de limitación regional, se hizo hincapié en la advertencia de configuración y se eliminó la indicación de tiempo sobre la entrada en vigor de los cambios<br>• Perfil de configuración de Accelerate: supervisión: se ha eliminado una afirmación contradictoria sobre el ID de configuración<br>• Perfil de configuración de Accelerate: sustitución de pseudoparámetros: se agregaron pseudoparámetros para los nuevos tipos de recursos y se actualizaron las descripci | 31 de marzo de 2026 |

| | | |
|---|---|---|
| | ones existentes para las instancias y los discos de EC2, los dominios de Elasticsearch y Elastic Load Balancing<br>• Ejemplos de configuración de alarmas de Accelerate: se eliminó la dimensión de ruta del ejemplo de alarma de disco de Linux porque el parámetro de ruta de disco ya no es compatible con Linux<br>• Se eliminó la página obsoleta «Visualización del número de recursos monitoreados por Alarm Manager», ya que la funcionalidad de generación de informes quedó obsoleta con la actualización del plano de control<br>• Inventario de recursos de Accelerate: actualizado para hacer referencia a un nuevo archivo de inventario de recursos que refleja los cambios en la arquitectura del plano de control | |
| Inventario de recursos actualizado para Accelerate | Se agregaron detalles sobre el control de cumplimiento de la infraestructura de AMS. | 27 de marzo de 2026 |

| | | |
|---|---|---|
| Se actualizaron los valores booleanos recomendados por Compute Optimizer | Se actualizaron todos los valores de los parámetros booleanos de mayúsculas () a minúsculas (True/False) para mantener la coherencia con las convenciones estándar. true/false | 24 de marzo de 2026 |
| Se actualizó AMS-STD-002 el punto 6.11 para las políticas multicuenta | Se aclaró que las políticas multicuentas que permiten el acceso por escrito a cuentas de terceros se pueden configurar asumiendo el riesgo. | 24 de marzo de 2026 |
| Notas AWS Health de monitoreo actualizadas | Se aclaró que las notificac iones se envían solo para AWS Health los eventos que requieren la acción de AMS Operations. | 24 de marzo de 2026 |
| Se agregó la corrección automática de la capacidad de volumen de ONTAP | Se ha añadido una AMSFSXONTAPVolumeC apacityUtilization alerta a la tabla de corrección automátic a y se ha añadido una nueva sección en la que se describe la automatización de la corrección de la capacidad de volumen de ONTAP. | 24 de marzo de 2026 |
| Etiqueta de campo de períodos de programación del Programador de Recursos actualizada | Se corrigió la etiqueta del campo de «Programaciones» a «Períodos» en el procedimi ento de agregar programación. | 11 de marzo de 2026 |

| | | |
|---|---|---|
| Alertas actualizadas del monitoreo de referencia en la sección AMS | Alertas actualizadas de la supervisión de referencia en la tabla AMS con una condición de activación actualizada para la instancia de Amazon EC2 (todos los sistemas operativos). | 22 de enero de 2026 |
| Se actualizó la sección del proceso de gestión de riesgos de seguridad del cliente | Se actualizó la sección del proceso de gestión de los riesgos de seguridad del cliente con información sobre la aceptación, la validez, la revisión y la exclusión de los riesgos. | 15 de enero de 2026 |
| Se actualizó la sección de automatización de la corrección de eventos de bajo almacenamiento de Amazon RDS en AMS: remediación automática de alertas | Se actualizó la sección de automatización de la corrección de eventos de bajo almacenamiento de Amazon RDS con información sobre las propiedades modificadas por las correcciones en función del evento desencadenante. | 15 de enero de 2026 |
| Tabla actualizada de la sección de operaciones bajo demanda | Se actualizó la tabla de la sección de operaciones bajo demanda con contenido actualizado. | 7 de enero de 2026 |

| | | |
|---|---|---|
| Se actualizó y agregó contenido nuevo a Trusted Remediator en la sección AMS con información sobre Security Hub (CSPM). | Se actualizó la sección Trusted Remediator en AMS con información sobre Security Hub CSPM y se agregó una nueva página, las recomenda ciones de Security Hub CSPM compatibles con Trusted Remediator. | 11 de diciembre de 2025 |
| Regiones compatibles actualizadas | Se agregaron notas en las siguientes secciones para los servicios que no están disponibles en la región Asia Pacífico (Malasia):<br>• Monitoriza con Amazon Macie<br>• Supervisión y gestión de incidentes para Amazon EKS en AMS Accelerate<br>• Instalación automática de SSM Agent<br>• Acelere Alarm Manager | 24 de octubre de 2025 |
| AWS CloudTrail Sección de gestión de registros actualiza da | Nueva información y nota sobre el AWS CloudTrail registro. | 25 de septiembre de 2025 |

| | | |
|---|---|---|
| Se agregaron 4 nuevas comprobaciones de optimización de Trusted Advisor costos compatibles con Trusted Remediator | Se agregaron las siguientes comprobaciones de optimización de costos:<br>• c1z7kmr00n: recomendaciones de optimización de costes para instancias en Amazon EC2<br>• c1z7kmr02n - Recomendaciones de optimización de costes de Amazon EBS para volúmenes<br>• c1z7kmr03n - Recomendaciones de optimización de costes de Amazon RDS para instancias de base de datos<br>• c1z7kmr05n AWS Lambda : recomendaciones de optimización de costos para las funciones | 22 de septiembre de 2025 |
| Nota de obsolescencia actualizada para el servicio Change Record | Se actualizó la nota de obsolescencia del servicio Change Record con soluciones alternativas. | 11 de septiembre de 2025 |
| Controles Trusted Advisor de seguridad actualizados compatibles con Trusted Remediator | Se actualizaron los parámetros y restricciones preconfigurados compatibles para comprobar Hs4Ma3G108: las rutas CloudTrail deberían integrarse con Amazon Logs CloudWatch | 5 de septiembre de 2025 |

| | | |
|---|---|---|
| Las comprobaciones de seguridad actualizadas son compatibles Trusted Advisor con Trusted Remediator | Se actualizó Trusted Advisor la comprobación de seguridad para añadir la versión 2 de Hs4Ma3G184: se debe habilitar el registro de los balanceadores de carga de aplicaciones y los balanceadores de carga clásicos | 5 de septiembre de 2025 |
| Las comprobaciones de excelencia Trusted Advisor operativa actualizadas son compatibles con la sección Trusted Remediator | Se actualizaron las comprobaciones de excelencia Trusted Advisor operativa compatibles con Trusted Remediator para añadir una nueva comprobación compatible c1fd6b96l4 Amazon S3 Access Logs Enabled. | 28 de agosto de 2025 |
| Se actualizó la sección Trusted Remediator para incluir contenido nuevo para Compute Optimizer | Se actualizó la sección Trusted Remediator para incluir contenido nuevo para las recomendaciones compatibles. AWS Compute Optimizer | 18 de agosto de 2025 |
| Se ha eliminado el enlace al glosario TOC | AWS Glosario. | 8 de agosto de 2025 |
| Se ha eliminado el enlace al glosario TOC | AWS Glosario. | 8 de agosto de 2025 |
| Nuevo campo en el informe de Patch Daily | Etiquetas de instancia: las etiquetas asociadas al ID de instancia de Amazon EC2. | 8 de agosto de 2025 |

| | | |
|---|---|---|
| Nuevas comprobaciones de Trusted Remediator | Trusted Advisor comprobaciones de optimización de costes compatibles con las comprobaciones de Trusted Advisor seguridad de Trusted Remediator compatibles con Trusted Remediator Hs4Ma3G120—, Hs4Ma3G230— y c18d2gz150—AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime. AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime | 8 de agosto de 2025 |
| Actualización del estándar de IAM en el punto 3.2 | Se ha aclarado el lenguaje y se ha eliminado la mención del etiquetado. | 25 de julio de 2025 |
| Se actualizaron los perfiles de configuración del etiquetador de recursos en Accelerate | Se agregó un nuevo AvailabilityZone filtro en los perfiles de configuración del etiquetador de recursos en Accelerate. | 25 de julio de 2025 |
| Se actualizaron los informes de incidentes, las solicitudes de servicio y las preguntas sobre facturación en Accelerate. | Se reemplazaron las referencias a los niveles de servicio Plus y Premium por un enlace al SLA del servicio. | 25 de julio de 2025 |
| Se actualizó la gestión de incidentes en Accelerate. | Información actualizada sobre los centros de operaciones. | 25 de julio de 2025 |

| | | |
|---|---|---|
| Página de patrones de AMS actualizada con los enlaces correctos. | Se corrigieron los enlaces SLA y SLO. | 25 de julio de 2025 |
| Actualización de las opciones de exclusión de alertas | La adición de una etiqueta le permite optar por no recibir otras dos alertas. | 25 de julio de 2025 |
| Nueva función para las copias de seguridad | Personalice las notificaciones en las bóvedas de respaldo con una nueva etiqueta. | 25 de julio de 2025 |
| Sección actualizada para las configuraciones compatibles en Accelerate | Configuraciones compatibles actualizadas para los sistemas operativos compatibles y los sistemas operativos de fin de soporte (EOS) compatibles en Accelerate. | 26 de junio de 2025 |
| Se ha eliminado la página Gestión de etiquetas para la gestión de parches en Accelerate | Se ha eliminado la página Gestión de etiquetas para la gestión de parches en Accelerate, ya que esta función está obsoleta. | 19 de junio de 2025 |
| Nota de seguridad important e sobre la gestión de parches para los repositorios de parches alternativos. | Nota de seguridad important e y prácticas recomendadas para el uso de repositorios de parches alternativos en AMS Accelerate. | 10 de junio de 2025 |
| AMS Accelerate cambia la obsolescencia de los registros. | El servicio AMS Accelerat e Change Record dejará de estar disponible a partir del 1 de julio de 2025. | 27 de mayo de 2025 |

| | | |
|---|---|---|
| Actualizaciones de sistemas operativos compatibles. | Los sistemas operativos compatibles con AMS Accelerate se actualizan, algunos se añaden y otros se eliminan. | 22 de mayo de 2025 |
| Nota sobre los servicios compatibles en la región de Oriente Medio (EAU). | El soporte para algunos servicios en la región de Oriente Medio (EAU) es limitado. | 22 de mayo de 2025 |
| Internal-only APIs. | Internal-only API que aparecen en algunos CloudWatch registros. | 22 de mayo de 2025 |
| Se agregaron las ubicaciones de registro que faltaban. | Se agregaron algunas ubicaciones de registro de Windows que faltaban. | 22 de mayo de 2025 |
| Actualizaciones de AMS Accelerate Trusted Remediator. | Cómo utilizar un parámetro nuevo,`preconfigured-parameters` , para personalizar las Trusted Advisor comprobaciones en Trusted Remediator. | 22 de mayo de 2025 |
| Preguntas frecuentes y actualizaciones sobre AMS Accelerate Trusted Remediator. | Varias actualizaciones de las Trusted Advisor comprobaciones compatibles y las preguntas frecuentes sobre Trusted Remediator (se agregó: «¿Qué recursos utiliza Trusted Remediator en sus cuentas?») y más. Consulte también las Trusted Advisor comprobaciones compatibles con Trusted Remediator. | 8 de mayo de 2025 |

| | | |
|---|---|---|
| Actualización de los controles de seguridad de AMS Accelerate Standard. | Se agregaron los controles de «uso compartido de grupos de seguridad». | 8 de mayo de 2025 |
| Acelere la actualización de las alertas de monitoreo. | Se agregaron alertas adicionales y se agregó el nombre de la alerta a la columna de notas. | 28 de abril de 2025 |
| Acelere el inventario de recursos. | Se actualiza el archivo de hoja de cálculo del inventario de recursos (comprimido). | 24 de abril de 2025 |
| Acelere las ubicaciones de registro. | Se agregaron ubicaciones de registro adicionales. | 24 de abril de 2025 |
| Acelere las nuevas funciones y responsabilidades (RACI) para responder a los incidentes de seguridad. | RACI para la respuesta a incidentes de seguridad. | 27 de marzo de 2025 |
| Acelere la nueva alerta de remediación automática de Amazon RDS. | ID de alerta: - 0224, se activa cuando el almacenamiento asignado solicitado alcanza o supera el umbral de almacenamiento máximo configurado. | 27 de marzo de 2025 |
| Acelera la actualización de la plantilla de roles de incorporación. | La plantilla de roles de incorporación de AMS Accelerate se ha actualizado para que sea compatible con GovCloud las regiones de AWS. | 25 de marzo de 2025 |
| Acelere la alerta de RDS de nuevas remediaciones automáticas. | RDS-EVENT-0224 agregado. | 17 de marzo de 2025 |

| | | |
|---|---|---|
| Acelere la nueva función: notificaciones de incidentes. | Se puede utilizar AppRegistry para crear aplicaciones y personalizar las notificaciones de incidentes para esas aplicaciones. | 13 de marzo de 2025 |
| Acelere la actualización al umbral de monitoreo de alarmas del RDS. | El umbral de alarma de uso medio de la CPU del RDS se ha cambiado del 75% al 90%. | 20 de febrero de 2025 |
| Acelere la actualización a la tabla de corrección automática de alertas de AMS. | La tabla de corrección de alertas se ha ampliado con contenido nuevo. | 20 de febrero de 2025 |
| Acelere la nueva función: Retain Alarms. | Puede configurar Alarm Manager para conservar las alarmas en CloudWatch lugar de eliminarlas automáticamente. | 20 de febrero de 2025 |

| | | |
|---|---|---|
| Self-service Informes actualizados con nuevas opciones de datos para la visualización de informes agregados | Se agregaron opciones de datos para incluir un nuevo nombre de campo:`Admin Account ID`, nombre de campo del conjunto de datos: y definición: `Trusted AWS Organization account enabled by the customer` para los siguientes Self-service informes: `aws_admin_account_id`<br>• Informe de parches (diario)<br>• Informe de Backup (diario)<br>• Informe de incidentes (semanal)<br>• Panel de control de Resource Tagger<br>• Panel de reglas de configuración de seguridad | 28 de enero de 2025 |

| | | |
|---|---|---|
| Se agregaron AWS Trusted Advisor comprobaciones adicionales compatibles con Trusted Remediator | Trusted Remediator admite ahora las siguientes Trusted Advisor comprobaciones:<br>• Optimización de costes<br>  • c1cj39rr6v - Configuración incompleta de cancelación de carga multiparte de Amazon S3<br>• Seguridad<br>  • Hs4Ma3G199: Las instancias de base de datos de RDS deben publicar registros en Logs CloudWatch<br>  • Hs4Ma3G326: La configuración de acceso público del bloque Amazon EMR debe estar habilitada<br>  • Hs4Ma3G272: Los usuarios no deberían tener acceso root a las instancias de ordenadores portátiles de IA SageMaker<br>  • Hs4Ma3G325: Los clústeres de EKS deben tener habilitado el registro de auditoría<br>  • HHs4Ma3G118 - Los grupos de seguridad predeterminados de VPC no deberían permitir el tráfico entrante o saliente | 28 de enero de 2025 |

    - Hs4Ma3G127: el registro de ejecución de API Gateway REST WebSocket y API debe estar habilitado
    - Hs4Ma3G124: Las instancias de Amazon EC2 deben usar Instance Metadata Service versión 2 (IMDSv2)
- Tolerancia a errores
    - c1qf5bt013 - Las instancias de base de datos de Amazon RDS tienen desactivado el escalado automático del almacenamiento
    - 7q GXsKIUw - Draining de conexión Classic Load Balancer
    - c18d2gz106 - Amazon EBS no está incluido en el plan AWS Backup
    - c18d2gz107 - La tabla de Amazon DynamoDB no está incluida en el plan AWS Backup
    - cc18d2gz117: Amazon EFS no está incluido en el plan AWS Backup
    - c18d2gz105 - Equilibri o de carga cruzada con Network Load Balancer

        - c1qf5bt026 - El parámetro synchronous_commit de Amazon RDS está desactivado
        - c1qf5bt030 - El parámetro innodb_flush_log_at_trx_commit de Amazon RDS no es 1
        - c1qf5bt031 - El parámetro sync_binlog de Amazon RDS está desactivado
        - c1qf5bt036 - La configuración del parámetro innodb_default_row_format de Amazon RDS no es segura
        - c18d2gz144 - La supervisión detallada de Amazon EC2 no está habilitada
    - Excelencia operativa
        - c18d2gz125 - Amazon API Gateway no registra los registros de ejecución
        - c18d2gz168: La protección elástica de carga no está habilitada para los balanceadores de carga BalancingDeletion
        - c1qf5bt012 - Amazon RDS Performance Insights está desactivado
    - Desempeño
        - c1qf5bt021 - El parámetro innodb_change_buffering

| | | |
|---|---|---|
| | de Amazon RDS utiliza un valor inferior al óptimo<br>• c1qf5bt025 - El parámetro de autovacuum de Amazon RDS está desactivado<br>• c1qf5bt028 - El parámetro enable_indexonlyscan de Amazon RDS está desactivado<br>• c1qf5bt029 - El parámetro enable_indexscan de Amazon RDS está desactivado<br>• c1qf5bt032 - El parámetro innodb_stats_persistent de Amazon RDS está desactivado<br>• c1qf5bt037 - El parámetro Amazon RD está activado Sgeneral_logging | |
| Hoja de cálculo de inventario de recursos actualizada | Hoja de cálculo de inventario de recursos actualizada. | 23 de enero de 2025 |
| Nueva función de AMS: informes agregados de autoservicio | Los informes de autoservicio agregados (SSR) le proporcio nan una vista de los informes de autoservicio existente s agregados a nivel de la organización y de forma transversal. | 21 de enero de 2025 |

| | | |
|---|---|---|
| Nueva función de aplicación de parches de Accelerate: Patch Hooks | Utilice esta función para configurar los «ganchos» con los documentos de comandos SSM para ejecutar comandos a nivel del sistema operativo antes o después de aplicar los parches. | 16 de enero de 2025 |
| Actualización de la sección Cómo funciona la supervisión | Se agregó información sobre una nueva función, que permite configurar las notificaciones de alerta por recurso o ID de instancia, en lugar de por incidente. | 8 de enero de 2025 |
| Actualización de la sección de incorporación de EKS Monitoring and Incident Management | Se actualizó la nota sobre el procedimiento de incorporación para aclarar cuándo se suspenden y reanudan las señales de alerta. | 19 de diciembre de 2024 |
| Se ha añadido el registro de la cuenta de los miembros a Trusted Remediator | Puede utilizar el registro de cuentas de los miembros para encontrar el ID de cuenta, la incorporación y el Regiones de AWS tiempo de ejecución de cada cuenta de miembro. | 19 de diciembre de 2024 |
| Requisitos previos para el uso del agente SSM | Se ha actualizado el contenido sobre el bloqueo del tráfico saliente. | 4 de diciembre de 2024 |
| Accelerate Monitoring and Incidents Management for EKS ya cuenta con soporte en Asia Pacífico (Hong Kong) Región de AWS | Asia-Pacífico (Hong Kong) ahora cuenta con el apoyo de Accelerate Monitoring and Incident Management para EKS | 21 de noviembre de 2024 |

| | | |
|---|---|---|
| Tabla actualizada de ofertas de operaciones bajo demanda | Se admiten los siguientes sistemas operativos para las actualizaciones locales:<br>• Microsoft Windows 2016 a Microsoft Windows 2022 y versiones posteriores | 11 de noviembre de 2024 |
| Ahora, en África (Ciudad del Cabo), se admite Accelerate Monitoring and Incidents Management para EKS Región de AWS. | África (Ciudad del Cabo) cuenta ahora con el apoyo de Accelerate Monitoring and Incident Management for EKS | 4 de noviembre de 2024 |
| Tabla actualizada de ofertas de operaciones bajo demanda | Se admiten los siguientes sistemas operativos para las actualizaciones locales:<br>• Microsoft Windows 2012 R2 a Microsoft Windows 2016 y versiones posteriores<br>• De Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8<br>• De Red Hat Enterprise Linux 8 a Red Hat Enterprise Linux 9<br>• De Oracle Linux 7 a Oracle Linux 8 | 1 de noviembre de 2024 |
| Plantilla de inicio rápido actualizada | Diagrama, parámetros de plantilla y archivo de plantilla yaml actualizados. | 28 de octubre de 2024 |

| | | |
|---|---|---|
| Trusted Advisor comprobaciones añadidas a Trusted Remediator en AMS | Las siguientes Trusted Advisor comprobaciones ya están disponibles en Trusted Remediator:<br>• z4Aubrnsmz: direcciones IP elásticas no asociadas<br>• c18d2gz128 - Repositorio de Amazon ECR sin política de ciclo de vida configurada<br>• c18d2gz138 - Recuperación de DynamoDB Point-in-time<br>• Hs4Ma3G323: Las tablas de DynamoDB deberían tener habilitada la protección contra la eliminación<br>• Hs4Ma3G247: Amazon EC2 Transit Gateway no debería aceptar automáticamente las solicitudes de adjuntos de VPC<br>• Hs4Ma3G308: Los clústeres de Amazon DocumentDB deben tener habilitada la protección de eliminación<br>• Hs4Ma3G299 - Los clústeres de base de datos de Neptune deberían tener habilitada la protección de eliminación<br>• Hs4Ma3G306 - Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas | 25 de octubre de 2024 |

| | | |
|---|---|---|
| | • Hs4Ma3G109: la validación del archivo de registro debe estar habilitada CloudTrail<br>• Hs4Ma3G217: los entornos de CodeBuild proyecto deben tener una configura ción de AWS de registro4<br>• Hs4Ma3G158: los documentos SSM no deben ser públicos<br>• Hs4Ma3G319 - Los firewalls de Network Firewall deben tener habilitada la protecció n de eliminación | |
| Configuraciones compatibles actualizadas | Se actualizaron los sistemas operativos Oracle Linux compatibles a 9.0-9.3, 8.0-8.9 y 7.5-7.9. | 24 de octubre de 2024 |
| AMS Accelerate ha añadido una nueva sección a Offboard | Instrucciones sobre cómo desconectarse con las dependencias Alarm Manager y Resource Tagger agregadas a Offboard desde AMS Accelerate. | 24 de octubre de 2024 |
| El panel de control de Resource Tagger ya está disponible. | El panel de control de Resource Tagger ya está disponible en Self-service los informes. | 26 de septiembre de 2024 |
| Ahora puede incluir varias direcciones de correo electróni co en las alertas basadas en etiquetas. | Ahora se admiten varias direcciones de correo electróni co en las alertas basadas en etiquetas. | 20 de septiembre de 2024 |

| | | |
|---|---|---|
| Los límites de AMS Accelerate ahora están incluidos en la administración de parches de AMS. | Los límites de AMS Accelerate están incluidos en la gestión de parches: cree un período de mantenimiento de parches. | 30 de agosto de 2024 |
| Actualización de AMS Accelerate Account Discovery | Se ha agregado una nueva sección en Account Discovery para la evaluación de instancias de Amazon EC2. | 29 de agosto de 2024 |
| La línea base de parches predeterminada de AMS Accelerate ya está disponible para los sistemas operativos Ubuntu. | La línea base de parches predeterminada de AMS Accelerate ya está disponible para los sistemas operativos Ubuntu. | 22 de agosto de 2024 |
| Actualización de AMS Accelerate Account Discovery | Se han agregado cuatro nuevas llamadas a la AWS API a la sección de AWS CloudTrail evaluación de la tabla de verificación operativa. | 2 de agosto de 2024 |
| Trusted Remediator ahora admite una comprobación adicional | Trusted Remediator ahora admite la comprobación de seguridad Hs4Ma3G192: las instancias de base de datos de RDS deberían prohibir el acceso público. | 30 de julio de 2024 |
| AMS ahora es compatible con el firewall DNS Amazon Route 53 Resolver | AMS ahora es compatible con el firewall DNS Amazon Route 53 Resolver | 30 de julio de 2024 |
| AMS Accelerate onboarding_role_minimal.zip ahora contiene el código de Terraform | AMS Accelerate onboarding_role_minimal.zip ahora contiene el código de Terraform. | 30 de julio de 2024 |

| | | |
|---|---|---|
| Panel de reglas de configuración de seguridad | El panel de reglas de Security Config ahora está disponible en los Self-Service informes. | 24 de julio de 2024 |
| AMS Accelerate ahora es compatible con Oracle Linux 8.9, RHEL 8.10 y RHEL 9.4. | AMS Accelerate ahora es compatible con Oracle Linux 8.9, RHEL 8.10 y RHEL 9.4. | 5 de julio de 2024 |
| Se ha actualizado el proceso de descubrimiento de cuentas de AMS Accelerate. | Se ha actualizado el proceso de detección de cuentas utilizado al Cuentas de AWS incorporarse a AMS Accelerate. | 1 de julio de 2024 |
| Trusted Remediator ya está disponible. | Ya está disponible Trusted Remediator, una solución de AWS Managed Services que automatiza la corrección de las AWS Trusted Advisor comprobaciones. | 24 de junio de 2024 |
| Eventos de firewall de DNS de Amazon Route 53 Resolver en Security Incident Response. | AMS ahora monitorea los eventos del firewall de DNS de Amazon Route 53 Resolver en Security Incident Response | 21 de junio de 2024 |
| Sistemas operativos compatibles actualizados | AMS Accelerate ahora es compatible con las AlmaLinux versiones 8.3-8.9 y 9.0-9.2 (solo AlmaLinux es compatible con la arquitectura x86) | 19 de junio de 2024 |
| El límite automático del perfil de instancia ahora aumenta si se cumple el valor predeterminado. | AMS ahora aumenta el límite predeterminado del perfil de instancia a 20 si se alcanza el límite predeterminado de 10. | 18 de junio de 2024 |

| | | |
|---|---|---|
| La función de instalación automática del agente AMS SSM ahora está habilitada de forma predeterminada. | La función de instalación automática del agente AMS SSM está habilitada de forma predeterminada para las cuentas incorporadas después de /2024. 6/03 | 7 de junio de 2024 |
| Se han añadido preguntas frecuentes sobre seguridad a la gestión de la seguridad. | Ya está disponible una sección de preguntas frecuentes sobre seguridad que cubre las preguntas más frecuentes sobre las mejores prácticas de seguridad, los controles, los modelos de acceso y los mecanismos de auditoría que se utilizan cuando un ingeniero de operaciones o un ingeniero de automatización de AMS accede a sus cuentas. | 3 de junio de 2024 |
| Monitoring and Incident Management para Amazon EKS ahora admite AWS regiones adicionales. | Monitoring and Incident Management for Amazon EKS ahora admite tres AWS regiones adicionales. | 23 de mayo de 2024 |
| Las notificaciones de solicitud de servicio de parches ahora se envían antes de los períodos de mantenimiento de parches. | El parcheo de AMS Accelerat e crea una nueva solicitud de servicio 4 días antes del período de mantenimiento de parches. Puede utilizar la solicitud de servicio para comunicarse con AMS para realizar ajustes en el parche u omitir un parche. | 3 de mayo de 2024 |

| | | |
|---|---|---|
| Los umbrales de alerta se han agregado a la tabla de alertas de referencia de monitoreo de AMS Accelerate EKS. | Los umbrales de alerta detallados ahora están disponibles en la tabla de alertas de referencia para el monitoreo de Amazon EKS. | 3 de mayo de 2024 |
| Actualizado: perfiles de configuración de Alarm Manager. | Se agregaron notas sobre la creación de alarmas de detección de anomalías con Alarm Manager. | 25 de abril de 2024 |
| Adiciones a los perfiles de configuración de Resource Tagger. | Las tablas de DynamoDB y los buckets de Amazon S3 ya están disponibles en Resource Tagger | 25 de abril de 2024 |
| Se agregó la sección de información sobre la gestión de eventos planificados (PEM). | La información detallada sobre la oferta de servicios PEM ya está disponible en la Guía del usuario de AMS Accelerate. | 25 de abril de 2024 |
| AMS es compatible con Red Hat Enterprise Linux (RHEL) 9.x. | AMS es compatible con Red Hat Enterprise Linux (RHEL) 9.x. | 25 de abril de 2024 |
| AMS Accelerate admite la generación de informes para todas las configuraciones AWS regionales. | AMS Accelerate admite la generación de informes de inventario mediante SSM para todas las configuraciones AWS regionales. | 25 de abril de 2024 |
| Actualizado: políticas AWS gestionadas. | Se actualizó AWSManagedServicesDeploymentToolkitPolicy con nuevos permisos de ECR. | 4 de abril de 2024 |

| | | |
|---|---|---|
| Actualizado: sección de perfiles de configuración del etiquetador de recursos | Añadido `AWS::EFS::FileSystem` a la ResourceTypelista. | 21 de marzo de 2024 |
| Actualizado: informes de incidentes y solicitudes de servicio en la sección Accelerate. | Se cambió el título del tema a Informes de incidentes, solicitudes de servicio y preguntas sobre facturación en Accelerate. Se agregó una nueva sección, Preguntas sobre facturación. | 21 de marzo de 2024 |
| Actualizado: sección sobre cómo funciona la gestión de las solicitudes de servicio. | Se ha añadido una aclaración sobre cómo AMS gestiona las solicitudes de servicio que contienen una solicitud de función o un error. | 21 de marzo de 2024 |
| Actualizado: cree el rol aws_managedservices_onboarding_role con la sección CloudFormation | Se agregaron comandos para crear el rol. AWS CloudShell | 21 de marzo de 2024 |
| Actualización: plantilla de inicio rápido (opcional) | Se agregaron comandos para descargar la plantilla AWS CloudShell. | 21 de marzo de 2024 |
| Hay nuevos tipos de recursos disponibles para los perfiles de configuración de Alarm Manager. | Se agregaron tipos de recursos para Amazon FSx, Amazon EFS y Elasticsearch a los perfiles de configuración de Alarm Manager. | 21 de marzo de 2024 |
| Hay disponibles sustituciones de pseudoparámetros adicionales para el perfil de configuración. | Se agregaron sustituciones de pseudoparámetros de Amazon EFS y Amazon FSx. | 21 de marzo de 2024 |

| | | |
|---|---|---|
| Se agregó una nueva sección a las características en el tema de descripción del servicio. | Se ha añadido una nueva sección, Gestión de solicitudes de servicio, en las funciones de AMS Accelerate. | 21 de marzo de 2024 |
| Se han añadido nuevas columnas al informe de autoservicio (informe semanal de incidentes) | Se agregaron nuevas columnas al informe semanal de incidentes para que pueda filtrar los incidentes según el trimestre, el mes, la semana o el día en que se creó o resolvió el incidente. | 11 de marzo de 2024 |

## Actualizaciones anteriores

En la siguiente tabla se describen los cambios importantes en la documentación de la guía AMS Accelerate antes de marzo de 2024.

| Cambio | Descripción | Fecha |
|---|---|---|
| Mejoras en la incorporación de CloudTrail senderos a AMS Accelerate | Mejoras en la incorporación de CloudTrail senderos a AMS Accelerate:<br>• Reúna todas las políticas de bucket en un solo bloque<br>• Elimine el segundo identificador de AWS la organización en las declaraciones de políticas<br>• Aclare los requisitos del entorno del cliente<br><br>Para obtener más información, consulte Revise y actualice sus configuraciones para permitir que AMS Accelerate utilice su CloudTrail sendero. | 23 de febrero de 2024 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualizado: proceso de incorporación de cuentas. | Se reestructuró la sección del proceso de incorporación de cuentas para que los pasos fueran más claros. También se agregó una plantilla de inicio rápido opcional para las funciones de incorporación.<br><br>Consulte Plantilla de inicio rápido (opcional) en Accelerate. | 22 de febrero de 2024 |
| Actualizado: se retira AMS Accelerate. | Se actualizó la sección de consideraciones sobre la desvinculación de AMS Accelerate para indicar que el proceso de desvinculación no elimina la `ams-access-management` CloudFormation pila ni la función de `ams-access-management` IAM.<br><br>Consulte AMS: acelera los efectos de desvinculación. | 22 de febrero de 2024 |
| Actualizado: conformidad con la configuración en Accelerate. | Se cambió la expresión «Informe de incidentes» por «Solicitud de servicio» cuando procedía para evitar confusiones sobre estos términos.<br><br>Consulte Cumplimiento de la configuración en Accelerate. | 22 de febrero de 2024 |
| Actualizado: descubrimiento de cuentas en Accelerate. | Se reorganizó la detección de cuentas en Accelerate para agrupar mejor los requisitos previos con la sección correspondiente.<br><br>Consulte Paso 1. Descubrimiento de cuentas en Accelerate. | 22 de febrero de 2024 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Se cambió el nombre: AMS Patch informa a la administr ación del host de AMS. | Se cambió el nombre de los informes de parches de AMS a la administración del host de AMS y se cambió el nombre del informe, informe de detalles del parche, a informe de cobertura de agentes de SSM.<br><br>Consulte Informes de gestión de hosts de AMS. | 22 de febrero de 2024 |
| Se actualizó el catálogo de operaciones bajo demanda | Se actualizó la tabla del catálogo de ofertas de Operations on Demand para eliminar las referencias a la «salud» en`Amazon EKS cluster maintenance` .<br><br>Consulte Solicitar AMS Operations On Demand. | 22 de febrero de 2024 |
| Se actualizó el router de eventos AMS | Se actualizó `AMSCoreRule` en la sección AMS Event Router.<br><br>Consulte Uso de Amazon EventBridge Managed Rules en AMS. | 22 de febrero de 2024 |
| Sistemas operativos compatibl es actualizados. | Se actualizaron los sistemas operativos compatibles para incluir SUSE Linux Enterprise Server 15 SP5.<br><br>Consulte Configuraciones admitidas. | 22 de febrero de 2024 |
| Se actualizó la automatización de la corrección del uso de volúmenes de EC2 | Se actualizó la sección de automatización de la remediación del uso de volúmenes de EC2 con el programa de expansión de capacidad correcto.<br><br>Consulte Automatización de la corrección del uso de volúmenes de EC2. | 22 de febrero de 2024 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualizado: revise y actualice sus configuraciones para que Accelerate pueda utilizar su ruta CloudTrail | Se actualizó la sección de políticas de cubos CloudTrail S3 de AMS Accelerate Organizat ion. Consulte Revise y actualice sus configura ciones para permitir que AMS Accelerate utilice su CloudTrail sendero | 15 de febrero de 2024 |
| Nueva función agregada: instalación automática de SSM Agent | Se agregó una nueva sección para la instalaci ón automática de SSM Agent<br><br>Consulte Instalación automática de SSM Agent. | 26 de enero de 2024 |
| Actualizado: configuraciones compatibles | Se agregó información sobre las versiones compatibles de AWS Control Tower<br><br>Consulte Configuraciones admitidas. | 26 de enero de 2024 |
| Actualizado: informes sobre los parches de AMS. | Se eliminaron tres secciones de los informes de parches de AMS:<br>• Informe resumido de detalles de la instancia de parche<br>• Informe de detalles del parche<br>• Informe de casos en los que no se detectaro n parches<br><br>Consulte Informes de gestión de hosts de AMS. | 22 de diciembre de 2023 |
| Actualizado: acelere los requisitos previos de incorpora ción. | Se actualizaron los planes de soporte necesarios para incorporar AMS Accelerate.<br><br>Consulte Acelere los requisitos previos de incorporación. | 15 de diciembre de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualizado: crea una ventana de mantenimiento de parches. | Se ha eliminado la sección del ciclo de parches predeterminado, ya que esta función está obsoleta.<br><br>Consulte Cree una ventana de mantenimiento de parches en AMS. | 13 de diciembre de 2023 |
| Actualizado: configuración de notificaciones en Accelerate. | Se aclaró qué correo electrónico se usa para las notificaciones.<br><br>Para obtener más información, consulte Configuración de notificaciones en Accelerate. | 12 de diciembre de 2023 |
| Actualización: `AMSAccelerateCustomerAccessPolicies` plantilla. | Se actualizó la `AMSAccelerateCustomerAccessPolicies` plantilla para corregir un error de sintaxis.<br><br>Para obtener más información, consulte Permisos para usar las funciones de AMS. | 12 de diciembre de 2023 |
| Agregado: solicitar cambios, revisiones de seguridad | Se agregó una nueva sección sobre las revisiones de seguridad de las solicitudes de cambio en la sección Gestión de la seguridad.<br><br>Para obtener más información, consulte Revisiones de seguridad de la solicitud de cambios. | 11 de diciembre de 2023 |
| Actualizado: resource_inventory.xlsx | Se actualizó el archivo resource_inventory .xlsx para incluir las funciones de analista de seguridad.<br><br>Para obtener más información, consulte Inventario de recursos para Accelerate. | 17 de noviembre de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualizado: descripción del rol de ams-access-admin-operations | Se actualizó la descripción de ams-access-admin-operations.<br><br>Para obtener más información, consulte Por qué y cuándo AMS accede a tu cuenta y Autenticación con identidades en AMS Accelerate. | 17 de noviembre de 2023 |
| Actualizado: consideraciones sobre la desincorporación de AMS Accelerate | Se actualizó la sección de seguridad para aclarar lo que está disponible en Amazon GuardDuty y AWS Config las reglas después de la salida del servicio.<br><br>Para obtener más información, consulte AMS: acelera los efectos de desvinculación. | 17 de noviembre de 2023 |
| Se agregó: Supervisión y administración de incidentes para Amazon EKS | Monitoring and Incident Management for Amazon EKS supervisa los recursos de Amazon EKS para detectar errores, degradación del rendimiento y problemas de seguridad.<br><br>Para obtener más información, consulte Supervisión y gestión de incidentes para Amazon EKS en AMS Accelerate. | 14 de noviembre de 2023 |
| Actualizado: etiquetado | Se agregó información sobre el etiquetado proporcionado por el cliente.<br><br>Para obtener más información, consulte Etiquetas proporcionadas por el cliente en Accelerate. | 7 de noviembre de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualizado: perfiles de configuración del etiquetador de recursos | Se agregaron AWS::AutoScaling::AutoScaling Group, AWS: :EKS: :Cluster, AWS::Elasticsearch: :Domain y AWS: :FSx:: a la sección de filtros. FileSystem<br><br>Para obtener más información, consulte Perfiles de configuración del etiquetador de recursos en AMS Accelerate. | 27 de octubre de 2023 |
| Actualización: descripción del servicio | Se agregó Ubuntu 22.04 a los sistemas operativos compatibles. Consulte Descripción del servicio | 29 de septiembre de 2023 |
| Actualizado: Requisitos previos de incorporación de AMS Accelerate | Se agregó una nota a los puntos finales de VPC de AMS Accelerate para incluir una plantilla. CloudFormation Consulte Acelere los requisitos previos de incorporación. | 29 de septiembre de 2023 |
| Actualizado: ¿Detectar | Se ha eliminado el tipo de protección de puntos finales de la respuesta de seguridad de AMS Accelerate. Consulte Detect. | 29 de septiembre de 2023 |
| Actualizado: alertas de monitoreo de referencia en AMS | Se agregó AWS Outposts a la tabla de alertas de monitoreo de referencia. Consulte Detect monitoring-default-metrics. | 29 de septiembre de 2023 |
| Actualizado: cree el rol aws_managedservices_onboarding_role con CloudFormation | Captura de pantalla actualizada para Specify Stack Details. Consulte Cree `aws_managedservices_onboarding_role` con CloudFormation para Accelerate. | 29 de septiembre de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualizado: AMS Accelerate implementó Amazon EventBridge Managed Rules | Se ha añadido una nueva regla EventBridge gestionada por AMS Accelerate Amazon AMSCoreRule.<br><br>Se ha actualizado la regla de EventBridge gestión de Amazon de AMS Accelerate AMSAccessRolesRulepara añadir un nuevo rol.<br><br>Para obtener más información, consulte Amazon EventBridge Managed Rules implementadas por AMS. | 19 de septiembre de 2023 |
| Actualizado: perfiles de configuración de Alarm Manager | Se agregaron identificadores de sustitución de pseudoparámetros de AWS Outposts. Consulte Supervisión y gestión de eventos en AMS Accelerate. | 11 de septiembre de 2023 |
| Actualizado: perfiles de configuración de Resource Tagger | Se agregó el tipo de recurso AWS Outposts. Consulte Perfil de configuración de Accelerate: sustitución de pseudoparámetros. | 11 de septiembre de 2023 |
| Actualizado: servicios compatibles | Se agregó Amazon Elastic File System a la sección Servicios monitoreados por CloudWatch alarmas.<br><br>Para obtener más información, consulte Descripción del servicio. | 6 de septiembre de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualizado: monitoreo de parches y corrección de errores | Se agregó la siguiente nota a la sección Uso de Patch Orchestrator:<br><br>«Las alertas de error de los parches no se crean para las instancias que tienen sistemas operativos no compatibles o que se detienen durante el período de mantenimiento»<br><br>Para obtener más información, consulte Comprenda la administración de parches en AMS Accelerate. | 6 de septiembre de 2023 |
| Actualizado: manual de respuesta aclarado a los eventos de malware | Se ha aclarado el manual de respuesta a los eventos de malware para la respuesta a los incidentes de seguridad. Para obtener más información, consulte Respuesta a incidentes de seguridad en AMS. | 6 de septiembre de 2023 |
| Actualizado: Cómo conectar tu cuenta de Accelerate con Transit Gateway | Pasos aclarados para conectar una nueva VPC de una cuenta de Accelerate a la red AMS Multi-Account Landing Zone (crear un adjunto de VPC de TGW): consulte Conectar su cuenta de Accelerate con Transit Gateway para obtener más información. | 5 de septiembre de 2023 |
| Actualizado: alertas del monitoreo de referencia en AMS | Se eliminó la referencia a dos alarmas obsoletas AMSReadLatencyAlarm y AMSWriteLatencyAlarm. Para obtener más información, consulte Alertas del monitoreo de referencia en AMS. | 5 de septiembre de 2023 |
| Se agregó: AMS Event Router | Se agregó documentación para el AMS Event Router. Consulte Uso de Amazon EventBridge Managed Rules en AMS para obtener más información. | 5 de septiembre de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualizado: lista de pseudoparámetros de Alarm Manager. | Se actualizó la lista de pseudoparámetros de Alarm Manager. El parámetro de nombre de instancia EC2 se agregó a las configuraciones de alarma de disco EC2 y de instancia EC2. Para obtener más información, consulte Perfil de configuración de Accelerate: sustitución de pseudoparámetros. | 29 de agosto de 2023 |
| Se agregó: AMS Access Offboarding | Se ha añadido una consideración a la hora de cancelar la contratación de AMS Access. Consulte AMS: acelera los efectos de desvinculación. | 24 de agosto de 2023 |
| Se agregó: Respuesta a incidentes de seguridad de AMS | Se agregó documentación para usar la respuesta a incidentes de seguridad de AMS. Consulte Respuesta a incidentes de seguridad en AMS. | 18 de agosto de 2023 |
| Actualizado: AMS Accelerate accede a las funciones | Se ha corregido un error tipográfico en los nombres de los roles. Consulte AWS Identity and Access Management en AMS Accelerate. | 10 de agosto de 2023 |
| Actualizado: Declaraciones de política | Se reemplazaron los nombres de los roles codificados de forma rígida por caractere s comodín. Consulte Revise y actualice sus configuraciones para permitir que AMS Accelerate utilice su CloudTrail sendero. | 10 de agosto de 2023 |
| Actualizado: lista de servicios monitoreados con alertas de EFS. | Se actualizó la lista de servicios de monitoreo con nuevas alertas de EFS para el monitoreo de referencia de AMS. Se agregaron 4 nuevos tipos de alertas de EFS. Para obtener más información, consulte Alertas del monitoreo de referencia en AMS. | 3 de agosto de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualizado: tabla de inventario de recursos de Acelerate | Se eliminaron ams-backup-config-rule-stack y los recursos relacionados. Consulte Inventario de recursos para Accelerate. | 18 de julio de 2023 |
| Actualizado: AMS Accelerate accede a las funciones | <8-digit hash><8-digit hash>Se eliminaron los roles ams-backup-config-rule-st-ams y ams-backup-config-rule-st-amsBackupAlertConfigRule. BackupPlanConfigRuleH Consulte AWS Identity and Access Management en AMS Accelerate. | 18 de julio de 2023 |
| Actualizado: lista de alertas de RDS monitorizadas. | Se actualizó la lista de alertas de RDS para el monitoreo de referencia de AMS. Se agregaron 9 nuevos tipos de alertas de RDS y se eliminaron 3 tipos de alertas de RDS existentes. Para obtener más información, consulte Alertas del monitoreo de referencia en AMS. | 19 de junio de 2023 |
| Nuevo: las funciones de acceso de AMS Accelerate | Se agregaron nuevas funciones de acceso para AMS Security. | 16 de junio de 2023 |
| Nuevo: la administración de CloudTrail registros de AMS Accelerate ahora puede utilizar los registros de CloudTrail los clientes. | Se actualizaron las opciones compatibles con Accelerate para la gestión de CloudTrail registros, que incluyen el registro implementado de Accelerate o la integración con el registro de la organización o la CloudTrail cuenta gestionada por el cliente. Para obtener más información, consulte Revise y actualice sus configuraciones para permitir que AMS Accelerate utilice su CloudTrail sendero. | 09 de junio de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualizado: Informe de configuración de respuesta de AMS Accelerate Config Rules. | Se actualizaron los informes a pedido para el informe de configuración de respuesta de AWS Config Rules. Consulte Acelerar las actualizaciones de los informes a pedido. Consulte Informe de configuración de respuesta de AMS Config Rules. | 26 de mayo de 2023 |
| Actualizado: Política de fecha de inicio de facturación del servicio. | Definiciones actualizadas de la fecha de inicio de la facturación enTérminos clave de AMS. | 15 de mayo de 2023 |
| Actualizado: políticas AWS gestionadas. | Se actualizó AWSManagedServicesDeploymentToolkitPolicy con nuevos permisos de CFN y ECR y se amplió el alcance de las acciones existentes con caracteres comodín. Consulte Acelerar las actualizaciones de los roles vinculados al servicio. Consulte Acelere las actualizaciones de las funciones vinculadas al servicio. | 9 de mayo de 2023 |
| Actualizado: acceda a los enlaces de la política de roles. | Los roles de acceso ahora se pueden descargar directamente desde las ubicaciones de los depósitos de Accelerate S3.<br><br>Consulte Por qué y cuándo AMS accede a tu cuenta y AWS Identity and Access Management en AMS Accelerate. | |
| Actualizado: Self-Service informe de facturación mensual. | Nota adicional: Los informes de facturación mensual solo están disponibles en una cuenta de Management Payer (AMS Advanced multi-account landing zone), pero están disponibles para todas las cuentas AMS Accelerate-managed vinculadas.<br><br>Consulte Informe de facturación (mensual). | 13 de abril de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualización: lista de alertas. | CloudTrail Referencias eliminadas.<br><br>Consulte Administración de registros en AMS Accelerate. | 13 de abril de 2023 |
| Actualizado: Lista de alertas. | Se agregaron tres nuevas alertas de agentes de SSM.<br><br>Consulte Alertas del monitoreo de referencia en AMS. | 13 de abril de 2023 |
| Actualizado: acelere los requisitos previos. | Se aclaró que Accelerate requiere la existencia de uno de los cuatro planes de AWS Support y no incluye el plan para desarrolladores.<br><br>Consulte Acelere los requisitos previos de incorporación. | 13 de abril de 2023 |
| Actualizado: política de funciones vinculadas al servicio de Accelerate. | Se ha actualizado el archivo zip de la política del Servicio de Contactos.<br><br>Consulte AWS políticas gestionadas para AMS Accelerate. | 13 de abril de 2023 |
| Actualizado: Programador de recursos de AMS. | Nombre de función incorrecto AWSManage dServices-DescribeScheduleOrPeriod, corregido a AWSManagedServices-Describe ScheduleOrPeriods. Consulte Optimización de costes con AMS Resource Scheduler. | 13 de abril de 2023 |
| Actualizado: políticas AWS gestionadas. | Se actualizó Respuestas a los hallazgos personalizados con instrucciones para actualizar las respuestas personalizadas en una o varias cuentas. | 13 de abril de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualizado: Resource Tagger | Se agregaron advertencias sobre «especifi car el nombre de la nueva configuración (SampleConfigurationBlock en el ejemplo proporcionado), ya que podría anular inadverti damente la AMS-managed configuración con el mismo nombre». Consulte Casos de uso de Resource Tagger en AMS Accelerate. | 16 de marzo de 2023 |
| Actualizado: parche RACI | Varias actualizaciones y aclaraciones de la RACI para la aplicación de parches. Consulte Descripción del servicio. | 16 de marzo de 2023 |
| Actualizado: Acciones en el kit de herramientas de despliegu e SLR JSON | Política y acciones actualizadas. Consulte: Uso de funciones vinculadas a servicios para AMS Accelerate. | 16 de marzo de 2023 |
| Actualizado: remediación automática | Se ha eliminado el soporte de LVM para la automatización de volúmenes de EC2. Consulte: Remediación automática de alertas por parte de AMS. | 16 de marzo de 2023 |
| Actualizado: acelere la incorporación. | Se ha aclarado el uso de los roles, especialm ente el rol mínimo. La plantilla para crear funciones de AMS | 16 de marzo de 2023 |
| Actualizado: Self-service presentación de informes. | Los informes de respaldo diarios ahora son compatibles con las regiones principales y secundarias. Ambos se indican en el campo Región de recursos deInforme de Backup (diario). | 16 de marzo de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualizado: Guía de aplicación de parches | Se ha añadido una advertencia para no personalizar las líneas base de aplicación de parches predeterminadas, que son gestionadas por AMS. En su lugar, cree una nueva línea base de aplicación de parches personalizada. Consulte: Línea base predeterminada del parche y. Línea base de parches personalizada con AMS Accelerate | 16 de marzo de 2023 |
| Política de terminación del servicio actualizada. | Definiciones actualizadas de terminación del servicio y fecha de finalización del servicio enTérminos clave de AMS. Las notificaciones de rescisión deben emitirse antes del día 20 del mes anterior al último mes completo. | 16 de marzo de 2023 |
| Actualizado: políticas AWS gestionadas. | Nombre de la política aclarado:Contacta con el rol vinculado al servicio para AMS Accelerate. | 16 de febrero de 2023 |
| Nuevo: políticas AWS gestionadas. | Política añadida:Contacta con el rol vinculado al servicio para AMS Accelerate. | 16 de febrero de 2023 |
| Actualizado: conformidad con la configuración. | Se corrigió una palabra mal escrita en:. Cumplimiento de la configuración en Accelerate | 16 de febrero de 2023 |
| Contenido nuevo: sistemas operativos no compatibles | Se agregó información sobre los servicios que ofrece AMS para los sistemas operativos (SO) no compatibles, consulte. Capacidades para sistemas operativos no compatibles en Accelerate | 16 de febrero de 2023 |
| Actualizado: Crea ventanas de parches | Se agregó un enlace CloudShell para usarloCree una ventana de mantenimiento con la interfaz de línea de comandos (CLI) de Systems Manager para AMS Accelerate. | 16 de febrero de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Contenido actualizado: recursos de gestión de la incorporación | Se actualizaron las plantillas JSON comprimid as en. La plantilla para crear funciones de AMS | 16 de febrero de 2023 |
| Contenido nuevo: conformidad con la configuración | Se agregó un tema nuevo:Respuestas a los hallazgos personalizados. | 16 de febrero de 2023 |
| Nuevo: políticas AWS gestionadas. | Política añadida:Amazon regula EventBrid ge la función vinculada al servicio para AMS Accelerate. | 07 de febrero de 2023 |
| Actualizado: políticas AWS gestionadas. | Se actualizó `AWSManagedServices DeploymentToolkitPolicy` con los nuevos permisos de S3. Consulte Acelere las actualizaciones de las funciones vinculadas al servicio. | 30 de enero de 2023 |
| Nueva región de suscripción: CPT. | AMS Accelerate ya está disponible en la región de suscripción voluntaria de Ciudad del Cabo (CPT). Para suscribirse, consulte Administr ación. Regiones de AWS | 12 de enero de 2023 |
| Actualización: descripción del servicio. | Se agregaron servicios FSx monitoreados por CloudWatch alarmas a. Descripción del servicio | 12 de enero de 2023 |
| Actualizado: monitoreo de las métricas predeterminadas. | Se agregaron 6 alarmas FSx a. Alertas del monitoreo de referencia en AMS | 12 de enero de 2023 |
| Actualizado: patrones AMS. | Se agregó Personalizar las notificaciones de alarma de Cloudwatch aPatrones AMS. | 12 de enero de 2023 |
| Actualizado: recursos de gestión de la incorporación. | Se actualizó la tabla de plantillas y se agregó una fila para `ams-onboarding-ssm-execution-role` entrarLa plantilla para crear funciones de AMS. | 12 de enero de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualizado: conformidad con la configuración. | Detalles adicionales para solicitar solucione s personalizadas (en el cuadro Important e) enCumplimiento de la configuración en Accelerate. | 12 de enero de 2023 |
| Actualizado: Service-linked-rol e permisos. | Se eliminaron los permisos antiguos o duplicados. Consulte Uso de funciones vinculadas a servicios para AMS Accelerate. | 15 de diciembre de 2022 |
| Actualizado: administración de parches, ventanas de mantenimiento. | Se agregó una guía a las instrucciones de la consola (paso 5) para crear un período de mantenimiento. Consulte Cree una ventana de mantenimiento desde la consola de Systems Manager para AMS Accelerate. | 15 de diciembre de 2022 |
| Nuevo: sección de administr ación de parches. | Se ha añadido una sección para las ventanas de mantenimiento de Patch Tuesday. Consulte Cree una ventana de mantenimiento periódica «Patch Tuesday» desde la consola AMS (recomendado). | 15 de diciembre de 2022 |
| Actualizado: Programador de recursos AMS. | Se actualizó el nombre de la CloudFormation pila. Consulte Uso de recursos con AMS Resource Scheduler. | 15 de diciembre de 2022 |
| Actualizado: etiquete sus recursos para respaldarlos. | Se agregó una guía para usar AMS Resource Tagger. Consulte Etiquete sus recursos para aplicar los planes de respaldo de AMS. | 15 de diciembre de 2022 |
| Actualizado: selecciona un plan de respaldo. | Indicó qué planes ofrecen copias de seguridad continuas. Consulte Seleccione un plan de respaldo de AMS. | 15 de diciembre de 2022 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualizado: Programador de recursos AMS. | Se actualizó el ejemplo de AWS CLI para eliminar un período o un programa. Consulte Trabajar con períodos y cronogramas en AWS Managed Services Resource Scheduler. | 15 de diciembre de 2022 |
| Actualizado: políticas AWS gestionadas. | Se agregó el`AWSManagedServices DeploymentToolkitPolicy` . Consulte AWS políticas gestionadas para AMS Accelerate. | 15 de diciembre de 2022 |
| Nuevo: se agregó una sección que describe la nueva función vinculada al servicio de AMS, AWSServiceRoleForManagedServices _. Detective ControlsConfig | Se agregaron GovCloud regiones y permisos. Consulte El Detective controla la función vinculada al servicio para AMS Accelerate. | 15 de diciembre de 2022 |
| Nuevo: política AWS gestionada | Se agregó una sección que describe cómo se usa la política AWS-administrada, AWSManagedServices _AlarmManagerPermissionsBoundary, en la política de roles vinculados al servicio, AWSManagedServices _ AlarmManager _ServiceRolePolicy, para restringir los permisos de los roles de IAM creados por el rol vinculado al servicio _. AWSServiceRoleForManagedServices AlarmManager Consulte AWS políticas gestionadas para AMS Accelerate. | 15 de diciembre de 2022 |
| Actualizado: Operaciones bajo demanda. | Ofertas adicionales: SQL Server en EC2 Operations y AMI Building and Vending. Consulte Operaciones bajo demanda. | 10 de noviembre de 2022 |
| Actualizado: Monitoreo y gestión de eventos. | Explicación actualizada de las notificaciones de servicio y los informes de incidentes. Consulte Cómo funciona la supervisión. | 10 de noviembre de 2022 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualizado: regiones de Service-linked roles | Se agregaron GovCloud regiones y permisos. Consulte Uso de funciones vinculadas a servicios para AMS Accelerate. | 10 de noviembre de 2022 |
| Nuevo: Service-linked rol. | Se agregó un nuevo rol:`AWSServiceRoleForAMSDetectiveControls` .<br><br>Consulte El Detective controla la función vinculada al servicio para AMS Accelerate. | 10 de noviembre de 2022 |
| Actualizado: Gestión de acceso. | Subsecciones actualizadas con instrucciones mejoradas. Consulte Gestión de acceso en AMS Accelerate. | 10 de noviembre de 2022 |
| Actualizado: descripción del servicio. | Se actualizaron los patrones AMS en la matriz RACI. Consulte Descripción del servicio. | 10 de noviembre de 2022 |
| Actualizado: patrones AMS. | Los clientes son responsables de la implement ación de los patrones. Consulte Patrones AMS. | 10 de noviembre de 2022 |
| Actualizado: Offboarding. | Se agregaron detalles sobre lo que ocurre con los recursos específicos de Backup and Monitoring durante la desconexión. Consulte Fuera de AMS Accelerate. | 10 de noviembre de 2022 |
| Actualizado: administración de parches.. | Guía actualizada y abreviada sobre las políticas de IAM. Consulte Creación de una función de IAM para la aplicación de parches bajo demanda a AMS Accelerate. | 10 de noviembre de 2022 |
| Nuevo: enlaces a diagramas de arquitectura. | Se han añadido enlaces a varios temas a los diagramas de arquitectura de referencia de AMS. Por ejemplo, consulte Supervisión y gestión de eventos en AMS Accelerate. | 10 de noviembre de 2022 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Nuevo: oferta de operaciones bajo demanda | Se agregó la sección «Operaciones acelerado ras en la zona de aterrizaje». Consulte Operaciones bajo demanda. | 13 de octubre de 2022 |
| Actualización: gestión de la supervisión. Las alertas generan informes de incidente s, no solicitudes de servicio | Cómo funciona la supervisión. | 13 de octubre de 2022 |
| Nuevo: creación de una ventana de mantenimiento de parches con una Accelerate-custom plantilla CFN | CloudFormation plantillas de configuración de ventanas de parches. Consulte Cree una ventana de mantenimiento de parches en AMS. | 15 de septiembre de 2022 |
| Actualizado: Offboarding | Hizo hincapié en que los planes de respaldo de Accelerate ya no funcionan después de la desconexión. Consulte Fuera de AMS Accelerate. | 15 de septiembre de 2022 |
| Actualizado: detalles CloudWatch del cambio de configuración | Se ha corregido un error en los ejemplos de Windows y Linux. Consulte CloudWatch detalles del cambio de configuración. | 15 de septiembre de 2022 |
| Actualizado: Uso del programador de recursos AMS | Se agregó una guía sobre las etiquetas de asignación de costos. Consulte Estimador de costos en AMS Resource Scheduler. | 15 de septiembre de 2022 |
| Actualizado: Biblioteca de reglas de configuración AMS | Se agregaron dos reglas de `ams-eks-` configuración a la tabla de reglas. Consulte Biblioteca de reglas AMS Config. | 15 de septiembre de 2022 |
| Actualizado: Backup Management | Se eliminó la etiqueta engañosa PITR (recuperación puntual) de los títulos y descripci ones de los planes de respaldo. Consulte Seleccione un plan de respaldo de AMS. | 15 de septiembre de 2022 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualización: descripción del servicio Accelerate | Descripciones actualizadas de las reglas de configuración y los canarios. Consulte Descripción del servicio. | 15 de septiembre de 2022 |
| Actualizado: descripción del servicio, configuraciones compatibles | Se ha eliminado la fecha de fin de servicio de Windows 2008 R2. Accelerate no es compatibl e con Windows 2008. Consulte Configura ciones admitidas. | 11 de agosto de 2022 |
| Actualización: descripción del servicio, funciones y responsabilidades | Se actualizó la tabla RACI. Se eliminaron los registros de acceso al ELB de la última fila de la sección de redes. No habilitamos los registros de acceso al ELB para los clientes de Accelerate. Consulte Funciones y responsab ilidades. | 11 de agosto de 2022 |
| Actualizado: conformidad con la configuración | Se corrigió un error tipográfico en la columna de marcos de la tabla de reglas. NIST-CSF aparecía incorrectamente como NIST-CIS. Consulte Cumplimiento de la configuración en Accelerate. | 11 de agosto de 2022 |
| Nuevo: Acelere la desconexi ón | Consideraciones y proceso de desvinculación. Consulte Cómo dejar de operar AMS Accelerat e. | 11 de agosto de 2022 |
| Actualización: lista de los sistemas operativos de los agentes SSM preinstalados | Se agregó «Ubuntu Linux 18.04 y 20.04» a la lista. Consulte Incorporación de EC2 instancias para acelerar. | 11 de agosto de 2022 |
| Nuevo: Programador de recursos | Utilice el programador de recursos de AMS para optimizar los costos al detener e iniciar los recursos solo cuando sea necesario. Consulte Optimización de costes con AMS Resource Scheduler. | 14 de julio de 2022 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualización: descripción del servicio del programador de recursos | Se actualizaron varias secciones de la descripción del servicio para la nueva oferta de Resource Scheduler. Consulte Descripción del servicio. | 14 de julio de 2022 |
| Nuevo: AMS Patterns | AMS ofrece plantillas de patrones, una solución generalizada que resuelve una familia de casos de uso en el entorno gestionado por AMS. Primer patrón en oferta:Patrones AMS. | 14 de julio de 2022 |
| Nuevo: nota de optimización de costes | Se agregó una nota que explica cómo los costos pueden aumentar con el uso de los recursos. Consulte Inventario de recursos para Accelerate. | 14 de julio de 2022 |
| Actualizado: Reglas de configuración de AMS | Se reorganizaron las tablas en. Biblioteca de reglas AMS Config La tabla HTML tiene menos columnas, para que sea más fácil de leer de un vistazo. La hoja de cálculo descargable tiene columnas adicionales que permiten ordenar y filtrar. | 14 de julio de 2022 |
| Actualizado: Gestión de acceso | Se actualizó la CloudFormation plantilla de muestra enPermisos para usar las funciones de AMS. La `AMSAccelerateAdmin Access` política ahora incluye las `IAMReadOn lyPolicy` políticas `AmsResourceSchedul erPassRolePolicy` y. | 14 de julio de 2022 |
| Actualizado: Self-Service Informes | Se agregaron instrucciones para cifrar AWS Glue los metadatos con claves KMS. Consulte el recuadro denominado Importante activado. Informes de autoservicio | 14 de julio de 2022 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualizado: monitoreo de referencia del AMS | Se agregó DeleteRecoveryPoint una alerta de respaldo. Alertas del monitoreo de referencia en AMS | 14 de julio de 2022 |
| Actualizado: sistemas operativos compatibles | Se agregó la fecha de fin de soporte para Amazon Linux 2. Descripción del servicio | 14 de julio de 2022 |
| Actualizado: Informes de AMS | Se agregó una nota sobre Opt-in las regiones. Informes y opciones | 14 de julio de 2022 |
| Programador de recursos | Se agregó información sobre la incorporación y el uso del programador de recursos de AMS para ayudar a optimizar los costos mediante la programación de las horas de inicio y parada de los recursos. Además, se actualizó la descripción del servicio Accelerate para incluir una mención al Resource Scheduler. Además, se actualizó la fecha de finalización del soporte compatible con Amazon Linux 2 a 2024. Consulte Optimización de costes con AMS Resource Scheduler y Descripción del servicio. | 30 de junio de 2022 |
| Nueva alarma | Se ha añadido una AWS Backup alarma. Alertas del monitoreo de referencia en AMS | 21 de junio de 2022 |
| Contenido nuevo | Se agregó el contenido del rol vinculado al servicio. Uso de funciones vinculadas a servicios para AMS Accelerate | 16 de junio de 2022 |
| | AWS Network Firewall Operations se agregó al catálogo de ofertas de Operations on Demand (OOD). Operaciones bajo demanda | 16 de junio de 2022 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Contenido actualizado | Se agregó la descripción de la función de administración de problemas. Descripción del servicio | 16 de junio de 2022 |
| | Se agregó una nota sobre el conjunto de reglas de configuración que no admite determinadas regiones de suscripción. Cumplimiento de la configuración en Accelerate | 16 de junio de 2022 |
| | Conformidad con la configuración. «Bibliote ca de reglas de AMS Config» -> «Tabla de reglas», se actualizó y se eliminó solo a ZIP. Cumplimiento de la configuración en Accelerate | 16 de junio de 2022 |
| | Se eliminaron los correos electrónicos de escalada. Ruta de escalación | 16 de junio de 2022 |
| | Se ha movido la lista de temas a la parte inferior de los párrafos iniciales. ¿Qué es AMS Accelerate? | 16 de junio de 2022 |
| | Se actualizó el contenido de la corrección automática. Remediación automática de alertas por parte de AMS | 16 de junio de 2022 |
| Contenido actualizado: Descripción del servicio | Se agregó EKS a la lista de servicios monitorea dos por AMS Config Rules enServicios admitidos.<br><br>Se actualizó la descripción de la supervisión en la tabla RACI deFunciones y responsab ilidades. | 12 de mayo de 2022 |
| Contenido actualizado: Conformidad con la configura ción | Se agregaron reglas de EKS-related configura ción. Consulte Cumplimiento de la configura ción en Accelerate. | 12 de mayo de 2022 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Contenido actualizado: Cómo empezar, descubrimiento de cuentas | Se agregó una versión más reciente del AwsAccountDiscoveryCli script (en el archivo zip del registro de cambios de Account Discovery) en. Paso 1. Descubrimiento de cuentas en Accelerate | 12 de mayo de 2022 |
| Contenido actualizado: monitoreo, métricas predeterminadas | Se actualizaron las condiciones de activación de ALB-related las métricas. Consulte Alertas del monitoreo de referencia en AMS. | 12 de mayo de 2022 |
| Contenido actualizado: Parcheando la incorporación | Se ha añadido un requisito previo explícito para la instalación de parches: es necesario suscribirse a EBS. Consulte Integración de parches en Accelerate. | 12 de mayo de 2022 |
| Contenido actualizado: tabla de inventario de recursos de Accelerate | Se modificaron las reglas de ams-detective-controls-config-rules-cdk y se agregaron reglas para ams-detective-controls-recorder-cdk y ams-detective-controls-infrastructure-cdk. Consulte Inventario de recursos para Accelerate. | 14 de abril de 2022 |
| Contenido actualizado: Conformidad con la configuración | Introducción a los estándares del sector, las reglas de configuración y los tipos de respuestas. Hace hincapié en que los clientes no eligen reglas o respuestas de configuración individuales. Cumplimiento de la configuración en Accelerate. | 14 de abril de 2022 |
| Contenido actualizado: descripción del servicio | Se trasladó la sección actual sobre el alcance de los cambios a Funciones y responsabilidades. Consulte Funciones y responsabilidades. | 14 de abril de 2022 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Contenido actualizado: Etiquetado y monitoreo | Se agregó `AWS::Synthetics:Canary` a las listas de tipos de recursos permitidos para el etiquetado y la supervisión. Consulte Perfiles de configuración del etiquetador de recursos en AMS Accelerate y Perfil de configuración de Accelerate: sustitución de pseudoparámetros. | 14 de abril de 2022 |
| Contenido actualizado: Acelere los requisitos previos | Se agregaron permisos SSM-required de bucket a. Amazon EC2 Systems Manager en Accelerate | 14 de abril de 2022 |
| Contenido nuevo: aplicación de parches y supervisión | Se agregó un código de muestra para usar Cloudformation para implementar configura ciones de etiquetado y monitoreo. Consulte Implementación de un perfil de configuración con CloudFormation for Accelerate y Uso CloudFormation para implementar Accelerate los cambios de configuración. | 10 de marzo de 2022 |
| Contenido actualizado: consola de mantenimiento de parches | Se han reordenado los pasos Cree una ventana de mantenimiento desde la consola de Systems Manager para AMS Accelerate para que coincidan con la interfaz de la consola. | 10 de marzo de 2022 |
| Contenido actualizado: CLI de mantenimiento de parches | Parámetros CLI actualizados (horario, duración y límite) para Cree una ventana de mantenimi ento con la interfaz de línea de comandos (CLI) de Systems Manager para AMS Accelerate | 10 de marzo de 2022 |
| Contenido nuevo: Auto Instance Config | Se agregó la definición de `AMSInstan ceProfileBasePolicy` to Detalles de cambio de permisos de IAM | 10 de marzo de 2022 |
| Contenido nuevo: Incorpora ción | Se agregó un ejemplo de comando de Linux a Conectividad a Internet saliente en Accelerate | 10 de marzo de 2022 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Contenido nuevo: Incorporación | Se agregó una opción de privilegios mínimos a. La plantilla para crear funciones de AMS | 10 de marzo de 2022 |
| Contenido actualizado: Acelere las instrucciones de escalamiento | Se agregaron guías, enlaces y contactos de correo electrónico a Ruta de escalación | 10 de marzo de 2022 |
| Contenido actualizado: Configuraciones compatibles | AMS espera finalizar el soporte para RHEL 6 y 7 el 14 de CentOs marzo de 2023. Consulte Configuraciones admitidas | 10 de marzo de 2022 |
| Contenido actualizado: tabla de recursos | Se agregaron las funciones de acceso e IAM de AMS a la tabla de Inventario de recursos para Accelerate recursos | 10 de marzo de 2022 |
| Contenido actualizado: Onboarding and Backup | Se agregaron instrucciones para suscribirse a y AWS Backup Incorporación en AWS Backup Accelerate Gestión de la continuidad en AMS Accelerate | 10 de marzo de 2022 |
| Contenido actualizado: Administración de acceso | Se eliminaron Advanced-specific las instrucciones de la guía de AccelerateCómo y cuándo usar la cuenta de usuario root en AMS. | 10 de marzo de 2022 |
| Contenido actualizado: Configuraciones compatibles | AMS ahora es compatible con Oracle Linux 8.3 y Ubuntu 18.04 y 20.04. Consulte Configuraciones admitidas. | 28 de febrero de 2022 |
| Contenido actualizado: Acuerdo de nivel de servicio | Se actualizó el acuerdo de nivel de servicio descargable enServicios admitidos. | 28 de febrero de 2022 |
| Contenido actualizado: Gestión de acceso | Actualizado Cómo accede AMS a tu cuenta con preguntas frecuentes sobre las funciones de la consola de operador de AMS y una advertencia para no modificarlas ni eliminarlas. | 28 de febrero de 2022 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Contenido actualizado: Alarm Manager | Actualizado Perfil de configuración de Accelerate: monitoreo. Alarm Manager ya no se limita a las alarmas de una sola métrica. | 28 de febrero de 2022 |
| Contenido actualizado: Cómo empezar | Actualizado Paso 2. Incorporación de recursos de gestión en Accelerate. Se agregó una función de IAM con un acceso mínimo a los recursos de incorporación. | 28 de febrero de 2022 |
| Contenido nuevo: alcance de los cambios en la descripción del servicio | Se agregó una nueva sección, Alcance de los cambios realizados por AMS Accelerate que hace hincapié en los límites y las acciones que AMS Accelerate no realiza. | 10 de febrero de 2022 |
| Contenido actualizado: Cómo empezar | El nuevo proceso de incorporación comienza con la configuración y las funciones predeterminadas antes de personalizarlas. Las subsecciones contienen objetivos específicos de las funciones y enlaces relacionados. Consulte Cómo empezar con AMS Accelerate. | 10 de febrero de 2022 |
| Contenido actualizado: AMS Backup Management. | Acortó y reorganizó el Gestión de la continuidad en AMS Accelerate capítulo para facilitar la lectura. | 10 de febrero de 2022 |
| Contenido actualizado: etiquetado | Se agregó una sección de herramientas de etiquetado para incluir ejemplos de código CloudFormation y otras herramientas. Consulte Etiquetado en AMS Accelerate. | 10 de febrero de 2022 |
| Contenido actualizado: Monitorización de referencia | La mejora del estado de activación de la alarma de RedShift clúster reduce las falsas alarmas durante el mantenimiento. Consulte Alertas del monitoreo de referencia en AMS. | 10 de febrero de 2022 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Contenido actualizado: Parcheo | Se actualizó un ejemplo de comando CLI para registrar una ventana de mantenimiento. Consulte Cree una ventana de mantenimiento con la interfaz de línea de comandos (CLI) de Systems Manager para AMS Accelerate. | 10 de febrero de 2022 |
| Contenido actualizado: AWS Config Rules Inventory. | Se ha eliminado la regla `ams-nist-cis-ec2-security-group-attached-to-eni` de configuración obsoleta de la tabla de inventario de reglas de AWS configuración. Consulte Tabla de reglas. | 27 de enero de 2022 |
| Contenido nuevo: creación de ventanas de mantenimiento de parches. | Se agregó un enlace al tutorial de SSM y ejemplos de comandos para crear ventanas de mantenimiento de parches desde la línea de comandos. Consulte Cree una ventana de mantenimiento con la interfaz de línea de comandos (CLI) de Systems Manager para AMS Accelerate. | 27 de enero de 2022 |
| Contenido nuevo: Resource Tagger reconoce el nuevo tipo de recurso de Auto Scaling Groups (ASG). | Se agregaron grupos de Auto Scaling a los tipos de recursos filtrables con los perfiles de configuración de Resource Tagger. Consulte Sintaxis y estructura. | 13 de enero de 2022 |
| Contenido nuevo: planes de respaldo y bóvedas adicionales. | Se agregaron nuevos planes y bóvedas de respaldo para mitigar los escenarios de alto riesgo, incluidos los ataques de ransomware. Consulte Ver copias de seguridad en bóvedas de AMS y Ver copias de seguridad en bóvedas de AMS. | 13 de enero de 2022 |

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.